Provvedimento dell'8 febbraio 2024 [9991183]

VEDI ANCHE Newsletter del 7 marzo 2024

[doc. web n. 9991183]

Provvedimento dell'8 febbraio 2024

Registro dei provvedimenti
n. 62 dell'8 febbraio 2024

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 dott. Claudio Filippi, vice 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 d.lgs. 30 giugno 2003, n. 196 recante "Codice in materia di protezione dei dati personali (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 vice 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, doc. web n. 1098801;

Relatore l'avv. Guido Scorza;

PREMESSO

1. La violazione dei dati personali

La società Medtronic Italia (di seguito "Società"), con atto del XX, successivamente integrato con comunicazione del XX, ha notificato all'Autorità una violazione di dati personali, ai sensi dell'art. 33 del Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 (di seguito "Regolamento").

In relazione a tale evento, la Società ha comunicato che: “Il XX alle 15:30 circa, un membro del team Medtronic Diabete ha inviato una notifica via e-mail agli utenti dell’app MiniMed Mobile situati in vari paesi all'interno e all'esterno dell'UE per informarli su (1) un aggiornamento di manutenzione del server e (2) l'obbligo per gli utenti di accedere nuovamente al software CareLink™ Personal, come parte di questo aggiornamento di manutenzione del server. Sono state inviate un totale di 11 notifiche e-mail, utilizzando Microsoft Outlook, come soluzione temporanea in attesa dell'implementazione di un nuovo processo automatizzato. 10 notifiche e-mail contenevano tra 490 e 495 indirizzi e-mail, mentre 1 notifica e-mail conteneva 8 indirizzi e-mail. Sulla base dell'indagine eseguita fino ad oggi, il membro del team Diabete non ha seguito il processo definito da Medtronic per le interruzioni del server pianificate e non pianificate, e ha incluso gli indirizzi e-mail dei destinatari nel campo “A”, anziché nel campo “CCN”. A causa di questo errore umano, gli indirizzi e-mail dei destinatari erano visibili agli altri destinatari, ovvero circa 489-494 destinatari o 7 destinatari, a seconda dell'e-mail inviata. Sono stati esposti circa 5.001 indirizzi e-mail di utenti dell’app MiniMed Mobile in tutto il mondo, di cui 732 in Italia. Il contenuto della notifica e-mail non includeva alcun dato personale in modo che solo gli indirizzi e-mail erano visibili agli altri destinatari. Immediatamente dopo essere venuta a conoscenza del problema, Medtronic ha adottato misure per rimediare al problema e impedire che si ripresenti. È stato immediatamente effettuato un tentativo di richiamare tutte le e-mail e un'e-mail è stata inviata a tutti gli utenti interessati chiedendo loro di eliminare qualsiasi copia dell'e-mail ricevuta il XX. Medtronic ha formato nuovamente il personale interessato per ricordare loro l'importanza di seguire i processi standard di notifica e-mail e sta per implementare un nuovo strumento automatizzato per evitare che ciò possa accadere in futuro”.

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” e che “solo gli indirizzi e-mail erano visibili agli altri destinatari della e-mail. Il contenuto dell'e-mail non includeva alcun dato personale ma rivela che i destinatari sono utenti dell'app MiniMed Mobile e quindi persone che potrebbero essere affette da diabete”.

In relazione alle probabili conseguenze è stato valutato che “l’incidente potrebbe causare tentativi di phishing. Tuttavia, Medtronic ha adottato misure per richiamare le e-mail e ha chiesto a tutti gli utenti di eliminare qualsiasi copia dell'e-mail ricevuta in modo che Medtronic possa ragionevolmente aspettarsi che tali utenti si conformino alle istruzioni di Medtronic e non intraprendano ulteriori azioni con tali informazioni”.

Inoltre, la Società ha rappresentato di disporre di “una procedura rigorosa per le interruzioni pianificate e non pianificate del server con diversi passaggi da seguire per informare gli utenti. Tuttavia, la procedura standard di Medtronic non è stata seguita nel caso in esame. Inoltre, Medtronic sta rivedendo i suoi processi attuali per migliorarli ulteriormente, utilizzando un nuovo strumento automatizzato per evitare che questo incidente si verifichi in futuro”.

La Società ha, altresì, dichiarato che:

- per porre rimedio alla violazione e ridurne gli effetti negativi per gli interessati, “immediatamente dopo aver scoperto questo problema, Medtronic ha intrapreso una serie di azioni correttive, tra cui (1) il richiamo delle e-mail; (2) istruire i destinatari dell’e-mail a (i) eliminare qualsiasi copia dell'e-mail ricevuta con gli indirizzi e-mail del destinatario nel campo “a” e (ii) a non intraprendere ulteriori azioni con tali informazioni; e (3) formare nuovamente il personale interessato”;

- per prevenire simili violazioni future “sta rivedendo i propri processi per migliorarli ulteriormente (ad esempio, implementando ulteriori controlli prima di inviare qualsiasi notifica e-mail). Medtronic sta anche implementando un nuovo strumento per evitare che ciò accada in futuro”;

- “la medesima violazione viene riportata da altre consociate del gruppo Medtronic, ciascuna in qualità di titolare, alle Autorità competenti in tema di protezione dei dati di Belgio, Repubblica Ceca, Finlandia, Germania, Paesi Bassi, Norvegia, Spagna, Svezia, Francia, Regno Unito”.

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). In tale ambito, ad integrazione di quanto già comunicato, la Società, nel rappresentare di far parte del “gruppo Medtronic, il cui quartier generale operativo si trova negli Stati Uniti” e che “il gruppo Medtronic è un leader globale nello sviluppo e nella produzione di dispositivi medici per la cura e il trattamento di svariate patologie, tra cui il diabete”, ha dichiarato che:

- “l’app MiniMed™ Mobile è un’app Medtronic che collega - tramite Bluetooth - la pompa per insulina MiniMed™ allo smartphone dell'utente, consentendo a quest'ultimo di visualizzare le informazioni della pompa e del sensore sul proprio smartphone. L'app MiniMed™ Mobile richiede la registrazione a CareLink™ Personal, un software classificato come dispositivo medico (…)”;

- “una volta creato un account CareLink™ Personal e completata la registrazione l'app MiniMed™ Mobile riceve i dati dalla pompa per insulina MiniMed™ dell'utente e può essere, a discrezione di quest'ultimo, sincronizzata manualmente o automaticamente con l'account CareLink™ Personal dell'utente (…)” che ha lo scopo di “fornire una visualizzazione secondaria sullo smartphone dell'utente, per l'automonitoraggio da parte dell'utente stesso e per sincronizzare i dati con CareLink™ Personal”;

- “il trattamento dei dati personali degli utenti tramite CareLink™ Personal e la relativa app MiniMed Mobile è descritto in una specifica informativa sulla privacy (…). Trattandosi di una categoria speciale di dati personali (dati sanitari), viene richiesto il consenso esplicito degli utenti per la fornitura dei servizi, incluso l’invio agli utenti di comunicazioni di natura operativa, come gli aggiornamenti della manutenzione del server”;

- “l’informativa viene mostrata per la prima volta agli utenti, e il consenso è prestato da questi ultimi, al momento della registrazione su CareLink™ Personal prima che gli utenti forniscano dati personali” ed è “sempre assicurata la possibilità di modificare o revocare il proprio consenso in qualsiasi momento accedendo al proprio account personale (…)”;

- “l’app MiniMed™ Mobile è disponibile in vari Paesi. In ciascun Paese, la società del gruppo Medtronic ivi stabilita è responsabile della fornitura di assistenza tecnica e supporto agli utenti dell'app MiniMed™ Mobile residenti nel paese in cui tale società è stabilita, incluso l'invio di comunicazioni correlate. Di conseguenza, la scrivente Società agisce in qualità di titolare del trattamento dei dati personali degli utenti dell’app MiniMed™ Mobile ubicati in Italia (…)”;

- “nell'ambito del gruppo Medtronic, (…) [la Società] si avvale di funzioni centralizzate di helpdesk al fine di fornire servizi dl assistenza tecnica e di supporto. (…) forniti da Medtronic MiniMed, Inc. Tra tali servizi è inclusa la fornitura da parte di Medtronic MiniMed, Inc. di assistenza tecnica e supporto di secondo e terzo livello, per problemi che non possono

essere risolti localmente, nonché per l'invio di comunicazioni urgenti di interruzione dei servizi, come quella oggetto della notifica di violazione";

- "Medtronic MiniMed, Inc. fornisce tali servizi (…) in qualità di responsabile del trattamento mentre ciascuna di tali consociate (inclusa la scrivente Società) agisce quale autonomo titolare del trattamento dei dati personali degli utenti dell'app MiniMedTM Mobile che si trovano nel rispettivo Paese".

Con particolare riferimento alla natura transfrontaliera del trattamento, la Società ha rappresentato che:

- essa e, più in generale, il gruppo Medtronic, non hanno uno "stabilimento principale ai sensi dell'art. 4, par. 16, del Regolamento. La Società agisce esclusivamente in qualità di titolare in relazione al trattamento dei dati personali degli utenti dell'app MiniMed™ Mobile in Italia" e "non ha trattato i dati personali di soggetti ubicati al di fuori del territorio italiano, né per proprio conto né per conto di altre consociate del gruppo Medtronic stabilite in altri Stati membri dell'UE";

- "le consociate del gruppo Medtronic stabilite nel territorio dell'UE prendono decisioni autonome in merito alle finalità e ai mezzi del trattamento dei dati personali degli utenti dell'app MiniMed™ Mobile nel loro paese";

- "nel caso in esame, tuttavia, dato che la comunicazione e-mail in questione doveva essere inviata con urgenza, la scrivente Società (così come le altre consociate UE) si è avvalsa dei servizi del team di assistenza tecnica e supporto 24 ore su 24 forniti da Medtronic MiniMed, Inc. per inviare la comunicazione";

- "(…) non ha trattato dati personali di soggetti ubicati al di fuori del territorio italiano, né per proprio conto né per conto di altre consociate del Gruppo Medtronic nell'UE".

In relazione al presupposto giuridico in base al quale sono stati trattati i dati personali degli interessati e che avrebbe consentito l'invio della email a questi ultimi, la Società ha chiarito che "è stato richiesto il consenso esplicito degli utenti per il trattamento dei loro dati personali per la fornitura dei servizi, compreso l'invio di comunicazioni correlate di natura operativa, conformemente all'art. 6, par. 1, lett. a), e all'art. 9, par. 2, lett. a), del Regolamento" e che "laddove l'Informativa si riferisce all'impiego del consenso per altre finalità, viene richiesto un consenso esplicito separato e specifico per tali finalità, come il miglioramento e lo sviluppo di prodotti e servizi e il miglioramento generale della gestione della terapia e lo sviluppo di pubblicazioni e materiali di marketing".

