Norme Vincolanti d'Impresa di GSK

Dichiarazione pubblica del piano d'azione di GSK

Novembre 2022

Introduzione

In GSK (**noi, nostro/a/i/e**), le attività di risorse umane (**HR**) e ricerca e allo sviluppo (**R&D**) comportano il trattamento di "dati personali" (si veda il Glossario), incluso il trasferimento internazionale di tali dati personali. Ci impegniamo a porre in essere elevati standard di integrità nel trattamento dei dati personali e abbiamo adottato le Norme Vincolanti d'Impresa (**Binding Corporate Rules - BCR**) per poter effettuare trasferimenti internazionali di dati personali all'interno del nostro gruppo societario, in conformità alle leggi sulla protezione dei dati dell'Unione Europea e del Regno Unito, in particolare al Regolamento Generale sulla Protezione dei Dati (Regolamento 2016/679) (**GDPR**) e alla legislazione equivalente in vigore nel Regno Unito.

Che cosa sono le Norme Vincolanti di Impresa (BCR)?

Le nostre BCR comprendono una serie di documenti, tra cui la nostra Politica sulla Privacy e lo Standard per la Privacy, un accordo intragruppo tra le società GSK e la presente Dichiarazione pubblica del piano d'azione. Sono inoltre supportate da corsi di formazione e audit. La presente Dichiarazione pubblica del piano d'azione è concepita per spiegare le BCR e garantire che le persone (**Lei**) di cui trattiamo i dati personali nel contesto delle nostre attività di R&D e HR, siano consapevoli dei propri diritti ai sensi delle BCR e di come esercitarli.

Un glossario dei termini utilizzati nel presente documento è disponibile alla fine del documento. Se sono necessarie ulteriori informazioni, contattare il nostro Responsabile per la Protezione dei Dati per UE/UK al seguente indirizzo: EU.DPO@GSK.com.

Campo di applicazione delle nostre BCR

In seguito all'uscita del Regno Unito dall'Unione Europea, abbiamo predisposto due tipologie di BCR, le nostre **BCR dell'UE** (EU BCR) e le nostre **BCR del Regno Unito** (UK BCR). Tutti i riferimenti alle BCR contenuti nella presente dichiarazione si riferiscono sia alle EU BCR che alle UK BCR. Tutti i riferimenti al GDPR contenuti nella presente dichiarazione si riferiscono, in relazione alle nostre UK BCR, alle equivalenti leggi sulla protezione dei dati del Regno Unito, ivi inclusi l'UK Data Protection Act 2018 e il GDPR, in quanto parte integrante della legislazione del Regno Unito (noto come UK GDPR).

Le **EU BCR** si applicano ai dati personali raccolti nell'ambito delle nostre attività di HR e di R&D (come descritto ulteriormente di seguito), qualora vengano trasferiti a livello internazionale:

- da una società GSK che è soggetta alle leggi sulla protezione dei dati del SEE, nei Paesi del SEE indicati di seguito
- a un Paese al di fuori dello Spazio Economico Europeo (**SEE**), dove le leggi non offrono un livello adeguato di protezione dei dati personali.

Paesi SEE in cui è stata ottenuta l'approvazione: GSK ha ricevuto l'approvazione per le nostre BCR in: Austria, Belgio, Bulgaria, Croazia, Cipro, Danimarca, Estonia, Finlandia, Francia, Germania, Grecia, Islanda, Irlanda, Italia, Lettonia, Lituania, Lussemburgo, Malta, Norvegia, Paesi Bassi, Polonia, Portogallo, Regno Unito, Repubblica Ceca, Romania (solo R&D), Slovacchia, Slovenia, Spagna, Svezia, Svizzera e Ungheria.

Le **UK BCR** si applicano ai dati personali raccolti nell'ambito delle nostre attività di HR e di R&D (come descritto ulteriormente di seguito), qualora vengano trasferiti a livello internazionale:

- da una società GSK che è soggetta alle leggi sulla protezione dei dati del Regno Unito
- a un Paese al di fuori del Regno Unito, dove le leggi non offrono un livello adeguato di protezione dei dati personali.

Le nostre attività HR includono: (i) la gestione del processo di reclutamento, che comprende tutte le verifiche di screening, background e di eventuali iscrizioni sul casellario giudiziale; (ii) la gestione della nostra forza lavoro, tra cui l'amministrazione di retribuzione e benefit, dei programmi di assistenza sanitaria, pensioni, assistenza dei dipendenti, congedo, assicurazione e piani di risparmio, di malattia, salute e benessere, inclusione e diversità, gestione dei rapporto con i dipendenti, di procedimenti disciplinari e cessazioni del rapporto di lavoro; la fornitura di sistemazioni legate al lavoro o di prestazioni sanitarie e assicurative; di risposte a domande o richieste nonché la gestione di attività e documentazione successive alla fine del rapporto di lavoro; (iii) lo svolgimento delle operazioni aziendali, che comprende l'allocazione di beni e risorse, l'implementazione di pianificazione strategica e gestione dei progetti, la creazione di budget e bilanci d'esercizio, la conduzione di audit trail e il mantenimento della documentazione; (iv) l'analisi della nostra forza lavoro in modo da poter utilizzare e allocare al meglio i beni aziendali e le risorse umane; (v) la gestione della vendita di beni, fusioni, acquisizioni e riorganizzazioni; (vi) comunicazione con il personale,