Per quanto riguarda il trasferimento dei dati infragruppo la Società ha evidenziato che "per lo svolgimento delle attività di assistenza tecnica e di supporto è necessario che taluni dati personali vengano trasferiti alla società statunitense Medtronic MiniMed" e che "in conformità alla normativa vigente, sono state recentemente stipulate le nuove Clausole Contrattuali Standard basate sulla Decisione di Esecuzione (UE) 2021 /914 della Commissione". In ogni caso "il team di assistenza tecnica e supporto 24 ore su 24 di Medtronic, che ha effettivamente inviato le comunicazioni in questione, si trova in Canada, riconosciuto dalla Commissione Europea come un paese che assicura un livello adeguato di protezione dei dati (secondo la decisione della Commissione del 20 dicembre 2001)". Il personale canadese del team di assistenza tecnica e supporto 24 ore su 24 di Medtronic ha ricevuto una formazione specifica sulla procedura a gennaio 2021, ovvero prima della violazione notificata.

Al fine di evitare il ripetersi di eventi simili, la Società ha dichiarato di aver svolto un'attività formativa nei confronti del "personale interessato al fine di sottolineare l'importanza di seguire i

processi aziendali standard per l'invio delle notifiche agli utenti e ribadire la necessità di includere i destinatari nel campo "CCN"" e di aver "implementato un processo di peer-review in modo tale che tutte le notifiche inviate agli utenti dell'app Minimed TM Mobile siano ricontrollate da un secondo dipendente incaricato, per assicurare che i destinatari siano stati inclusi solo nel campo "CCN", allegando la documentazione che attesta l'attuazione di questo nuovo processo e che "è in fase di implementazione una nuova soluzione per l'invio di notifiche agli utenti, in modo da ridurre i passaggi manuali coinvolti nel processo, che di solito vengono eseguiti dal personale. Ciò comporta l'automazione del processo per includere i destinatari nel campo "CCN", riducendo il rischio di una divulgazione non autorizzata di dati personali causata da errori umani, quando si inviano notifiche agli utenti dell'app Minimed™ Mobile".

Con successiva nota del XX, la Società ha fornito riscontro all'ulteriore richiesta di informazioni dell'Autorità (nota del XX, prot. n. XX) avente ad oggetto in particolare, i profili di protezione dei dati personali effettuati dalle figure del "Medico" e del "Centro medico" citati nell'informativa sul trattamento dei dati personali acquisita agli atti del procedimento. In particolare, con riferimento al sistema CareLink™ Personal, oggetto del presente procedimento la Società ha chiarito che:

> si tratta di un dispositivo medico "costituito da un'applicazione gratuita basata sul web destinata direttamente alle persone affette da diabete che utilizzano dispositivi medici Medtronic compatibili ("Utenti del dispositivo") e alle persone che li assistono ("Care Partner"- un Care Partner è qualsiasi persona che fornisce assistenza (familiare, amico, ecc.) che ha ricevuto l'autorizzazione da un individuo con diabete per visualizzare le sue informazioni sul diabete su un accesso secondario sul di CareLink™ Personal)(congiuntamente, "Utenti di CareLink™ Personal")";
>
> "gli Utenti di CareLink™ Personal possono registrarsi in modo indipendente creando il proprio account CareLink™ Personal e accedendo ai dati dell'Utente del Dispositivo caricati in CareLink™ Personal (tramite un uploader cui si accede dalla piattaforma web o, per dispositivo compatibile, tramite l'app MiniMed™ Mobile) per aiutarli a gestire la malattia";
>
> "nel 2020, durante la pandemia di Covid-19, (…) è stata attivata in Italia la funzionalità aggiuntiva e opzionale disponibile tramite CareLink™ Personal denominata "Health Partner Share" ("HPS"). La funzione HPS permette agli Utenti del dispositivo, che lo consentono in modo espresso e specifico, di condividere solo con il proprio Professionista Sanitario i dati del dispositivo caricati nel proprio account CareLink™ Personal";
>
> "la condivisione dei dati è possibile solo se il Professionista Sanitario ha creato un account individuale tramite CareLink™ Personal";
>
> "la funzione HPS è completamente facoltativa poiché gli Utenti del dispositivo possono sfruttare appieno l'account CareLink™ Personal per supportare la propria gestione del diabete indipendentemente dal collegamento con l'account HPS del proprio Professionista Sanitario. Si prega inoltre di notare che Medtronic sta valutando se rimuovere la funzionalità HPS";
>
> "il "CareLink™ system" e il CareLink™Personal (…) sono due sistemi diversi e separati che possono comunicare tra loro solo (i) a discrezione del Professionista Sanitario e subordinatamente alla richiesta del Professionista Sanitario di collegare l'account del "CareLink™ system" all'account CareLink™ Personal del suo paziente e (ii) se il paziente acconsente espressamente al collegamento".

In relazione alle attività di trattamento dei dati personali e ai ruoli assunti, la Società ha chiarito di essere titolare del trattamento dei dati correlati alla creazione dell'account degli utenti CareLink™ Personal e "alla generazione dei report dei dati caricati dai dispositivi medici al fine di supportare

le persone affette da diabete a comprendere meglio la gestione della patologia". Qualora l'utente attivi la funzionalità HPS sopra descritta "i dati personali dell'Utente del dispositivo sono trattati da Medtronic e dal Professionista Sanitario per le rispettive finalità (Medtronic: con la finalità di fornire i servizi richiesti agli Utenti di CareLink™ Personal; quanto al Professionista Sanitario: con la finalità di fornire supporto e supervisione ai pazienti nella gestione della cura del diabete). Medtronic e il Professionista Sanitario agiscono in qualità di titolari autonomi del trattamento".

Secondo quanto riferito dalla Società, la funzionalità HPS comprende le seguenti attività di trattamento dei dati personali:

> "a) Creazione dell'account del Professionista Sanitario in CareLink™ Personal:• Medtronic è il titolare e il Professionista Sanitario è un interessato.
>
> b) Collegamento dell'account HPS del Professionista Sanitario all'account dell'Utente del dispositivo: • Medtronic e il Professionista Sanitario sono titolari autonomi in relazione al trattamento dei dati personali dell'Utente del dispositivo. Infatti, il Professionista Sanitario tratterà solo il nome utente CareLink ™ Personal utilizzato dai propri pazienti per collegare gli account (…): quel nome utente è fornito dall'Utente del dispositivo direttamente al suo Professionista Sanitario nel contesto delle attività di trattamento dati compiute dal Professionista Sanitario per il trattamento medico.
>
> c) Visualizzazione (e qualsiasi ulteriore utilizzo determinato dal Professionista Sanitario) dei dati personali caricati in CareLink™ Personal e condivisi dall'Utente del dispositivo con il Professionista Sanitario per scopi di trattamento medico: • il Professionista Sanitario è l'unico titolare".

In relazione alle basi giuridiche del trattamento, la Società ha chiarito che, per la creazione dell'account CareLink™ Personal e per la generazione dei report, essa va individuata nel consenso degli interessati, ai sensi degli artt. 6, par. 1, lett. a) e 9, par. 2 lett. a) del Regolamento.

Con riferimento, al collegamento dell'account HPS del Professionista Sanitario all'account dell'utente del dispositivo, la Società ha dichiarato che "è richiesto il consenso espresso dell'Utente del Dispositivo. Un meccanismo di consenso è integrato nel software CareLink™ Personal per consentire all'Utente del dispositivo di scegliere se permettere a Medtronic di abilitare il collegamento con il Professionista Sanitario tramite la funzionalità HPS, in modo che i dati del dispositivo dell'Utente del dispositivo siano visualizzabili nell'account HPS del Professionista Sanitario. Gli Utenti del dispositivo sono liberi di revocare il proprio consenso in qualsiasi momento scollegando il proprio account CareLink™ Personal dall'account HPS del Professionista Sanitario attraverso le impostazioni del loro account CareLink™ Personal. Una tale scelta interrompe qualsiasi condivisione dei dati del dispositivo con l'account HPS del Professionista Sanitario".

La Società ha, inoltre, precisato che per attivare il collegamento dell'account HPS del professionista sanitario con quello dell'utente (CareLink™ Personal) e rendere quindi accessibili i propri dati al professionista sanitario è necessario il consenso espresso del paziente che "è un requisito integrato nel software CareLink™ Personal". In tal caso, "il Professionista Sanitario è un titolare del trattamento autonomo per l'ulteriore trattamento dei dati su CareLink™ Personal a fini di cura medica. In quanto tale, il Professionista Sanitario è responsabile del rispetto degli obblighi di trasparenza applicabili nei confronti dei propri pazienti, con i quali il Professionista Sanitario ha una relazione medico/paziente preesistente finalizzata alla fornitura di servizi di assistenza medica". Sarebbero dunque gli utenti a scegliere se consentire il collegamento del proprio account e dunque condividere i dati con i professionisti sanitari.

La Società ha, infine, descritto i processi di registrazione dell'account Care Link™ Personal e del

Professionista sanitario che intende avvalersi della funzionalità HPS e il processo di associazione dell'account del medico con quello del proprio paziente. A tale riguardo è stato precisato che tale collegamento può avvenire attraverso due modalità, durante la visita del paziente presso l'ambulatorio del professionista sanitario ovvero "tramite un invito generato tramite CareLink™ Personal".

Nel primo caso "il Professionista Sanitario, che in precedenza ha creato il suo account in CareLink™ Personal, accede al suo account (…) inserisce il nome e la data di nascita del suo paziente per creare il profilo del paziente nell'account del Professionista Sanitario (…) seleziona "Effettuare il collegamento adesso utilizzando il nome utente e la password del paziente (il paziente è presente e immette le proprie credenziali per collegare gli account)". A questo punto "il Professionista Sanitario viene reindirizzato a una pagina destinata ai propri pazienti (…) leggerà il testo che appare in quella pagina al proprio paziente, prima di chiedere al paziente di inserire le proprie credenziali CareLink™ Personal in questa stessa pagina. Inserendo le proprie credenziali CareLink™ Personal, il paziente fornisce il consenso espresso all'attivazione del collegamento; una volta inserite correttamente le credenziali, l'account CareLink™ Personal del paziente e l'account HPS del Professionista Sanitario sono collegati e i dati del dispositivo del paziente possono essere condivisi con il Professionista Sanitario".

Nel caso di collegamento da remoto "(…) il paziente deve fornire il proprio nome utente CareLink™ Personal al Professionista Sanitario" che "crea un account e il profilo di un paziente nel suo account HPS; o il Professionista Sanitario seleziona "Inviare una richiesta di collegamento utilizzando il nome utente del paziente (il paziente confermerà la richiesta dal proprio account CareLink™ Personal)"; o il Professionista Sanitario riceve un testo, che deve leggere prima di inserire il nome utente CareLink™ Personal del paziente in CareLink™ Personal e fare clic su "Collega"; o il paziente riceverà quindi un'e-mail all'indirizzo e-mail associato al suo nome utente CareLink™Personal, nonché una notifica sul suo account CareLink™ Personal; il paziente deve accedere al proprio account CareLink™ Personal (un collegamento alla pagina web CareLink™ Personal è contenuto nell'e-mail) per accedere alla richiesta di collegamento inviata dal Professionista Sanitario; o per completare il collegamento, il paziente deve leggere il testo prima di accettare la richiesta di collegamento; o una volta fornita l'accettazione, i dati del dispositivo caricati nel CareLink™ Personal del paziente possono essere visualizzati dal Professionista Sanitario".

In entrambi i casi, il collegamento tra i due account è possibile solo (1) a seguito di una specifica valutazione sul punto tra il Professionista Sanitario e il paziente, e (2) dopo che il paziente ha fornito con un comportamento attivo le informazioni pertinenti per consentire alla Società di abilitare il collegamento.

In relazione a tali aspetti, l'informativa privacy acquisita agli atti del procedimento specifica che: "Qualora scegliesse di condividere i dati personali con gli operatori sanitari nell'ambito del trattamento medico o con altre parti esterne a Medtronic, essi saranno gli unici responsabili per l'uso, o ulteriore trattamento, dei dati personali" (pag. 2 "Informativa sulla privacy", All. A alla nota del XX).

Sulla base di quanto rappresentato dal titolare del trattamento nell'atto di notifica di violazione e nelle note con le quali ha fornito riscontro alle richieste di informazioni, nonché delle successive valutazioni svolte, 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, dalla legge n. 689 del 24/11/1981).

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 di circa 732 soggetti italiani ad altrettanti soggetti, 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 e in assenza di adeguate misure di sicurezza, in violazione dell'art. 32 del Regolamento; con riguardo al trattamento dei dati personali effettuato dalla Società in occasione del processo di registrazione dell'account Care Link™ Personal e di quello del Professionista sanitario che intende avvalersi della funzionalità HPS nonché del processo di associazione dell'account del medico a quello del proprio paziente, la Società ha omesso di fornire ai pazienti l'elemento informativo relativo alla base giuridica in virtù della quale viene effettuata la richiamata comunicazione di dati personali, che costituisce una nuova operazione di trattamento di dati personali, ivi inclusi quelli sulla salute da parte dei professionisti sanitari, in qualità di titolari autonomi del trattamento; ciò in violazione dei citati principi di correttezza e trasparenza di cui agli artt. 5, par. 1 lett. a), e degli artt. 12 e 13 del Regolamento, nonché degli artt. 7 e 9 del Regolamento, in quanto la predetta omissione avrebbe inficiato la validità stessa del consenso eventualmente prestato dal paziente.

3. Memorie difensive

Con nota del XX (prot. n.XX), la Società, ha fatto pervenire le proprie memorie difensive, ai sensi dell'art. 166, comma 6, del Codice senza chiedere di essere audita, fornendo altresì gli elementi di cui all'art. 83, par. 2, del Regolamento, nelle quali, è stato in particolare rappresentato 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, ha dichiarato che:

- "il trattamento dei dati personali degli utilizzatori del software CareLink™ Personal è basato sul consenso esplicito degli stessi (…). Tutti gli utenti dell'app MiniMed™ Mobile hanno volontariamente scaricato l'app dopo essere stati compiutamente informati dei termini di utilizzo e delle caratteristiche del trattamento dei loro dati personali";

- "è ovvio come la rivelazione accidentale "in chiaro" degli indirizzi e-mail degli utenti ad altri utenti del servizio, avvenuta in data XX, è stata interamente dovuta ad un errore umano non intenzionale, commesso in violazione delle misure tecniche e organizzative predisposte da Medtronic per la protezione dei dati personali degli utenti. Bisogna, infatti, differenziare il profilo di responsabilità del soggetto, Medtronic, che ha diligentemente predisposto misure tecniche e organizzative ed ha tempestivamente riferito la loro violazione (…) all'Autorità, da quello di chi le ha violate, anche se per errore";

- "l'erronea comunicazione di cui si discute è avvenuta in circostanze straordinarie di urgenza (e non certo con finalità promozionali o per altre utilità di Medtronic) dovute alla necessità di avvertire quanto prima gli utenti che l'app MiniMed™ Mobile sarebbe stata oggetto di taluni interventi manutentivi non programmati sui sistemi. Non si deve dimenticare come i pazienti diabetici "vivano" di dati: la conoscenza dei propri livelli glicemici nelle 24 ore è per loro di importanza vitale e, dopo che un paziente ha acconsentito ad utilizzare l'app MiniMed™ Mobile, è doveroso informarlo di qualsiasi problema di connessione";

- "tale errore è (…) avvenuto in violazione di una specifica procedura che era stata adottata da Medtronic proprio al fine di prevenire che si verificassero situazioni come quella oggetto dell'odierno procedimento. Peraltro, tale procedura era stata oggetto di specifica attività di formazione in favore dei dipendenti e collaboratori. Infatti: Medtronic ha adottato una

specifica procedura (…) diretta a regolare la predisposizione e l'invio di comunicazioni agli utenti in caso di interventi di manutenzione non programmata, la quale prevede espressamente che gli indirizzi e-mail degli utenti destinatari della comunicazione debbano essere inseriti nel campo copia nascosta ("CCN") e non nel campo destinatari ("A") e che ciascuna comunicazione debba essere rivista da un responsabile della divisione di supporto tecnico prima di essere inviata; tale procedura è stata oggetto di diffusione e formazione indirizzata ai membri del team Medtronic Diabete incaricati dell'invio delle comunicazioni agli utenti (…); si sottolinea che tale formazione è avvenuta prima della violazione riscontrata; più in generale, Medtronic ha adottato una serie di misure tecniche e organizzative (…) volte, tra le altre cose, a gestire gli accessi da parte di tutto il personale autorizzato, prevenire accessi non autorizzati, adottare tutte le misure di sicurezza informatiche e fisiche sui sistemi, ecc.";

- "lo strumento dell'invio via e-mail di comunicazioni agli utenti è la soluzione tecnica più idonea per la gestione di comunicazioni agli utenti in caso di interventi urgenti e non programmati sui sistemi; in tali casi, infatti, Medtronic può trovarsi nella necessità di dover inviare avvisi agli utenti in tempi molto ristretti e lo strumento della comunicazione via e-mail è attivabile in tempi molto brevi; l'app MiniMed™ Mobile non prevede – allo stato attuale – funzionalità alternative per inviare comunicazioni agli utenti in situazioni di urgenza. Inoltre, l'app MiniMed™ Mobile costituisce parte del software CareLink™ Personal, un dispositivo medico munito di marcatura CE soggetto ad un processo di certificazione e non liberamente modificabile da Medtronic a propria discrezione, che prevede che le notifiche agli utenti debbano essere inviate esclusivamente tramite e-mail; e un errore umano quale quello verificatosi non era prevedibile, né altrimenti evitabile. Come riconosciuto dall'EDPB, nonostante l'adozione di misure tecniche e organizzative, "è molto difficile per i titolari del trattamento (...) adottare misure per evitare [violazioni di dati personali dovuti ad errore umano]";

- "se è innegabile (ed anzi è stato volontariamente riconosciuto da Medtronic) che di un data breach si sia trattato, non si deve dimenticare che tale data breach non è avvenuto nel vuoto di misure tecniche e organizzative, che anzi, fino a quel momento, si sono dimostrate adeguate";

- "successivamente all'evento verificatosi, Medtronic ha adottato una serie di azioni di rimedio, tra le quali: (i) l'immediato tentativo di richiamo di tutti i messaggi e-mail inviati; (ii) l'invio di un messaggio a tutti i destinatari, con il quale si è chiesto di eliminare il messaggio precedentemente ricevuto e di non procedere con trattamenti di alcun tipo rispetto ai dati erroneamente comunicati (…); (iii) il personale interessato è stato oggetto di nuova formazione mirata per evitare il ripetersi di eventi analoghi (…); (iv)è stato implementato un nuovo strumento automatizzato per adiuvare il processo di comunicazione agli utenti, che richiederà al personale di Medtronic Diabete di caricare gli indirizzi e-mail degli utenti su una piattaforma dedicata e che minimizzerà la possibilità di errori umani nell'invio di e-mail ai destinatari, che saranno sempre in copia nascosta";

- "le conseguenze concrete, ove esistenti, derivanti dall'errore nell'invio della comunicazione agli utenti, risultano essere particolarmente limitate. Infatti: solamente gli indirizzi e-mail degli utenti sono stati oggetto di comunicazione, mentre nessun altro dato personale, né dato sanitario specifico o relativo alla salute degli utenti è stato oggetto di comunicazione; solo in alcuni casi e solo indirettamente gli indirizzi e-mail potrebbero portare all'identificazione di uno specifico utente: in molti casi, infatti, l'indirizzo e-mail di un utente non riflette il nome e cognome del paziente; parimenti, molti indirizzi e-mail potrebbero appartenere a soggetti che non sono pazienti, ma semplicemente a soggetti che forniscono assistenza ai pazienti (i cui dati sanitari non sono stati rivelati); non è stata ricevuta da Medtronic alcuna segnalazione o richiesta di risarcimento dagli utenti interessati dalla erronea comunicazione a distanza di un

anno e mezzo”.