compreso nei casi di emergenza, e creazione di contenuti come registrazioni, video o fotografie per scopi di comunicazione e formazione interne; (vi) la gestione di formazione, sviluppo, performance e gestione dei talenti; (vii) la gestione di prodotti, sistemi, reti e canali di comunicazione IT di GSK, anche per consentirne l'utilizzo da parte del personale, nonchè la gestione dei diritti di accesso e dell'uso accettabile, la creazione di backup e la raccolta di dati statistici sul loro utilizzo; (viii) le attività di natura giuridica e di conformità che prevedono il rispetto di requisiti legali, normativi e di altro tipo, quali leggi e regolamenti in materia di occupazione, previdenza sociale e medicina del lavoro, le imposte sul reddito e le detrazioni assicurative nazionali; il rispetto degli obblighi di registrazione e rendicontazione, il completamento del monitoraggio e della reportistica sulle pari opportunità, la conduzione di audit e la gestione del rischio; il rispetto delle ispezioni governative, la risposta a procedimenti legali, il perseguimento di azioni correttive e dei diritti giuridici, difesa nei contenziosi e gestione delle richieste o dei reclami interni, il rispetto delle politiche e le procedure interne e monitoraggio delle attività entro i limiti consentiti o e secondo quanto richiesto dalle leggi locali; (ix) il monitoraggio dell'uso delle risorse IT di GSK e delle indagini aziendali; (x) le attività in materia di salute, sicurezza e tutela e (xi) l'applicazione del processo Speak Up per consentire di sollevare o segnalare preoccupazioni internamente.

Le nostre attività R&D includono: studi clinici interventistici e non interventistici, avviati, gestiti o finanziati esclusivamente o congiuntamente da noi, e la conformità alle norme pertinenti, come il monitoraggio della sicurezza e la rendicontazione degli eventi avversi. I dati personali trattati comprendono i dati relativi ai "Ricercatori esterni" e ai "Soggetti di Ricerca" (vedere il Glossario).

Fuori dal campo di applicazione: le nostre BCR non regolano il trattamento e il trasferimento dei dati personali da parte delle nostre funzioni commerciali (ad esempio, i dati personali relativi ai consumatori oppure alle persone collegate ai fornitori delle nostre funzioni commerciali). Tali dati vengono protetti in base a meccanismi legali diversi. Le nostre UE BCR non coprono i trasferimenti dei dati personali da parte di società GSK situate al di fuori dello Spazio Economico Europeo (SEE), dove non sono soggetti alle leggi sulla protezione dei dati dell'UE. Le nostre UK BCR non coprono i trasferimenti dei dati personali da parte di società GSK situate al di fuori del Regno Unito, dove non sono soggetti alle leggi sulla protezione dei dati del Regno Unito.

Aziende GSK coperte dalle BCR: le nostre BCR sono vincolanti per tutte le aziende del nostro gruppo che hanno firmato l'accordo intragruppo di cui sopra. Queste società del gruppo forniranno alle autorità di controllo, su richiesta, le informazioni sugli audit relative alle informazioni personali trattate ai sensi delle presenti BCR i e consentiranno loro di effettuare controlli per dimostrare la conformità alle presenti BCR.

Per le EU BCR: GlaxoSmithKline (Ireland) Limited, società con sede in Irlanda, ha la responsabilità generale di garantire che le altre società del gruppo in tutto il mondo rispettino le EU BCR , compreso il porre rimedio ad eventuali violazioni delle EU BCR.
Per le UK BCR: GlaxoSmithKline plc, società con sede nel Regno Unito, ha la responsabilità generale di garantire che le altre aziende del gruppo in tutto il mondo rispettino le UK BCR , compreso il porre rimedio ad eventuali violazioni delle UK BCR .

Le nostre regole (come riportato nel nostro Standard sulla privacy)

1. Trattiamo i dati personali in modo corretto e lecito

Rispettiamo le leggi applicabili relative al trattamento dei dati personali. In caso di conflitto tra queste BCR e le leggi applicabili, soprattutto se tale conflitto può avere un sostanziale effetto negativo, incluse eventuali richieste legalmente vincolanti per la divulgazione di dati personali da parte di un'autorità preposta all'applicazione della legge o un organismo di sicurezza nazionale, sarà necessario segnalarlo a (per le EU BCR) GlaxoSmithKline (Ireland) Limited oppure a (per le UK BCR) GlaxoSmithKline plc e all'autorità di vigilanza competente. Qualora le leggi applicabili vietino alla società del gruppo in questione di procedere a tale notifica all'autorità di controllo competente, faremo del nostro meglio per ottenere una deroga a tale divieto.

Nel caso in cui tali sforzi non abbiano esito positivo, la società del gruppo fornirà all'autorità di controllo competente, ogni 12 mesi, informazioni generali sulle richieste ricevute da tali autorità, compreso il numero di richieste di divulgazione, il tipo di dati richiesti e, laddove possibile, l'identità dell'organismo richiedente.

In nessun momento, una società del gruppo fornirà informazioni personali a enti governativi di qualsiasi Paese in maniera indiscriminata, sproporzionata o su larga scala, con modalità che vadano oltre le necessità di una società democratica.

Motivo del trattamento: trattiamo i dati personali solo se abbiamo uno scopo aziendale legittimo per farlo e il trattamento è necessario per tale scopo. Tutte le attività di trattamento sono in linea con un'adeguata base giuridica ai sensi del GDPR.

Base giuridica per il trattamento: facciamo affidamento sulle seguenti basi giuridiche per trattare i dati personali. Il trattamento deve essere necessario:

- per l'esecuzione di un contratto con il soggetto che fornisce i dati personali o per prendere provvedimenti su sua richiesta prima di stipulare tale contratto;
- per adempiere ai nostri obblighi legali;
- per l'esecuzione da parte di GSK di un compito svolto nell'interesse pubblico;
- per tutelare gli interessi vitali del soggetto che fornisce i dati personali; o
- per gli interessi legittimi perseguiti da noi o da un soggetto terzo, a condizione che gli interessi, i diritti e le libertà del soggetto che fornisce i dati personali non abbiano la precedenza su tali interessi.

Categorie particolari di dati personali: data la natura delle "categorie particolari di dati personali" (vedere il Glossario), si applicano ulteriori misure di salvaguardia. Trattiamo le categorie particolari di dati personali solo se:

- è necessario per consentirci di rispettare i nostri obblighi giuridici e di esercitare i nostri diritti giuridici nell'ambito delle normative sul lavoro;
- è necessario per proteggere gli interessi vitali del soggetto che fornisce i dati personali qualora il soggetto sia fisicamente o legalmente incapace di dare il consenso;
- il trattamento riguarda dati personali che sono manifestamente resi pubblici dal soggetto che li fornisce;
- è necessario per accertare, esercitare o difendere diritti o procedimenti giuridici;
- è necessario per motivi di interesse pubblico effettivo; o
- per scopi di medicina preventiva o del lavoro, nonché per la valutazione della capacità lavorativa di uno dei nostri dipendenti, la diagnosi medica, l'erogazione di un trattamento sanitario o di assistenza sociale o la gestione dei sistemi e servizi di assistenza sanitaria o sociale, nell'ambito delle normative vigenti o di un contratto con un operatore sanitario. In tali circostanze, il trattamento sarà effettuato da un operatore sanitario vincolato dall'obbligo del segreto professionale o da un'altra persona soggetta a un appropriato obbligo di segretezza.

Laddove la legge lo richieda o nel caso in cui non sia possibile fare affidamento su una delle motivazioni di cui sopra per trattare i dati personali, richiederemo il consenso esplicito. Tratteremo le categorie particolari di dati personali esclusivamente in presenza di un consenso esplicito. Qualora venga fornito il consenso, è possibile revocarlo liberamente in qualsiasi momento. Se si desidera procedere in tal senso, è necessario comunicarlo contattandoci secondo le modalità indicate nelle nostre Informative sulla privacy disponibili qui.

2. Raccogliamo e conserviamo la quantità minima di dati personali necessaria per perseguire scopi aziendali specifici, espliciti e legittimi

Raccogliamo la quantità minima di dati personali necessaria per perseguire ogni specifico, esplicito e legittimo scopo commerciale. Garantiamo che i dati personali siano adeguati, pertinenti e limitati agli scopi per i quali li raccogliamo e/o li trattiamo ulteriormente. Qualora dovessimo venire a conoscenza di dati personali inesatti, adotteremo tutte le misure ragionevoli per cancellarli o rettificarli senza indugio. Ove possibile, facciamo affidamento su "dati anonimizzati" (vedere il Glossario) piuttosto che sull'uso di dati personali per raggiungere i nostri obiettivi. Garantiamo che i dati personali siano accurati e, laddove necessario, aggiornati.

Conserviamo un registro di tutte le attività di trattamento che svolgiamo sui dati personali, che mettiamo a disposizione delle autorità di controllo su richiesta. Questo registro contiene i recapiti di ciascuna società GSK che tratta i dati personali, le finalità del trattamento dei dati personali (ossia il motivo per cui utilizziamo i dati personali), le categorie di individui, i tipi di dati personali, le categorie di destinatari con cui condividiamo i dati personali, i trasferimenti internazionali dei dati personali e lo strumento giuridico pertinente che utilizziamo a tale scopo e, laddove possibile, i termini di conservazione previsti e una descrizione generale delle misure di sicurezza applicate alle attività di trattamento.

Laddove il nostro utilizzo dei dati personali possa comportare un rischio elevato per i diritti e le libertà degli individui, prima di procedere al trattamento effettuiamo una valutazione dell'impatto del trattamento sulla protezione dei dati personali. Eseguiamo queste valutazioni d'impatto sulla protezione dei dati con il supporto del

Responsabile per la Protezione dei Dati per UE/UK per gestire eventuali rischi del trattamento e individuare misure di sicurezza e altri meccanismi per garantire la protezione dei dati personali.
Conserviamo i dati personali solo per il tempo necessario a raggiungere il legittimo scopo aziendale. Dopodiché, li eliminiamo, distruggiamo o anonimizziamo.

3. Spieghiamo in che modo saranno utilizzati i dati personali e i diritti del soggetto che li fornisce

Trasparenza: siamo trasparenti riguardo alle nostre attività di trattamento dei dati personali. Ci assicuriamo che le informazioni sulle nostre attività di trattamento siano rese disponibili, come richiesto dalle leggi applicabili, generalmente al momento dell'acquisizione dei dati personali. Per informazioni su come GSK utilizza i dati personali, si possono consultare le nostre Informative sulla Privacy disponibili qui. Come minimo, forniremo o garantiremo la realizzazione di quanto segue.