3.2 Le ulteriori contestazioni

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, in relazione alla funzionalità denominata Health Partner Share (“HPS”), implementata durante il periodo pandemico, che permette al paziente di collegare il proprio account CareLink™ Personal con quello del professionista sanitario che lo ha in cura, ha dichiarato che:

- “Medtronic ha fornito chiara informativa rispetto al trattamento oggetto della presente contestazione, che – è utile chiarirlo – consiste nella sola connessione tra gli account dell’utilizzatore e del suo professionista sanitario (e non si estende certamente anche all’ulteriore attività di trattamento svolta dal professionista sanitario, in qualità di titolare autonomo). Difatti (…), in primo luogo vi sono richiami alla connessione degli account, e alla correlativa condivisione dei dati del dispositivo con i professionisti sanitari, sia nell’informativa di settembre 2020 (cfr. pagina 3 dell’Allegato A alla nostra comunicazione del XX) che in quella successiva del 2022 (cfr. pagina 2 dell’Allegato A alla nostra comunicazione del XX), e in secondo luogo vi è la specifica ed analitica informativa che viene fornita all’utente nel momento in cui gli si chiede il consenso per effettuare il collegamento con l’account del medico curante”;

- “l’informativa resa al paziente in fase di collegamento del suo account CareLink™ Personal con l’account CareLink™ HPS del professionista sanitario soddisfa i requisiti minimi di contenuto affinché il consenso sia “informato”;

- “una specifica, esaustiva e adeguata informativa viene resa al paziente nel momento in cui il suo consenso è richiesto per collegare il suo account CareLink™ Personal con l’account HPS del professionista sanitario. Il processo di collegamento dell’account CareLink™ Personal del paziente con l’account HPS del professionista sanitario è stato descritto nella nota di Medtronic del XX, ma può essere utile ribadire il funzionamento di tale processo e descrivere in maniera più approfondita il contenuto del modulo di consenso che viene presentato al paziente al momento del collegamento. Come illustrato, il collegamento può essere stabilito in due modi: (a) durante la visita del paziente nello studio del suo professionista sanitario, oppure (b) da remoto, tramite un invito generato tramite CareLink™ Personal”;

- nel descrivere il processo di collegamento durante la visita del paziente nello studio del suo medico curante: “Il paziente (utilizzatore del CareLink™ Personal) si reca presso il suo medico curante presso lo studio di quest’ultimo. Il medico – che ha preventivamente creato il suo account in CareLink™ Personal – accede al proprio account. Il professionista sanitario inserisce il nome e la data di nascita del suo paziente per creare il profilo del paziente nell’account del professionista sanitario. Il professionista sanitario seleziona “Collegamento del profilo del paziente a CareLink™ Personal” e “Effettuare il collegamento adesso utilizzando il nome utente e la password del paziente”. Successivamente, il professionista sanitario viene reindirizzato ad una pagina destinata al suo paziente. In pratica, il professionista sanitario leggerà l’avviso che appare sulla pagina destinata al paziente, prima di chiedere al paziente di inserire le sue credenziali CareLink™ Personal sulla medesima pagina. Immettendo le proprie credenziali CareLink™ Personal e cliccando sul pulsante “Collega”, il paziente esprime il proprio consenso esplicito per l’attivazione del collegamento. L’avviso che compare sulla pagina destinata al paziente è il seguente”: “Collegamento del profilo del paziente a CareLink™ Personal del proprio professionista sanitario: Collegamento del proprio account CareLink™ Personal alla cartella del paziente nell’account del software CareLink™ del proprio professionista sanitario. Selezionando il pulsante “Collega” si

fornisce, in qualità di proprietario dell'account CareLink™ Personal, il proprio consenso esplicito ad autorizzare Medtronic ad effettuare il cllegamento del proprio account CareLink™ Personal all'account del software CareLink™ del proprio professionista sanitario, in modo che quest'ultimo possa visualizzare i dati dei dispositivi caricati in CareLink™ Personal. È possibile revocare il proprio consenso andando su CareLink™ Personal e rimuovendo il collegamento con il proprio professionista sanitario. Per maggiori informazioni sulle modalità di trattamento dei propri dati personali da parte di Medtronic, consultare la nostra informatica sulla privacy https://carelink.medtronic.eu/crs/pow/3.7/media/hsp_privacy_policy_it.pdf. Si prega di far riferimento al proprio professionista sanitario per conoscere le modalità di trattamento dei propri dati di CareLink™ Personal da parte del proprio professionista sanitario, comprese le modalità di trattamento dei propri dati sanitari. Immettere il nome utente e la password personali per il collegamento a CareLink™ Personal";

- "in conformità alle linee guida EDPB 05/2020 sul consenso, adottate il 4 maggio 2020, l'avviso di cui sopra, letto in combinazione con l'informativa ivi richiamata, contiene tutte le informazioni minime affinché il consenso del paziente sia "informato", ossia: l'identità di entrambi gli autonomi titolari del trattamento: Medtronic, da una parte, la quale viene identificata nell'ambito dell'informativa poc'anzi richiamata quale titolare del trattamento per la creazione dell'account CareLink™ Personal degli utenti; dall'altra parte, il professionista sanitario, identificato quale destinatario dei dati nell'ambito del medesimo avviso; la finalità delle operazioni di trattamento per le quali il consenso viene richiesto, cioè collegare l'account CareLink™ Personal del paziente con l'account HPS del professionista sanitario, in modo tale che il professionista sanitario possa vedere i dati del dispositivo caricati dal paziente sul CareLink™ Personal; le tipologie di dati raccolti e utilizzati, cioè i dati del dispositivo caricati sul CareLink™ Personal; e l'esistenza del diritto di revocare il consenso: l'avviso fa esplicito riferimento alla possibilità per il paziente di revocare il proprio consenso rimuovendo il collegamento tra i due account";

- nel descrivere il processo di collegamento da remoto (tramite invito) "il professionista sanitario e il paziente hanno discusso della possibilità di collegare l'account CareLink™ Personal del paziente con l'account HPS del professionista sanitario da remoto. Al fine di assicurare che l'account del professionista sanitario sia collegato al corretto account CareLink™ Personal del paziente (quando l'operazione viene effettuata da remoto), il paziente deve fornire al professionista sanitario il proprio nome utente CareLink™ Personal. Il professionista sanitario crea un proprio account e il profilo del paziente nel proprio account HPS. Il professionista sanitario seleziona "Collegamento del profilo del paziente a CareLink™ Personal" e "Inviare una richiesta di collegamento utilizzando il nome utente del paziente". Il professionista sanitario riceve un avviso che deve leggere prima di inserire il nome utente CareLink™ Personal del paziente e cliccare "Collega". L'avviso è il seguente: Collegamento del profilo del paziente a CareLink™ Personal: Collegamento del profilo del paziente nel proprio account all'account CareLink™ Personal del paziente. Immettendo il nome utente CareLink™ Personal del paziente e facendo clic sul pulsante "Collega", si invita il paziente a collegare l'account CareLink™ Personal di quest'ultimo a questo account del software CareLink™. Una volta completata la procedura di collegamento, sarà possibile visualizzare i dati dei dispositivi Medtronic del paziente collegati e che sono stati caricati nell'account CareLink™ Personal di quest'ultimo a questo account del software CareLink™. Una volta completata la procedura di collegamento, sarà possibile visualizzare i dati dei dispositivi Medtronic del paziente collegati e che sono stati caricati nell'account CareLink™ Personal di quest'ultimo. Lei, in qualità di professionista sanitario del paziente, dichiara di aver informato quest'ultimo della Sua richiesta di collegamento all'account CareLink™ Personal del pazinete e di aver utilizzato il nome utente del paziente a tale scopo. Non copiare o memorizzare il nome utente del paziente una volta stabilito il collegamento.

Immettendo il nome utente CareLink™ Personal del paziente e facendo clic sul pulsante “Collega”, si dichiara di 1. Essere un professionista sanitario abilitato; 2. Richiedere il collegamento del proprio account del software CareLink™ all’account CareLink™ Personal del paziente selezionato e di comprendere che il paziente deve fornire il proprio consenso a tale collegamento per attivare la condivisione dei dati tra gli account-Condizioni d’uso-Politica sulla privacy. Immettere il nome utente CareLink™ Personal del paziente”;

- “il paziente, successivamente, riceve una e-mail all’indirizzo associato al suo nome utente CareLink™ Personal e una notifica sul suo account CareLink™ Personal. L’e-mail inviata al paziente è la seguente: “Gentile …, il Suo professionista sanitario desidera collegare il suo account CareLink™ Personal al proprio account del software CareLink™. Una volta collegati i due account, il Suo professionista sanitario sarà in grado di visualizzare i dati raccolti dai Suoi dispositivi medici collegati e che sono stati caricati sul suo account CareLink™ Personal, anche in momenti diversi da quelli delle visite effettuate di persona con il Suo professionista sanitario. Il collegamento può consentire al Suo professionista sanitario di visualizzare un insieme più completo dei dati generati dai Suoi dispositivi medici e di fornirle assistenza a distanza. Il collegamento è volontario. Se desidera collegare il Suo account, acceda al Suo account CareLink™ Personal all’indirizzo https://carelink-stage2.mimimed.eu e risponda a questa richiesta nella pagina delle impostazioni. Cordiali saluti, il team Medtronic CareLink™”;

- “il paziente, quindi, accede al suo account CareLink™ Personal (un link alla pagina web CareLink™ Personal è contenuto nella e-mail ricevuta dal paziente) al fine di accedere alla richiesta di collegamento inviata dal professionista sanitario. Per completare il collegamento, il paziente deve leggere il seguente avviso prima di accettare la richiesta di collegamento: “Condivisione con i professionisti sanitari- Il Suo professionista sanitario ha richiesto di collegarsi al Suo account CareLink™ Personal. Una volta completata la procedura di collegamento, il Suo professionista sanitario sarà in grado di visualizzare i dati raccolti dai Suoi dispositivi medici collegati e che sono stati caricati sul Suo account CareLink™ Personal, anche in momenti diversi da quelli delle visite effettuate di persona con il Suo professionista sanitario. Il collegamento è volontario e Lei può, pertanto, scegliere di non collegare il proprio account. La decisione di non collegare il Suo account non influirà sulla possibilità di ottenere prodotti e servizi di Medtronic Diabete, né sulla possibilità di ottenere cure, vantaggi o pagamenti. E’ possibile scollegare l’account in qualsiasi momento accedendo al Suo account CareLink™ Personal e selezionando “Interrompi condivisione” con il professionista sanitario indicato. In tal modo, Lei interromperà qualsiasi ulteriore condivisione dei Suoi dati CareLink™ Personal con l’account del software CareLink™ del professionista sanitario in questione; ciò, tuttavia, non comporterà la rimozione dei dati da Lei già condivisi. Facendo clic su “Approva”, Lei autorizza Medtronic a collegare il Suo account CareLink™ Personal all’account del software CareLink™ del Suo professionista sanitario. Per maggiori informazioni sulle modalità di trattamento dei Suoi dati personali da parte di Medtronic, consultare la nostra Informativa sulla privacy”;

- anche in questo caso, l’avviso che precede, letto in combinazione con l’informativa ivi richiamata, contiene tutte le informazioni minime affinché il consenso del paziente sia “informato”: l’identità di entrambi gli autonomi titolari del trattamento: Medtronic, da una parte, la quale viene identificata nell’ambito dell’informativa poc’anzi richiamata e il professionista sanitario, che riceve i dati ed è identificato nell’ambito del medesimo avviso; occorre puntualizzare che l’utente vede chiaramente il nome del suo professionista sanitario prima di consentire il collegamento del suo account CareLink™ Personal all’account HPS del professionista sanitario; la finalità delle operazioni di trattamento per le quali il consenso viene richiesto: collegare l’account CareLink™ Personal del paziente con l’account HPS del professionista sanitario, in modo tale che il professionista sanitario possa vedere i dati del

dispositivo caricati sul CareLink™ Personal; le tipologie di dati raccolti e utilizzati: i dati del dispositivo caricati sul CareLink™ Personal; e l'esistenza del diritto di revocare il consenso: si fa esplicito riferimento alla possibilità per il paziente di interrompere il collegamento in qualsiasi momento, revocando il proprio consenso";

- "in entrambi i casi, indipendentemente da quale processo di collegamento viene seguito (presso lo studio del professionista sanitario o da remoto), la richiesta di consenso alla condivisione dei dati è sufficientemente esplicita da rendere il paziente-utente consapevole, in termini chiari e semplici, del fatto che la base giuridica di tale trattamento è costituita precisamente dal consenso";

- "il trattamento dei dati da parte di Medtronic si sostanzia ed è limitato solo ed esclusivamente al collegamento dell'account CareLink™ Personal del paziente all'account HPS del professionista sanitario e alla conseguente condivisione dei dati del dispositivo, previo consenso del paziente. Dopodiché, per effetto della condivisione, (…) il trattamento ulteriore dei dati è effettuato da un diverso titolare (il professionista sanitario), il quale avrà la piena ed esclusiva responsabilità di fornire le dovute informazioni al paziente in relazione al trattamento dei dati sanitari del paziente. In altre parole, le finalità del trattamento ad opera di Medtronic, legittimate da un esplicito consenso, sono solo quelle di permettere tale collegamento, e le stesse sono perfettamente esplicitate dalle informazioni che vengono rese al paziente al momento del collegamento (ove si legge che "una volta completata la procedura di collegamento, il Suo professionista sanitario sarà in grado di visualizzare i dati raccolti dai Suoi dispositivi medici collegati e che sono stati caricati sul Suo account CareLink™ Personal, anche in momenti diversi da quelli delle visite effettuate di persona con il Suo professionista sanitario."). Non può essere infatti richiesto a Medtronic, titolare di un trattamento del tutto autonomo, di informare il paziente in merito alle finalità sottese al trattamento dei dati ad opera del professionista sanitario (il quale agisce come autonomo titolare del trattamento);

- "il destinatario della condivisione di dati personali non è un professionista sanitario qualsiasi, bensì il professionista sanitario che già si sta occupando della terapia del paziente-utente e che dà inizio alla richiesta di avere il suo account HPS collegato all'account CareLink™ Personal del paziente. Orbene, tale professionista sanitario, oltre che essere, come già detto, esplicitamente individuato nell'ambito della schermata che precede il collegamento, è già assolutamente noto al paziente in quanto suo medico curante. L'utilizzo dell'app MiniMed™ Mobile, infatti, non è che l'ultima fase di un lungo processo di cura che inizia con la diagnosi del diabete e prosegue con la prescrizione di un microinfusore da parte del medico; inoltre, come in precedenza richiamato, la condivisione dei dati con il professionista sanitario avviene di solito in sua presenza o, in seguito ad una discussione con il professionista sanitario a tale riguardo, da remoto. È quindi lecito presumere che il professionista sanitario incaricato, per quanto concerne le attività di trattamento che gli spettano, abbia già reso idonea informativa al paziente al momento della prima instaurazione del rapporto di cura, o che comunque la intenda rendere in un momento successivo, in conformità ed entro i limiti espressamente previsti dall'art. 14 comma 3 del GDPR (che, per il caso di titolare che riceve i dati personali da soggetti diversi dall'interessato, prevede la possibilità di fornire l'informativa in un momento successivo)";

- "Medtronic, nel rendere l'informativa collegata alla richiesta di consenso per il trattamento che le compete, non può certo sostituirsi al professionista sanitario rispetto all'obbligo di fornire l'informativa legata al trattamento dei dati posto in essere da quest'ultimo nel corso dell'attività di cura. Ciò contrasterebbe con il principio di responsabilizzazione (art. 5 comma 2 del GDPR) e con il ruolo di autonomo titolare del trattamento ricoperto dal professionista sanitario, che non è mai stato posto in dubbio. Peraltro, i dettagli del trattamento dei dati effettuato dal professionista sanitario non sono nemmeno noti a Medtronic, in quanto

assoggettati a obbligo di segreto professionale";

- "occorre sottolineare che solamente i dati raccolti dal dispositivo dell'utente (es. misurazioni e parametri registrati dal dispositivo stesso) sono condivisi con il professionista sanitario dell'utente in seguito al collegamento dell'account CareLink™ Personal dell'utente con l'account HPS del professionista sanitario; nessun altro dato o informazioni, quali dati, appunti o informazioni caricati manualmente dall'utente nel suo account CareLink™ Personal, sono condivisi con il professionista sanitario";

- "il fatto che tra il professionista sanitario che richiede la condivisione ed il paziente-utente che vi acconsente esista già un rapporto professionale sottostante (che, ancora una volta, Medtronic presume sia stato instaurato in conformità con i dovuti obblighi informativi), e che il trattamento posto in essere da Medtronic non costituisca altro che uno strumento per facilitare ulteriormente tale preesistente rapporto di cura, esenterebbe addirittura Medtronic dal fornire qualsiasi tipo di informativa in relazione a tale attività, giusto quanto previsto dall'art. 13 comma 4 del GDPR. Le informazioni di cui (…) l' Autorità contesta l'assenza sono, in sostanza, già (o quantomeno dovrebbero essere già) in possesso dell'utente-paziente";

- "l'informativa fornita all'utente non è carente rispetto a (a) il "presupposto giuridico sui cui la comunicazione si basa", (b) "l'identità del titolare" e (c) "le finalità del trattamento" in quanto: senza il consenso del paziente, nessuna condivisione di dati è possibile. La funzionalità HPS realizza concretamente il principio di "empowerment" del paziente nella gestione della sua malattia e dei propri dati, assolutamente in linea con i principi a cui si ispira il GDPR, nonché la medicina contemporanea. La stessa funzionalità HPS è stata progettata sulla base di questo fondamentale principio: all'utente è illustrato in termini semplici e chiari che il suo consenso è necessario per la condivisione dei dati e può essere in qualsiasi momento revocato. L'attivazione della funzionalità HPS è condizionata al consenso dell'utente, che decide come e con chi condividere i propri dati; Peraltro, la base giuridica per la condivisione dei dati attraverso la funzionalità HPS è resa evidente all'utente-paziente; l'avviso che appare prima della condivisione dei dati chiarisce l'identità del nuovo titolare del trattamento nel caso in cui l'utente opti per la condivisione dei dati: si tratta, peraltro, di un soggetto già noto all'utente in quanto suo medico curante; quanto alle finalità del trattamento, Medtronic informa preventivamente l'utente che il consenso all'attivazione della funzionalità HPS consente il collegamento tra l'account CareLink™ Personal del paziente e l'account HPS del professionista sanitario. Medtronic non può fornire informazioni circa le "finalità del trattamento cui sono destinati i dati personali" in quanto afferiscono all'autonoma decisione di un diverso titolare del trattamento, cui competono gli obblighi informativi del caso (Medtronic non cura pazienti, ma commercializza dispositivi medici per la cura del diabete). Alla luce di quanto sopra, Medtronic ritiene che il consenso del paziente sia informato e, quindi, valido".

Infine, la Società ha fornito una serie di elementi valutati utili, nell'ambito di quelli individuati dall'art. 83, par. 2 del Regolamento, sia in relazione alla contestazione della violazione di dati personali avente ad oggetto la sopra descritta comunicazione dei dati sulla salute attraverso l'invio di email in "copia conoscenza" a più destinatari, sia in relazione alla contestazione della violazione riguardante gli obblighi informativi e l'acquisizione del relativo consenso.

In particolare, in relazione al primo profilo, la Società ha evidenziato che:

- "la violazione oggetto di notifica da parte di Medtronic si caratterizza per un basso livello di gravità. Rilevano in tal senso i seguenti elementi:

  "(…) la violazione contestata, in sostanza, deriva da un singolo evento isolato,

riconducibile ad un evidente errore umano, che si è ripercosso su un numero limitato di soggetti (ovvero i 732 destinatari della comunicazione di manutenzione non programmata del server), e che non potrà ripetersi, anche in considerazione dell'implementazione di una procedura automatizzata per la comunicazione urgenti relative ad interruzioni – manutenzioni;

(…) la violazione è avvenuta nel contesto di un trattamento che, oltre a esser stato espressamente acconsentito dagli interessati, ha la sola ed esclusiva finalità di informare e garantire la sicurezza del paziente, prevenendo eventuali malfunzionamenti del software CareLink™ Personal, che potrebbero ripercuotersi sulla sua salute o sulla sua terapia;

la violazione non ha prodotto alcun danno in capo agli interessati coinvolti, né di carattere fisico/materiale, né tantomeno di carattere immateriale o reputazionale. Ciò è ancor più evidente, se solo si pensa che nessuno dei soggetti interessati dalla violazione ha proposto alcun reclamo, né alcuna contestazione nei confronti di Medtronic, né tantomeno si è attivato al fine di richiedere alcun risarcimento del danno";

- "la contestata violazione è senza dubbio colposa e non dolosa, essendo la stessa connotata dall'assenza di volizione in relazione alla causazione del data breach. (…) la violazione è derivata da un errore umano non intenzionale, che è conseguito alla mancata applicazione, da parte di un membro del team di Medtronic Diabete, di regole e procedure adottate da Medtronic proprio al fine di prevenire eventi come quello oggetto della contestazione. Qualora tale dipendente si fosse attenuto alle procedure interne, la violazione non sarebbe avvenuta. (…). Orbene, anche ai sensi di quanto previsto dalle Linee Guida Sanzioni ("Linee-guida 01/2021 su esempi riguardanti la notifica di una violazione dei dati personali" adottate il 14 dicembre 2021 dal Comitato Europeo per la Protezione dei Dati), l'errore umano, la mancata lettura e il mancato rispetto delle procedure esistenti, nonché la loro mancata applicazione, sono tutti sintomi di negligenza del singolo operatore (non di Medtronic), che escludono la sussistenza di una qualsivoglia volontarietà";