Informazioni su GSK:
- l'identità e i recapiti della società GSK che agisce in qualità di "titolare del trattamento" (vedere il Glossario) dei dati personali e, laddove applicabile, del rappresentante di tale titolare;
- i recapiti del nostro Responsabile per la Protezione dei Dati (Responsabile per la Protezione dei Dati per UE/UK);

Informazioni su come utilizziamo le informazioni personali:
- le modalità e le ragioni per cui siamo autorizzati, ai sensi delle leggi vigenti, a raccogliere e utilizzare i dati personali, incluse le finalità del trattamento per cui i dati personali sono raccolti;
- nel caso in cui utilizziamo i dati personali per un legittimo scopo aziendale, le informazioni relative a tale legittimo interesse;
- informazioni su con chi condividiamo i dati personali, inclusi i destinatari o le categorie di destinatari, laddove possibile;
- in quali casi trasferiamo i dati personali al di fuori del Paese di residenza (o al di fuori del SEE, se la persona risiede nel SEE);
- nel caso in cui dovessimo fare affidamento alle presenti BCR oppure a un altro meccanismo legale per il trasferimento internazionale delle informazioni personali (a un Paese o un'organizzazione non ritenuti idonei ai sensi delle leggi vigenti), le informazioni relative alle BCR o al meccanismo legale e le modalità con cui è possibile ottenerne una copia;
- per quanto tempo conserviamo i dati personali dell'utente, compreso il relativo periodo di conservazione oppure, se ciò non è possibile, i criteri utilizzati per stabilire tale periodo;

Informazioni sui diritti dell'interessato relativi alle informazioni personali:
- informazioni sui diritti dell'interessato, ivi incluso il diritto di richiedere l'accesso, la correzione o la cancellazione dei dati personali o di limitare ovvero opporsi al trattamento dei dati personali, nonché il diritto di richiedere che GSK trasferisca i dati a un'altra organizzazione;
- le modalità per revocare il proprio consenso al trattamento dei dati personali in qualsiasi momento;
- il diritto di presentare un reclamo presso un'autorità di vigilanza;

Informazioni su particolati attività di trattamento:
- se occorre utilizzare i dati personali di un interessato in base alla legge o per adempiere a un contratto e le conseguenze derivanti dal mancato conferimento dei dati da parte dell' interessato
- se prendiamo decisioni su un interessato utilizzando i dati personali attraverso processi automatizzati senza il coinvolgimento umano (il cosiddetto "processo decisionale automatizzato"), ivi inclusi la previsione del comportamento o la valutazione delle caratteristiche di un interessato (la cosiddetta "profilazione");
- se effettuiamo processi decisionali automatizzati o di profilazione, forniamo informazioni sul nostro approccio, sull'importanza di questo trattamento e sulle conseguenze del trattamento per l' interessato; e
- se intendiamo utilizzare i dati personali dell'interessato per ulteriori finalità (diverse da quelle comunicate), informazioni su tali finalità aggiuntive.

Laddove otteniamo i dati personali da terze parti invece che direttamente dall'interessato, potremmo (in base alla legge applicabile) non fornire i suddetti dati se ciò fosse impossibile o implicasse uno sforzo sproporzionato.

Gestione dei diritti degli interessati: consentiamo ai soggetti che forniscono i dati personali di esercitare i propri

diritti ai sensi del GDPR, inclusi i diritti indicati di seguito (che possono essere soggetti a determinate restrizioni in base alle circostanze:

(i) **diritto ad accedere ai dati personali:** nello specifico, il diritto di ottenere da noi la conferma che sia in corso il trattamento dei dati personali e, in tal caso, l'accesso ai dati personali e alle seguenti informazioni:
- le finalità del trattamento;
- le categorie di informazioni personali in questione;
- i destinatari o le categorie di destinatari a cui i dati personali vengono o verranno divulgati, in particolare quelli in Paesi terzi o nelle organizzazioni internazionali;
- laddove possibile, il periodo di conservazione previsto per i dati personali oppure, se ciò non è possibile, i criteri utilizzati per stabilire tale periodo;
- l'esistenza del diritto di richiedere la rettifica o la cancellazione dei dati personali o la limitazione del trattamento dei dati personali che riguardano l'interessato o di opporsi a tale trattamento;
- il diritto di presentare un reclamo presso un'autorità di controllo;
- nel caso in cui i dati personali non siano stati raccolti direttamente presso nteressato, tutte le informazioni disponibili sulla loro origine;
- l'esistenza di processi decisionali automatizzati, inclusa la profilazione, e almeno in tali casi, informazioni significative sulla logica implicata, nonché sul significato e sulle conseguenze previste di tale trattamento per l'interessato;
- laddove le informazioni personali vengano trasferite a un Paese terzo o a un'organizzazione internazionale, l'interessato ha il diritto di essere informato sulle opportune misure di tutela.

Forniremo una copia dei dati personali sottoposti al trattamento. Per ogni ulteriore copia richiesta o nel caso in cui una richiesta sia manifestamente infondata o eccessiva, in particolare per la sua natura ripetitiva, potremo addebitare una commissione ragionevole basata sui costi amministrativi. Qualora venga presentata una richiesta in tal senso per via elettronica, le informazioni saranno fornite in un formato elettronico di uso comune. Il diritto di ottenere una copia dei propri dati personali non deve pregiudicare i diritti e le libertà degli altri.

(ii) **diritto di rettificare (correggere) i dati personali:** nello specifico, l'interessato ha il diritto di ottenere da noi, senza ritardi ingiustificati, la correzione dei dati personali inesatti che lo/la riguardano. Tenendo conto delle finalità del trattamento, l'interessato avrà il diritto di richiedere il completamento dei dati personali incompleti, anche fornendo una dichiarazione supplementare.