- "del tutto innegabile che Medtronic, facendosi parte diligente, si sia debitamente attivata sin da subito al fine di attenuare, se non addirittura di sterilizzare, gli effetti dannosi derivanti dal data breach. Difatti, oltre ad esser stata in grado di identificare immediatamente la violazione commessa, Medtronic ha: provveduto a notificare tempestivamente la violazione all'Autorità; richiamato immediatamente le e-mail inviate; inviato, sempre tempestivamente, ai destinatari della comunicazione, un nuovo messaggio con l'invito a (i) eliminare qualsiasi copia dell'e-mail ricevuta, e (ii) non intraprendere ulteriori azioni con le informazioni ivi contenute; e provveduto ad assoggettare il personale interno a nuove sessioni di training";

- "Medtronic ha implementato un nuovo sistema automatizzato, che minimizza il rischio di errore per il futuro. Il nuovo sistema automatizzato, infatti, esclude che l'operatore debba scegliere tra un'elencazione degli indirizzi e-mail dei destinatari in chiaro o in copia nascosta, provvedendo automaticamente ad inviare una comunicazione via e-mail con i destinatari in copia nascosta";

- "da tali misure adottate si desume che Medtronic ha agito sin da subito con grande tempestività, responsabilità e trasparenza, facendo quanto in suo potere per correggere le proprie azioni ed anzi cercando in qualsiasi modo di eliminare eventuali effetti dannosi, "assumendosi la responsabilità di correggere o limitare l'impatto delle sue azioni" (cfr. Linee Guida Sanzioni, cap. III l. c) ultimo capoverso)";

- "al fine di prevenire eventi della specie di quello verificatosi, Medtronic aveva

precedentemente stilato una specifica procedura interna (…) atta a disciplinare nel dettaglio il procedimento che deve essere seguito dai propri dipendenti e collaboratori nei casi in cui, per ragioni di urgenza, si rende necessario procedere con una comunicazione agli utenti di interruzione non programmata del servizio. Tale procedura è stata, come provato per tabulas, debitamente diffusa, e tutti i dipendenti e collaboratori sono stati altresì assoggettati a specifici corsi di formazione";

- "è importante rammentare che gli artt. 25 e 32 del GDPR, nell'imporre l'adozione di misure tecniche e organizzative adeguate, stabiliscono un "obbligo di mezzi e non di risultato" (si veda, sul punto, Linee Guida Sanzioni, cap. III, l. d) terzo capoverso), con la conseguenza che non è sufficiente il prodursi di una violazione per ritenere inidoneo il sistema di misure organizzative, dovendosi invece analizzare l'adeguatezza astratta di tali misure a garantire un livello di sicurezza adeguato al rischio: adeguatezza che, vista la specificità delle procedure interne, la formazione su di esse e il fatto che l'errore umano si è verificato in una sola occasione, non può di certo ritenersi insussistente";

- "Medtronic si è sin da subito resa interamente disponibile all'Autorità al fine di porre rimedio alla violazione, fornendo tempestivamente, in maniera esaustiva e trasparente, tutte le informazioni che sono state richieste (…)";

- "è discutibile che la violazione abbia riguardato dati relativi alla salute ai sensi di quanto previsto dall'art. 9 del GDPR, poiché oggetto di data breach sono stati solamente gli indirizzi e-mail dei destinatari della comunicazione resi visibili agli altri destinatari, i quali non sempre permettono di identificare il soggetto titolare (non tutti gli indirizzi, difatti, corrispondono a nome.cognome@), né tantomeno permettono di associare automaticamente i destinatari della comunicazione (ove identificabili) a pazienti affetti da diabete, atteso che gli indirizzi mail ben possono riferirsi a soggetti diversi dal paziente, quali care-givers o genitori, in caso di utenti minori di età. Nessun dato direttamente connesso con la salute (quali, informazioni sulla glicemia degli utenti, sulle terapie cliniche o sull'utilizzo dei dispositivi collegati a CareLink™ Personal) è stato diffuso o comunicato a terzi";

- "la violazione è stata notificata da Medtronic in maniera spontanea ed entro i termini previsti dall'art. 33 del GDPR. È stata quindi la stessa scrivente a mettere l'Autorità al corrente del data breach e, sebbene la presentazione della relativa notificazione in caso di data breach costituisca oggetto di un autonomo obbligo giuridico in capo al titolare ai sensi di quanto previsto dal GDPR, denota sicuramente la piena intenzione da parte di Medtronic di mettersi a disposizione di codesta Autorità al fine di collaborare nella gestione delle conseguenze della violazione";

- "devono assumere autonomo valore attenuante: l'adozione, da parte di Medtronic, di un codice etico e di un modello organizzativo ai sensi del D. Lgs. 231/2001 che mirano anche a prevenire condotte illecite in relazione ai dati personali, nonché la continua formazione su entrambi; il particolare valore sociale delle finalità connesse al trattamento, e la correlativa assenza di qualsivoglia vantaggio in favore di Medtronic quale conseguenza dell'asserita violazione. Quello in oggetto, a ben vedere, è infatti un trattamento necessario al solo ed esclusivo fine di garantire il più alto grado di sicurezza in relazione all'utilizzo di CareLink™ Personal (…), salvaguardando la salute dei pazienti. Il tutto, ad esclusivo ed indubbio vantaggio del solo interessato, atteso che Medtronic non ottiene alcun vantaggio economico dal presente trattamento di dati; si precisa che CareLink™ Personal viene offerto gratuitamente agli utenti che siano già utilizzatori di un dispositivo Medtronic;la stessa violazione è già stata notificata dalle rispettive consociate di Medtronic alle Autorità Garanti dei rispettivi paesi di appartenenza (Belgio, Repubblica Ceca, Finlandia, Germania, Paesi Bassi, Norvegia, Spagna, Svezia, Francia, Regno Unito), e le stesse Autorità hanno concluso l'indagine archiviando la segnalazione".

In relazione al secondo profilo, relativo alla contestazione della violazione riguardante gli obblighi informativi e l'acquisizione del relativo consenso, la Società ha evidenziato che:

- "la finalità del trattamento (…) si sostanzia nella possibilità di creare un collegamento tra l'account del paziente e quello del suo professionista sanitario, rinvenibile al link: https://www.medtronic.com/content/dam/medtronic-com/it-it/corporate/documents/Codice-Condotta-Compass-Bussola-12-2020.pdf consentendo all'utente/paziente soggetto a determinate terapie (o al suo care-giver) di condividere in maniera semplice, rapida e diretta i dati relativi alla propria malattia con il professionista sanitario che ha già in carico la gestione della relativa terapia, così consentendogli di accedere ai dati sulla glicemia del proprio paziente. Ancora una volta, l'unica finalità connessa al trattamento in oggetto è quella di facilitare il percorso terapeutico e di accrescere il controllo dei medici sulle terapie dagli stessi assegnate ai propri pazienti. Il tutto, chiaramente, previo consenso da parte del relativo paziente. Medtronic non comunica alcun dato a professionisti sanitari che non siano già i medici curanti degli utenti;

- i dati del paziente riguarderebbero il solo paziente interessato, e verrebbero comunicati solo al suo professionista sanitario (il quale peraltro, avendo già in cura il paziente, è verosimile che già possieda – o che possa comunque ottenere aliunde – i dati oggetto della comunicazione);

- l'asserita violazione non ha prodotto alcun danno in capo agli interessati coinvolti, né di carattere fisico/materiale, né tantomeno di carattere immateriale o reputazionale (anzi, comporta un indubbio vantaggio clinico). Ciò è ancor più evidente se solo si pensa che nessuno dei pazienti utilizzatori di CareLink™ Personal ha proposto alcun reclamo, né alcuna contestazione diretta nei confronti di Medtronic in relazione alla funzionalità HPS, né tantomeno si è attivato al fine di richiedere un eventuale risarcimento del danno. Anzi, il trattamento in oggetto ha permesso di ottimizzare i percorsi terapeutici connessi alla cura di malattie particolarmente inabilitanti, quali il diabete, ottenendo il favore (ed il consenso) dei relativi utilizzatori;

- "(…), Medtronic regolarmente rivede e aggiorna le proprie comunicazioni e informative privacy. Benché Medtronic ritenga che il consenso dei pazienti per la condivisione dei dati con i propri professionisti sanitari tramite la funzionalità HPS sia sufficientemente informato e valido, Medtronic ha provveduto all'aggiornamento della propria informativa privacy (versione di luglio 2022) per accrescere ulteriormente il livello di trasparenza reso agli utilizzatori del CareLink™ Personal e soddisfare qualsiasi quesito a riguardo. Come aggiornata, l'informativa privacy fa esplicito riferimento alla base giuridica (cioè il consenso esplicito) per il predetto trattamento dei dati. La versione aggiornata dell'informativa privacy (…) nell'ambito del paragrafo denominato "Consenso (Esplicito)": riporta quanto segue "Trattamento dei dati sanitari- Con il consenso esplicito dell'utente elaboreremo i dati sanitari per le finalità specifiche riportate di seguito: - Creare l'account CareLink™ Personal, al fine di caricare i dati dei dispositivi e generare i report di CareLink™ Personal; - aggregare i dati sanitari in modo da non identificare direttamente gli utenti. Utilizzeremo tali informazioni per generare report interni al fine di svolgere ulteriori ricerche e sviluppare nuovi prodotti e servizi per la gestione del diabete e migliorare prodotti e servizi esistenti e/o sviluppare materiali presentati ai medici e agli enti pubblici e in occasione di conferenze per mostrare le prestazioni dei prodotti e consentire a Medtronic di migliorare i programmi di istruzione, formazione e supporto; - ove applicabile, al fine di abilitare il collegamento del Suo account CareLink™ Personal all'account CareLink™ utilizzato dal Suo professionista sanitario nell'ambito del trattamento medico" (art. 83, par. 2 lett. a) del Regolamento);

- "carattere colposo dell'asserita violazione, la quale, stando alla lettera della contestazione, difetterebbe di sufficiente informativa. Tale asserita insufficienza, quand'anche ritenuta

sussistente, non potrebbe che sostanziarsi in una mera negligenza da parte di Medtronic" (art. 83, par. 2 lett. b) del Regolamento);

- "Medtronic ritiene che la formulazione del consenso al trattamento dei dati personali nell'ambito della funzionalità HPS sia sufficientemente chiaro e che il trattamento in questione sia del tutto legittimo e conforme agli artt. 5(1)(a), 7, 9, 12 e 13 del GDPR. Tuttavia, come menzionato nel paragrafo 3.2(a)(iv) di cui sopra, al fine di venire incontro ai rilievi dell'Autorità in relazione alle informazioni contenute nell'informativa privacy riguardanti la base giuridica del trattamento, Medtronic ha ulteriormente aggiornato la propria informativa privacy al fine di garantire una sempre maggiore trasparenza" (art. 83, par. 2 lett. c) del Regolamento);

- "Medtronic si è da sempre conformata agli obblighi sulla stessa gravanti ai sensi degli artt. 25 e 32 del GDPR. E così, nella fase di ottenimento del consenso da parte dell'utente/paziente per la condivisione dei dati con i professionisti sanitari, i principi di privacy by default e privacy by design (art. 25 del GDPR) devono ritenersi rispettati, in quanto la prestazione del consenso non è una opzione preselezionata, e la condivisione dei dati non potrebbe avvenire in assenza del previo consenso dell'interessato" (art. 83, par. 2 lett. d) del Regolamento);

- "Medtronic non ha in passato commesso e/o notificato alcuna violazione della specie oggetto dell'odierno procedimento. Ciò, oltre che avere autonomo valore attenuante, costituisce un ulteriore elemento di evidenza dell'adeguatezza dell'assetto organizzativo di Medtronic rispetto alla protezione dei dati personali di cui è titolare" (art. 83, par. 2 lett. e) del Regolamento);

- "anche in relazione alla sussistenza del presente elemento ed alla sua rilevanza attenuante, Medtronic si è sin da subito messa a piena disposizione dell'Autorità al fine di comprendere e porre rimedio alla violazione, fornendo tempestivamente, in maniera esaustiva e trasparente, tutte le informazioni che le sono state richieste, e proponendosi sin da subito di porre in essere misure di rimedio" (art. 83, par. 2 lett. f) del Regolamento);

- "il trattamento oggetto di contestazione riguarda dati riconducibili al genus "dati di salute" (ossia i dati connessi all'utilizzo dei dispositivi medici associati a CareLink™ Personal). Tuttavia, si ricorda che solamente i dati raccolti dal dispositivo dell'utente (es. misurazioni e parametri registrati dal dispositivo stesso) sono condivisi con il professionista sanitario dell'utente in seguito al collegamento dell'account CareLink™ Personal dell'utente con l'account HPS del professionista sanitario; nessun altro dato o informazione, quali dati, appunti o informazioni caricati manualmente dall'utente nel suo account CareLink™ Personal, sono condivisi con il professionista sanitario" (art. 83, par. 2 lett. g) del Regolamento);

- "(…) i dettagli specifici relativi alla funzionalità della funzionalità di collegamento del CareLink™ Personal del paziente con quello del professionista sanitario (in cui si annida, a parere di codesta Autorità, la violazione) sono stati comunicati da Medtronic in maniera trasparente, esaustiva e tempestiva" (art. 83, par. 2 lett. h) del Regolamento).

La Società, pertanto, nel ritenere non sussistenti le violazioni contestate, ha chiesto, in caso di diverso avviso dell'Autorità, di considerare tali violazioni come "minori" "nel senso di cui al considerando 148 del GDPR" e di ritenere "che la misura correttiva che meglio si attaglia al caso di specie, se mai ce ne fosse una, sia quella dell'ammonimento".

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 osserva 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, par. 1, nn. 1 e 15 del Regolamento);

il Considerando n. 35 del Regolamento precisa che i dati relativi alla salute "comprendono informazioni sulla persona fisica raccolte nel corso della sua registrazione al fine di ricevere servizi di assistenza sanitaria"; "un numero, un simbolo o un elemento specifico attribuito a una persona fisica per identificarla in modo univoco a fini sanitari";

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);

il titolare del trattamento deve mettere in atto misure tecniche e organizzative adeguate a garantire un livello di sicurezza adeguato al rischio, tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche (art. 32 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);

Tanto premesso, alla luce della definizione di dato personale sopra richiamata, gli indirizzi email sono riconducibili a tale nozione (cfr. sulla riconducibilità dell'indirizzo email alla nozione di dato personale, provv. 25 giugno 2002, doc. web n. 29864).

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 dell'app MiniMed Mobile situati in Italia, che collega - tramite Bluetooth - la pompa per insulina MiniMed™ allo smartphone dell'utente, 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 la pompa per l'insulina MiniMed™ che invia i dati alla predetta applicazione per smartphone (cfr. sul punto numerosi provvedimenti dell'Autorità, tra i quali: provv. 9 gennaio 2020, n. 1, doc. web n. 9261234; provv. 16 settembre 2021, n. 328, doc. web n. 9722297, provv. 13 maggio 2021, n. 206, doc. web n. 9688020; provv. 28 aprile 2022, n. 164, doc. web n. 9779057, provv. 7 luglio 2022, n. 242, doc. web 9809998, provv. 11 gennaio 2023, n. 7, doc. web n. 9861356).

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 forniti dai pazienti. Si evidenzia inoltre che la stessa Società 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) e agli obblighi in materia di sicurezza di cui all'art. 32 del Regolamento, nel caso di specie, le misure tecniche ed organizzative adottate dalla Società, non sono risultate idonee a garantire un livello di sicurezza adeguato al rischio vista la violazione di dati personali oggetto di notificazione da parte del titolare del trattamento e considerato il rilevante numero di indirizzi email (e quindi di destinatari) contenuti in una singola notifica (cfr. par. 6.2 delle Linee guida 01/2021 "su esempi riguardanti la notifica di una violazione dei dati personali", adottate il 14 gennaio 2021; provv. del 13 maggio 2021, doc. web 9688020; provv. del 16 settembre 2021, doc. web 9722297 e provv. del 7 luglio 2022, cit.). Del resto la stessa Società, nel corso dell'istruttoria, ha previsto l'adozione di ulteriori misure organizzative proprio al fine di evitare il ripetersi di eventi analoghi a quello occorso.

Pertanto, l'invio di comunicazioni mediante notifiche email a un numero plurimo di destinatari (di cui 732 in Italia), che 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 interessati configurandosi, pertanto, un trattamento di dati sulla salute in violazione degli artt. 5, par. 1 lett. a) e f), 9 e 32 del Regolamento.

4.2. Le ulteriori violazioni

In relazione alla condivisione dei dati clinici del paziente con il professionista sanitario attraverso la funzionalità "Health Partner Share", che permette al paziente di collegare il proprio account CareLink™ Personal con quello del professionista sanitario che lo ha in cura, e alla contestazione avente ad oggetto la violazione degli obblighi informativi e l'acquisizione del relativo consenso al trattamento dei dati personali effettuato dalla Società in occasione del predetto collegamento, si osserva che:

i dati personali devono essere trattati nel rispetto dei principi applicabili al trattamento, e di "responsabilizzazione", in base al quale il titolare del trattamento deve essere in grado di comprovare il rispetto dei citati principi, con un ragionamento logico, prove concrete e comportamenti proattivi (art. 5, par. 1 e 2 e art. 24 del Regolamento);

in tale ambito rileva, in particolare, il citato principio di liceità in base al quale ogni trattamento di dati personali deve fondarsi su uno specifico presupposto giuridico (art. 5, par. 1, lett. a) del Regolamento);

nel caso in cui la condizione di liceità sia rappresentata dal consenso, esso deve essere libero, specifico, informato e inequivocabile relativamente al trattamento dei dati personali che riguardano l'interessato (Considerando nn. 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);

il consenso, per essere liberamente prestato, deve essere informato; perché sia tale "l'interessato dovrebbe essere posto a conoscenza almeno dell'identità del titolare del trattamento e delle finalità del trattamento cui sono destinati i dati personali" (art. 7 del Regolamento e Considerando n. 42; cfr., altresì, i par. 3.3.1 e 3.3.2 e in particolare il punto 64 delle Linee guida 5/2020 sul consenso ai sensi del Regolamento (UE) 2016/679, versione 1.1 adottate il 4 maggio 2020 secondo le quali "per ottenere un consenso valido siano necessarie almeno le seguenti informazioni [da fornire all'interessato]: i. l'identità del titolare

del trattamento; ii. la finalità di ciascuno dei trattamenti per i quali è richiesto il consenso; iii. quali (tipi di) dati saranno raccolti e utilizzati; iv. l'esistenza del diritto di revocare il consenso (…)";

i dati personali devono essere inoltre trattati nel rispetto del principio di trasparenza (art. 5, par. 1 lett. a) del Regolamento) 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 (Considerando nn. 39, 58 e art. 12 del Regolamento);

secondo le Linee guida sulla trasparenza ai sensi del Regolamento 2016/679, adottate il 29 novembre 2017 nella versione emendata adottata l'11 aprile 2018, "l'elemento della "facile accessibilità" implica che l'interessato non sia costretto a cercare le informazioni, ma che anzi gli sia immediatamente chiaro dove e come queste siano accessibili, ad esempio perché gli sono fornite direttamente, un link lo dirige verso di esse o le informazioni sono contrassegnate chiaramente oppure perché le informazioni si configurano come risposta a una domanda in linguaggio naturale (ad esempio in una dichiarazione/informativa sulla privacy stratificata online, in FAQ, mediante pop-up contestuali che si attivano quando l'interessato compila un modulo online oppure, in un contesto digitale interattivo, attraverso un'interfaccia chatbot, ecc.)" (par. 11 e anche par. 33-40);

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 (cfr. Parere 02/2013 (WP202), sulle applicazioni per dispositivi intelligenti adottato il 27 febbraio 2013 dal Gruppo di lavoro "Art. 29");

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

Tanto premesso, dalla documentazione in atti, emerge che l'"informativa sulla privacy", anche nella versione di luglio 2022, seppure modificata rispetto alla precedente versione del 24 settembre 2020, non reca chiare informazioni, in particolare, sul trattamento dei dati personali effettuato in occasione del processo di collegamento degli account CareLink™ Personal del paziente e del professionista sanitario, qualora il primo intenda avvalersi della funzione HPS.

Ciò, tenuto conto che, in relazione al trattamento in esame come sopra descritto, tale collegamento -realizzato attraverso le funzionalità tecniche messe a disposizione dalla Società- comporta una comunicazione di dati personali tra diversi titolari, rispetto alla quale va indicato, nella richiamata informativa, il presupposto giuridico su cui essa si basa, comportando una nuova operazione di trattamento di dati personali, ivi inclusi quelli sulla salute, da parte dei professionisti sanitari, in qualità di titolari autonomi.