(iii) **diritto di cancellare i dati personali:** nello specifico,l'interessato ha il diritto di ottenere tempestivamente da noi la cancellazione dei dati personali che lo/la riguardano e saremo tenuti a cancellare i dati personali senza indebito ritardo nel caso in cui si applichi una delle seguenti condizioni:
- i dati personali non sono più necessari in relazione agli scopi per cui sono stati raccolti o altrimenti trattati;
- il ritiro del consenso sui cui si basa il trattamento e l'assenza di altri presupposti a norma di legge che consentano il trattamento;
- l'interessato si oppone al trattamento e non sono disponibili basi legittime per il trattamento;
- i dati personali sono stati trattati illecitamente;
- i dati personali devono essere eliminati per l'adempimento di un obbligo legale a cui siamo soggetti; e
- i dati personali sono stati raccolti in relazione all'offerta di servizi di informazione societaria.

Nel caso in cui abbiamo divulgato le informazioni sui dati personali e siamo tenuti a cancellarle, dovremo, tenendo conto della tecnologia disponibile e dei costi di attuazione, adottare misure ragionevoli, incluse quelle tecniche, per informare gli altri titolari del trattamento dei dati personali che l'interessato ha richiesto la cancellazione da parte loro di qualsiasi collegamento, copia o riproduzione di tali dati personali.

Il diritto alla cancellazione non si applica nella misura in cui il trattamento è necessario:
- per esercitare il diritto di libertà di espressione e informazione;
- per l'adempimento di un obbligo legale che richiede il trattamento in base alla legge a cui siamo soggetti o per l'esecuzione di un compito svolto nel pubblico interesse;
- per motivi di interesse pubblico nel settore della salute pubblica;
- per scopi di archiviazione nel pubblico interesse, per scopi di ricerca scientifica o storica o per fini statistici oppure per l'istituzione, l'esercizio o la difesa di diritti legali.

(iv) **diritto di limitare o di opporsi al trattamento dei dati personali.** Nello specifico, l'interessato ha il diritto di ottenere da noi la limitazione del trattamento dei dati personali nel caso in cui si applichi una delle seguenti condizioni:

- l'accuratezza dei dati personali viene contestata dall'interessato, per un periodo che ci consenta di verificare l'accuratezza dei dati personali;
- il trattamento è illecito e l'interessato si oppone alla cancellazione dei dati personali e richiede invece la limitazione del loro utilizzo;
- non abbiamo più necessità dei dati personali per le finalità del trattamento, ma ci vengono richiesti dall'interessato per l'istituzione, l'esercizio o la difesa di rivendicazioni legali;
- l'interessato si è opposto al trattamento in attesa di verificare se i nostri motivi legittimi prevalgono su quelli dell'interessato.

Nel caso in cui il trattamento sia stato limitato, tali informazioni personali saranno trattate, ad eccezione della conservazione, solo previo consenso dell'interessato o per l'istituzione, l'esercizio o la difesa di diritti legali o per la tutela dei diritti di un'altra persona fisica o giuridica o per motivi di rilevante interesse pubblico ai sensi del diritto dell'UE o degli Stati membri del SEE (per i trasferimenti dal SEE) oppure ai sensi delle leggi del Regno Unito (per i trasferimenti dal Regno Unito). Qualora l'interessato abbia ottenuto la limitazione del trattamento, verrà informato da noi prima che la limitazione del trattamento venga revocata.

(v) **diritto alla portabilità dei dati:** il diritto di fornire una copia dei dati personali all'interessato oppure a terzi, in particolare: l'interessato ha il diritto di ricevere i dati personali che lo/la riguardano, che ci ha fornito, in un formato strutturato, di uso comune e leggibile da un dispositivo automatico e ha il diritto di trasmettere tali dati a un altro titolare del trattamento senza impedimenti da parte nostra, qualora:

- il trattamento si basi sul consenso dell'interessato; e
- il trattamento venga eseguito con mezzi automatici.

Nell'esercizio del diritto alla portabilità dei dati, l'interessato ha il diritto di ottenere la trasmissione dei dati personali direttamente da un titolare del trattamento a un altro, laddove ciò sia tecnicamente fattibile. Questo diritto non deve pregiudicare i diritti e le libertà degli altri.

(vi) **il diritto affinchè noi non prendiamo decisioni basandosi esclusivamente sul trattamento automatico.** Nello specifico, l'interessato ha il diritto di non sottostare a una decisione basata esclusivamente su un'elaborazione automatizzata, tra cui la profilazione, che produce effetti legali o di significatività simile. Ciò non si applica se la decisione:

- è necessaria per stipulare un contratto fra noi e il soggetto che fornisce i dati personali oppure per renderlo efficace;
- è autorizzata dalla legge a cui siamo soggetti e che prevede anche misure idonee a salvaguardare i diritti e le libertà dell'interessato e i suoi legittimi interessi; o
- si basa sul consenso esplicito dell'interessato.

Adotteremo misure adeguate per tutelare i diritti e le libertà dell'interessato e i suoi legittimi interessi, almeno il diritto di ricevere un intervento diretto da parte nostra e il diritto di esprimere il proprio punto di vista e di contestare la decisione.

(vii) **diritto di ritirare il proprio consenso:** qualora l'interessato abbia precedentemente fornito il proprio consenso al trattamento dei dati personali.

(viii) **diritto di opporsi a un trattamento effettuato sulla base di un legittimo interesse.** In particolare, l'interessato ha il diritto di opporsi in qualsiasi momento al trattamento dei propri dati personali sulla base dei legittimi interessi del titolare del trattamento o di terzi oppure se il trattamento è necessario per eseguire un compito di interesse pubblico o per l'esercizio di pubblici poteri di cui è investito il titolare del trattamento.

(ix) **diritto di opporsi a ricevere comunicazioni di marketing.** Nello specifico, l'interessato ha il diritto di opporsi in qualsiasi momento al trattamento dei dati personali per scopi di marketing.

Inoltre, rispettiamo le leggi applicabili nei Paesi che prevedono altri diritti in relazione ai dati personali. Potremmo limitare il diritto ad accedere ai dati personali al fine di tutelare altri (ad esempio, il diritto alla privacy di un'altra persona) o per adempiere i nostri obblighi legali.

Processo decisionale automatizzato: facciamo un uso limitato delle procedure decisionali automatizzate durante il trattamento dei dati personali. Ricorreremo a un processo decisionale automatizzato solo se:

- è necessario per stipulare un contratto fra noi e il soggetto che fornisce i dati personali oppure per renderlo efficace;
- è autorizzato nell'ambito della legge dell'Unione o di uno Stato Membro (in relazione alle EU BCR) o della legislazione del Regno Unito (in relazione alle UK BCR) e le misure di salvaguardia previste dalla legge sono state implementate; o
- il soggetto ha fornito il proprio consenso esplicito.

Se si desidera esercitare uno qualsiasi dei propri diritti, è necessario comunicarlo contattandoci secondo le modalità indicate nella nostra Informativa sulla Privacy. Qualora l'interessato decida di esercitare un diritto, cercheremo di fornire informazioni sulle azioni intraprese in risposta a tale richiesta entro un mese di calendario. A seconda della complessità della richiesta e del numero di altre richieste che riceveremo, potremmo avere bisogno di altri due mesi per fornire tali informazioni. Comunicheremo all'interessato, entro un mese dal ricevimento della richiesta, se la nostra risposta subirà ritardi.

4. Non utilizziamo i dati personali per scopi incompatibili con lo scopo per cui sono stati originalmente raccolti

Limitazione dello scopo: tratteremo i dati personali esclusivamente in modo compatibile con lo scopo aziendale specifico, esplicito e legittimo per cui sono stati originalmente raccolti. Comunicheremo eventuali nuovi scopi per il trattamento dei dati personali.

5. Utilizziamo adeguate misure di salvaguardia di sicurezza

Tutela della privacy: implementiamo adeguate misure di sicurezza tecniche e organizzative per prevenire la distruzione accidentale o illecita, la perdita, l'alterazione e la divulgazione non autorizzata dei dati personali, nonché l'accesso non autorizzato a essi. Queste misure sono adeguate ai rischi associati all'utilizzo dei dati personali e includono l'uso di tecnologie all'avanguardia.

Gestione degli incidenti e delle violazioni: Notificheremo tempestivamente le violazioni dei dati personali alle autorità di controllo (vedere il Glossario) e in ogni caso entro 72 ore dal momento in cui ne verremo a conoscenza, a meno che non risulti improbabile che tali violazioni possano comportare un rischio per i diritti e le libertà delle persone interessate. Comunicheremo le violazioni dei dati personali al soggetto che li ha forniti se è probabile che tali violazioni comportino un alto rischio per i suoi diritti e le sue libertà e (a nostra discrezione) in determinate altre circostanze. Conserviamo un registro delle violazioni dei dati personali che include dati sulle violazioni dei dati personali, le conseguenze (laddove applicabile) e le azioni correttive intraprese per risolvere la violazione. Su richiesta, metteremo tali registri a disposizione delle autorità di controllo competenti.

6. Controlliamo attentamente la divulgazione di dati personali a soggetti terzi

Gestione della privacy per soggetti terzi: divulghiamo i dati personali al di fuori di GSK laddove previsto dalla legge, in relazione a procedimenti giuridici e in altre circostanze limitate e legali. Potremmo anche trasferire i dati personali al di fuori del nostro gruppo a: (a) terze parti che operano per nostro conto, inclusi i fornitori; o (b) altre terze parti indipendenti, come i partner di ricerca e commerciali o le agenzie regolatorie.

Se facciamo affidamento su terze parti per trattare i dati personali per nostro conto, mettiamo in atto adeguati controlli contrattuali, organizzativi e operativi per garantire la riservatezza e la sicurezza dei dati personali. Richiediamo che tali terze parti accettino tutte le disposizioni di cui all'articolo 28 del GDPR. Se scopriamo che una terza parte sta trattando dati personali in modo incoerente con i requisiti imposti da noi o dalle leggi applicabili, adotteremo tutte le misure ragionevoli per garantire che tali carenze vengano affrontate il più rapidamente possibile.

Trasferimenti successivi a soggetti terzi: laddove effettuiamo un trasferimento internazionale di dati personali dal SEE o dal Regno Unito a terze parti situate in Paesi dove le leggi sulla protezione dei dati non offrono un livello adeguato di protezione dei dati personali, implementeremo clausole contrattuali standard con il destinatario di tali dati personali. Si tratta di protezioni contrattuali in una forma prescritta approvata dalla Commissione Europea (per i trasferimenti dal SEE) o dal Segretario di Stato o dall'ICO (per i trasferimenti dal Regno Unito), a seconda dei casi; i dettagli sono disponibili qui: https://commission.europa.eu/law/law-topic/data-protection/international-

dimension-data-protection/standard-contractual-clauses-scc_en e https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-data-transfer-agreement-and-guidance/). L'interessato ha diritto a ricevere una copia di queste clausole contrattuali standard e può richiederle via e-mail all'indirizzo EU.DPO@GSK.com. Queste clausole contrattuali standard prevedono che sia GSK, in qualità di mittente, sia la terza parte, in qualità di destinatario dei dati personali, accettino di conformarsi a rigorosi requisiti contrattuali relativi al trattamento dei dati personali per garantirne una protezione adeguata. In qualità di interessato, è possibile presentare un reclamo in base alle clausole contrattuali standard applicabili, qualora GSK o il destinatario violino tali requisiti.