L'informativa infatti, nella versione di settembre 2020, non reca alcuna informazione al riguardo, mentre, nella versione di luglio 2022, essa si limita a rappresentare al paziente che "Qualora scegliesse di condividere i dati personali con gli operatori sanitari nell'ambito del trattamento medico o con altre parti esterne a Medtronic, essi saranno gli unici responsabili per l'uso, o ulteriore trattamento, dei dati personali".

A ciò si aggiunga che le predette informazioni non sono fornite neppure nel momento in cui il paziente è in procinto di effettuare il predetto collegamento. Infatti, nella schermata conclusiva del

collegamento dell'account il paziente viene solo informato della circostanza che, digitando il tasto "accetta", autorizza Medtronic ad effettuare il predetto collegamento; nella medesima schermata il paziente è informato che qualora fosse interessato a ricevere maggiori informazioni sul trattamento dei dati personali da parte di Medtronic può consultare l'informativa privacy accessibile direttamente dalla medesima pagina attraverso un link ipertestuale, carente delle indicazioni circa la base giuridica su cui si fonda tale operazione di trattamento.

Pertanto, sia nel documento contenente l'informativa predisposto a settembre 2020 che in quello aggiornato nel luglio 2022, la Società ha omesso di fornire l'elemento informativo relativo alla base giuridica in virtù della quale viene effettuata la richiamata comunicazione di dati personali; ciò, in violazione dei citati principi di correttezza e trasparenza di cui agli artt. 5, par. 1 lett. a), nonché degli artt. 12 e 13 del Regolamento.

Soltanto nell'ultima versione del documento recante "Informativa sulla privacy", entrata in vigore il 20 gennaio 2023, risulta indicata la base giuridica del consenso per il trattamento dei dati sanitari "(…), al fine di abilitare il collegamento del Suo account CareLink™ Personal all'account CareLink™ utilizzato dal Suo professionista sanitario nell'ambito del trattamento medico".

5. Conclusioni

Alla luce delle valutazioni sopra richiamate, tenuto conto delle dichiarazioni rese dal titolare del trattamento nel corso dell'istruttoria e considerato che, salvo che il fatto non costituisca più grave reato, chiunque, in un procedimento dinanzi al Garante, dichiara o attesta falsamente notizie o circostanze o produce atti o documenti falsi ne risponde ai sensi dell'art. 168 del Codice "Falsità nelle dichiarazioni al Garante e interruzione dell'esecuzione dei compiti o dell'esercizio dei poteri del Garante", gli elementi forniti dal titolare del trattamento nella memoria difensiva sopra richiamata e nel corso dell'istruttoria, seppure meritevoli di considerazione, non consentono di superare integralmente i rilievi notificati dall'Ufficio con il richiamato 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 confermano le valutazioni preliminari dell'Ufficio e si rileva l'illiceità del trattamento di dati personali effettuato dalla società Medtronic Italia S.p.a., in violazione degli artt. 5, par. 1, lett. a), f), 9, 12, 13 e 32 del Regolamento. La violazione delle predette disposizioni rende altresì applicabile, ai sensi dell'art. 58, par. 2, lett. i), la sanzione amministrativa prevista dall'art. 83, parr. 4 e 5 del Regolamento, ai sensi degli artt. 58, par. 2, lett. i), e 83, par. 3, del Regolamento medesimo.

In tale quadro -considerato, in ogni caso, che la condotta ha esaurito i suoi effetti, tenuto conto che la Società ha dichiarato che, oltre a formare nuovamente il personale interessato all'invio di email, intende, in revisione delle procedure adottate, utilizzare un nuovo strumento automatizzato per evitare il verificarsi in futuro dell'incidente descritto, anche implementando ulteriori controlli prima di inviare qualsiasi notifica email e preso atto che la medesima Società ha provveduto a integrare l'informativa, entrata in vigore a gennaio 2023, nei termini sopra descritti- non ricorrono i presupposti per l'adozione di provvedimenti, di tipo prescrittivo o inibitorio, di cui all'art. 58, par. 2, del Regolamento.

6. 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).

Il Garante, 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).

Nel caso di specie, la Società ha posto in essere due distinte condotte, che devono essere considerate separatamente ai fini della quantificazione della sanzione amministrativa da applicarsi.

6.1. La condotta di cui al paragrafo 4.1

Tenuto conto che la violazione delle disposizioni citate nel precedente paragrafo 4.1, aventi ad oggetto l’invio di comunicazioni mediante notifiche email a un numero plurimo di destinatari, che sono stati inseriti nel campo copia conoscenza (c.c.), in assenza di idoneo presupposto giuridico, ha avuto luogo in conseguenza di un’unica condotta (stesso trattamento o trattamenti tra loro collegati), trova applicazione l’art. 83, par. 3, del Regolamento, ai sensi del quale l’importo totale della sanzione amministrativa pecuniaria non supera l'importo specificato per la violazione più grave. Considerato che, nel caso di specie, la violazione più grave riguarda gli artt. 5, par. 1, lett. a) e f) e 9 del Regolamento, l’importo totale della sanzione è da quantificarsi fino al 4% del fatturato qualora il bilancio, come nel caso in esame, superi l’importo di euro 20.000.000 (massimo edittale cd “statico”).

La predetta sanzione amministrativa pecuniaria inflitta, in funzione delle circostanze di ogni singolo caso, va determinata nell’ammontare tenendo in debito conto gli elementi previsti dall’art. 83, par. 2, del Regolamento.

Con specifico riguardo alle violazioni commesse dalla Società si evidenzia che il livello di gravità è stato considerato medio, tenuto conto del numero di interessati coinvolti, della durata della violazione nonché delle categorie di dati personali interessate (dati sulla salute) e del carattere non intenzionale (art. 83, par. 2, lett. a) e b) del Regolamento; cfr. Comitato europeo per la protezione dei dati, “Guidelines 04/2022 on the calculation of administrative fines under the GDPR” del 23 maggio 2023, punto 60).

Sono stati, poi, considerati gli ulteriori elementi previsti dall’art. 83, par. 2 del Regolamento e in particolare che:

> non sono pervenuti reclami o segnalazioni al Garante sull’accaduto (art. 83, par. 2, lett. k) del Regolamento);
>
> la Società ha preso in carico i rilievi sollevati dall’Ufficio revisionando le procedure adottate al fine di ridurre la replicabilità degli incidenti occorsi).

In ragione dei suddetti elementi, valutati nel loro complesso, si ritiene di determinare l’ammontare della sanzione pecuniaria nella misura di euro 250.000 (duecentocinquantamila) per la violazione degli artt. 5, par. 1, lett. a) e f) e 9 del Regolamento.

In ragione della particolare delicatezza dei dati trattati, 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.

Si rileva, infine, che ricorrono i presupposti di cui all’art. 17 del Regolamento n. 1/2019.

6.2. La condotta di cui al paragrafo 4.2

La violazione delle disposizioni citate nel precedente paragrafo 4.2, derivante dalla omessa

indicazione -sia nel documento contenente l'informativa predisposto a settembre 2020 che in quello aggiornato nel luglio 2022- dell'elemento informativo relativo alla base giuridica in virtù della quale viene effettuata la comunicazione di dati personali ai professionisti sanitari, ha avuto luogo in conseguenza di un'ulteriore unica condotta (stesso trattamento o trattamenti tra loro collegati). Nel caso di specie, la violazione degli artt. 5, par. 1, lett. a), 12 e 13 del Regolamento comporta l'applicazione dell'art. 83, par. 5 del Regolamento secondo il quale l'importo della sanzione è da quantificarsi fino al 4% del fatturato, qualora il bilancio, come nel caso in esame, superi l'importo di euro 20.000.000 (massimo edittale cd "statico").

La predetta sanzione amministrativa pecuniaria inflitta, in funzione delle circostanze di ogni singolo caso, va determinata nell'ammontare tenendo in debito conto gli elementi previsti dall'art. 83, par. 2, del Regolamento.

Con specifico riguardo alle violazioni commesse dalla Società si evidenzia che il livello di gravità è stato considerato basso, tenuto conto che la violazione ha riguardato l'assenza soltanto di uno specifico elemento informativo di cui all'art. 13 del Regolamento e del carattere non intenzionale della condotta (art. 83, par. 2, lett. a) e b) del Regolamento; cfr. Comitato europeo per la protezione dei dati, "Guidelines 04/2022 on the calculation of administrative fines under the GDPR" del 23 maggio 2023, punto 60).

Sono stati, infine, considerati gli ulteriori elementi previsti dall'art. 83, par. 2 del Regolamento e in particolare che:

non sono pervenuti reclami o segnalazioni al Garante sull'accaduto (art. 83, par. 2, lett. k) del Regolamento);

la Società ha provveduto a integrare l'informativa (art. 83, par. 2, lett. c) del Regolamento) e ha dimostrato un elevato grado di cooperazione con l'Autorità nel corso dell'istruttoria (art. 83, par. 2, lett. f) del Regolamento).

In ragione dei suddetti elementi, valutati nel loro complesso, si ritiene di determinare l'ammontare della sanzione pecuniaria nella misura di euro 50.000 (cinquantamila) per la violazione degli artt. 5, par. 1, lett. a), 12 e 13 del Regolamento.

In ragione della particolare delicatezza dei dati trattati, 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.

Si rileva, infine, che ricorrono i presupposti di cui all'art. 17 del Regolamento n. 1/2019.

TUTTO CIÒ PREMESSO IL GARANTE

dichiara l'illiceità del trattamento di dati personali effettuato dalla società Medtronic Italia S.p.a. per la violazione degli artt. 5, par. 1, lett. a) e f), 9, 12, 13 e 32 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, alla società Medtronic Italia S.p.a., con Sede legale in Milano, via Varesina, 162, c.a.p. 20156, C.F. e P.IVA 09238800156, in persona del legale rappresentante pro-tempore, di pagare la somma complessiva di euro 300.000 (trecentomila) 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 di ciascuna delle sanzioni comminate.

INGIUNGE

alla predetta società Medtronic Italia S.p.a., in caso di mancata definizione della controversia ai sensi dell'art. 166, comma 8, del Codice, di pagare la somma di euro 300.000 (trecentomila) 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.

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 giurisdizionale 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, 8 febbraio 2024

IL PRESIDENTE
Stanzione

IL RELATORE
Scorza

IL VICE SEGRETARIO GENERALE
Filippi