Garantire un livello di protezione sostanzialmente equivalente: potremo divulgare i dati personali all'interno del nostro gruppo di società e a terze parti che risiedono in Paesi al di fuori del SEE e del Regno Unito in cui le leggi sulla protezione dei dati non sono ritenute in grado di fornire un livello di protezione adeguato, dalla Commissione Europea (per i trasferimenti dal SEE) o dal Segretario di Stato (per i trasferimenti dal Regno Unito). Prima della divulgazione di dati personali a destinatari che si trovano in tali Paesi, eseguiremo un processo di valutazione in più fasi per stabilire se le nostre protezioni contrattuali (incluse le BCR e le clausole contrattuali standard per i trasferimenti successivi) forniscono garanzie adeguate per assicurare una protezione adeguata dei dati personali:

- Valuteremo se le leggi e le prassi del Paese ricevente possano compromettere le misure di protezione dei dati esistenti, inclusa la possibilità per i destinatari dei dati personali di adempiere ai propri obblighi di protezione dei dati personali. Ciò implica la valutazione dell'eventualità che le leggi e le prassi del Paese implichino che il destinatario divulghi informazioni personali alle autorità pubbliche o fornisca loro accesso in misura superiore a quanto necessario e proporzionato.
- Qualora da tale valutazione emerga il rischio che le BCR non forniscano garanzie adeguate per i dati personali, considereremo la possibilità di imporre misure aggiuntive al trasferimento dei dati personali per garantire un livello di protezione sostanzialmente equivalente. Questo può comportare l'applicazione di ulteriori misure tecniche di sicurezza.
- Il Responsabile per la Protezione dei Dati per UE/UK, insieme a GlaxoSmithKline (Ireland) Limited (per i trasferimenti dal SEE) e GlaxoSmithKline plc (per i trasferimenti dal Regno Unito), parteciperanno a tale valutazione.
- Informeremo le altre società GSK del risultato di questa valutazione e richiederemo loro di applicare tali misure di sicurezza aggiuntive per trasferimenti simili.
- Laddove dovessimo ritenere di non essere in grado di adottare misure di sicurezza aggiuntive adeguate per fornire un livello di protezione sostanzialmente equivalente ai dati personali o su richiesta di un'autorità di controllo competente, informeremo le altre società GSK e interromperemo o sospenderemo il trasferimento di tali dati personali.

Registrazioni normative: laddove necessario, secondo le leggi sulla protezione dei dati applicabili in qualsiasi Stato Membro del SEE o nel Regno Unito, notifichiamo o otteniamo l'approvazione dall'autorità garante per la protezione dei dati in merito al trattamento dei dati personali (inclusi i trasferimenti internazionali di dati personali) e garantiamo che le notifiche o le richieste di approvazione vengano mantenute aggiornate qualora dovessero subentrare modifiche.

7. Gestiamo una procedura di reclamo e rispettiamo il diritto dell'interessato ad azioni correttive

Presentare un reclamo presso GSK: se un interessato ritiene che non abbiamo rispettato le regole stabilite nelle nostre BCR, è libero di sollevare le proprie preoccupazionii direttamente con noi e di sottoporre il reclamo alla valutazione nell'ambito della nostra procedura interna di risoluzione dei reclami. Incoraggiamo a presentare reclami sulla privacy attraverso il nostro canale di segnalazione Speak Up.

Attività HR: per i dipendenti e le altre persone i cui dati vengono trattati in relazione ad attività HR, un reclamo sulla privacy potrebbe essere notificato a un line manager (nel caso dei dipendenti GSK), un responsabile di Compliance, Legal o HR locale o il loro equivalente regionale, i quali segnaleranno il reclamo sulla privacy al canale appropriato. Tale canale inoltrerà il reclamo alla funzione di Compliance della business unit e al Privacy Team, dove verranno esaminate in modo indipendente le azioni appropriate in risposta al reclamo.

Attività R&D: per le persone i cui dati personali vengono trattati in relazione ad attività R&D, i "Soggetti di ricerca" (vedere il Glossario) devono contattare il clinico o il ricercatore che si occupa dello studio, il quale inoltrerà il reclamo al nostro Privacy Team. Nel caso di "Ricercatori esterni" (vedere il Glossario), un reclamo sulla privacy potrebbe essere notificato presso la Compliance nazionale di GSK, Legal o l'equivalente regionale, i quali riporteranno il reclamo sulla privacy al canale appropriato all'interno di GSK, dove verranno esaminate in modo indipendente le azioni appropriate in risposta al reclamo.

Escalation: indipendentemente da dove riceviamo reclami relativi alla privacy, verranno segnalati come segue: (i) a un Referente per la privacy di GSK, i cui recapiti sono pubblicati sul nostro sito Web qui; o (ii) al Responsabile per la Protezione dei Dati per UE/UK di GSK all'indirizzo EU.DPO@GSK.com. Il Responsabile per la Protezione dei Dati per UE/UK rappresenta l'ultima soluzione all'interno di GSK per la risoluzione dei reclami relativi alle nostre BCR. Cerchiamo di risolvere tempestivamente i reclami e, salvo circostanze eccezionali, GSK contatterà l'interessato per iscritto entro un mese dal ricevimento di un reclamo. La comunicazione: (a) indicherà la nostra posizione in merito al reclamo e a qualsiasi azione che abbiamo intrapreso o che intraprenderemo in risposta al reclamo; o (b) specificherà quando il soggetto che fornisce i dati personali verrà informato della nostra posizione, il che avverrà entro e non oltre due mesi. Se lo si desidera, è possibile contattare direttamente il nostro Responsabile per la Protezione dei Dati per UE/UK.

Presentare un reclamo presso un'autorità di controllo o un tribunale:
Per le EU BCR: è possibile presentare un reclamo in relazione alle nostre EU BCR a uno dei seguenti enti: (i) l'autorità di controllo competente nel Paese del SEE in cui risiede o lavora l'interessato o in cui è avvenuta la presunta violazione; (ii) il Data Protection Commissioner irlandese o i tribunali irlandesi (in quanto sede di GlaxoSmithKline (Ireland) Limited); (iii) i tribunali del paese del SEE da cui i dati personali sono stati trasferiti; o (iv) i tribunali del paese del SEE in cui risiede l'interessato.
Per UK BCR: è possibile presentare un reclamo in relazione alle nostre UK BCR all'Information Commissioner o qualsiasi tribunale del Regno Unito (in quanto sede di GlaxoSmithKline plc).

Seguire la nostra procedura interna per i reclami non pregiudica in alcun modo il diritto dell'interessato di utilizzare queste opzioni.

L'interessato potrà avere il diritto di ottenere un risarcimento e, in determinate circostanze, un indennizzo in caso di violazione delle BCR. Se si presenta un reclamo e si può dimostrare di aver subito danni materiali o immateriali a causa di una violazione delle nostre EU o UK BCR, saremo tenuti a dimostrare che non si è verificata alcuna violazione delle BCR rilevanti.

Se un'autorità di controllo o un tribunale del SEE emette un'ingiunzione contro una società GSK al di fuori dello Spazio Economico Europeo (SEE) in relazione alle nostre EU BCR e la società GSK non può o non vuole, per qualsiasi motivo, pagare i danni o attenersi all'ingiunzione entro l'eventuale periodo di tolleranza applicabile, GlaxoSmithKline (Ireland) Limited dovrà pagare i danni direttamente all'interessato oppure dovrà garantire che la società GSK si atterrà all'ingiunzione.

Se l'UK Information Commissioner (o il suo successore o sostituto) o i tribunali del Regno Unito emettono un'ingiunzione contro un'azienda GSK al di fuori del Regno Unito in relazione alle nostre UK e la società GSK non può o non vuole, per qualsiasi motivo, pagare i danni o attenersi all'ingiunzione entro l'eventuale periodo di tolleranza applicabile, GlaxoSmithKline plc dovrà pagare i danni direttamente all'interessato oppure dovrà garantire che l'azienda GSK si atterrà all'ingiunzione.

Glossario

- Per "protezione adeguata" o "livello adeguato di protezione" si intende un livello di protezione dei dati in un Paese al di fuori del SEE (per i trasferimenti dal SEE) o del Regno Unito (per i trasferimenti dal Regno Unito) che, in base alle leggi sulla protezione dei dati, è considerato in grado di fornire un'adeguata protezione dei diritti e delle libertà degli individui per quanto riguarda i loro dati personali.
- Per "dati anonimizzati" si intendono dati personali resi anonimi in modo tale che una persona non sia, o non sia più identificata o identificabile.
- All'interno di GSK, per "complementary worker" si intende qualsiasi persona, esclusi i dipendenti di GSK, che fornisca servizi per o per conto di GSK, inclusi lavoratori a termine interni o esterni, consulenti professionisti, staff temporaneo, personale di fornitori e appaltatori di servizi.
- Per "titolare del trattamento" si intende una persona fisica o giuridica che stabilisce le finalità e i mezzi del trattamento dei dati personali, individualmente o congiuntamente ad altri.
- Per "Responsabile per la Protezione dei Dati per EU/UK " si intende il responsabile della protezione dei dati, che controlla la conformità alle nostre BCR ed è responsabile del controllo del rispetto della legge sulla protezione dei dati dell'UE e del Regno Unito. È possibile contattare il Responsabile per la Protezione dei Dati per EU/UK all'indirizzo EU.DPO@GSK.com.
- Per "ricercatori esterni" si intendono medici esterni o altri operatori sanitari che partecipano o possono partecipare ad attività R&D.

- Per "violazione dei dati personali" si intende qualsiasi violazione della sicurezza che porti alla distruzione accidentale o illecita, la perdita, l'alterazione e la divulgazione non autorizzata delle informazioni personali, nonché l'accesso non autorizzato a esse.
- Per "dati personali" si intendono dati relativi a una persona identificata o identificabile.
- Per "Soggetti di Ricerca" si intendono individui che partecipano ad attività di ricerca o candidati alla partecipazione a tali attività, oppure individui che assumono i nostri prodotti o trattamenti e di cui trattiamo i dati personali nel contesto delle attività di farmacovigilanza. I Soggetti di Ricerca includono partecipanti sia interni che esterni a GSK.
- Per "categorie particolari di dati personali" si intende un sottoinsieme di dati personali relativi a razza o etnia, opinioni politiche, convinzioni religiose o filosofiche, appartenenza sindacale, dati genetici, dati biometrici trattati allo scopo di identificare in modo univoco una persona fisica, dati riguardanti la salute o dati riguardanti la vita sessuale o l'orientamento sessuale di una persona fisica.

Novembre 2022