Dichiarazione pubblica sulle norme vincolanti d'impresa di GSK

Introduzione

In GSK **(noi, nostro/a/i/e – società appartenenti al gruppo GSK ed affiliate),** le attività relative alle risorse umane **(HR,** Human Resources**)** e alla ricerca e allo sviluppo **(R&D,** Research & Development**)** comportano il trattamento di "dati personali" (vedere il Glossario), incluso il trasferimento di tali dati personali a livello internazionale. Ci impegniamo a porre in essere elevati standard di integrità nel trattamento dei dati personali e abbiamo adottato le così dette Norme Vincolanti d'Impresa (Binding Corporate Rules - **BCRs)** per poter effettuare trasferimenti internazionali di dati personali all'interno del nostro gruppo in conformità alle leggi sulla protezione dei dati dell'Unione europea, in particolare al Regolamento generale sulla protezione dei dati (Regolamento 2016/679**) (GDPR).**

Che cosa sono le norme vincolanti d'impresa?

Le nostre norme vincolanti d'impresa comprendono una serie di documenti, tra cui il nostro standard e le nostre norme sulla privacy, un accordo intragruppo tra le aziende GSK e la presente dichiarazione pubblica. Inoltre, sono supportate da corsi di formazione e audit. La presente dichiarazione pubblica è concepita per spiegare le norme vincolanti d'impresa e garantire che le persone di cui trattiamo i dati personali nel contesto delle nostre attività R&D e HR siano consapevoli dei propri diritti ai sensi delle norme vincolanti d'impresa e di come esercitarli.

Un glossario dei termini utilizzati nel presente documento è disponibile alla fine del documento. Per ulteriori dettagli, è possibile ottenere una copia delle nostre norme vincolanti d'impresa contattando il nostro EU Data Protection Officer qui: EU.DPO@GSK.com.

Campo di applicazione delle nostre norme vincolanti d'impresa

Le norme vincolanti d'impresa si applicano ai dati personali raccolti nel contesto delle nostre attività R&D e HR, come spiegato dettagliatamente più avanti, laddove vengono trasferiti a livello internazionale, da parte di un'azienda GSK soggetta alle leggi sulla protezione dei dati del Regno Unito o dell'UE per paesi in cui è stata ottenuta l'approvazione, in un paese al di fuori dello Spazio economico europeo (SEE) dove le leggi non offrono un livello adeguato di protezione per i dati personali.

Paesi UE in cui è stata ottenuta l'approvazione: GSK ha ricevuto l'approvazione per le nostre norme vincolanti d'impresa 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 nostre attività HR includono: amministrazione e gestione della nostra forza lavoro; attività di pre-selezione e assunzione; creazione di un rapporto di lavoro; amministrazione di salari e benefit; formazione, sviluppo e performance; gestione di procedimenti disciplinari e reclami; comunicazioni con i dipendenti e fornitura di referenze; comunicazioni con i dipendenti in caso di emergenza; gestione del canale di segnalazione Speak Up per consentire di sollevare o segnalare dubbi internamente; garantire lo svolgimento delle operazioni aziendali e l'accesso ai sistemi per i dipendenti affinché siano in grado di svolgere le attività in base al proprio ruolo; controllo e monitoraggio delle comunicazioni dei dipendenti; conformità ai requisiti giuridici, ai regolamenti e a disposizioni di altro tipo applicabili a GSK, compresi quelli derivanti dalle leggi e dai regolamenti in materia di tasse, salute e sicurezza, antidiscriminazione, riservatezza dei dati, occupazione e immigrazione, dagli obblighi di registrazione e rendicontazione, dagli obblighi di revisione e dalle ispezioni governative; e risposta ad azioni giuridiche, perseguimento di azioni correttive e dei diritti giuridici, difesa nei contenziosi e gestione delle richieste o dei reclami interni. I dati personali trattati includono i dati relativi ai dipendenti attuali, passati o potenziali di GSK o ai lavoratori complementari (vedere il Glossario), nonché ai coniugi e alle persone a carico, laddove applicabile.

Le nostre attività R&D: comprendono 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 coinvolti nella ricerca (vedere il Glossario).

Fuori dal campo di applicazione: le nostre norme vincolanti d'impresa 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 con i fornitori delle nostre funzioni commerciali). Tali dati vengono protetti in base a meccanismi legali diversi, che non coprono i trasferimenti dei dati personali da parte di aziende GSK situate al di fuori dello Spazio economico europeo (SEE), dove non sono soggetti alle leggi sulla protezione dei dati del Regno Unito o dell'UE.

Aziende GSK coperte dalle norme vincolanti d'impresa: le nostre norme vincolanti d'impresa sono vincolanti per tutte le aziende del nostro gruppo che hanno firmato l'accordo intragruppo di cui sopra. GlaxoSmithKline plc, un'azienda con sede nel Regno Unito, ha la responsabilità generale di garantire che le altre aziende del gruppo in tutto il mondo rispettino le norme vincolanti d'impresa, compreso il porre rimedio ad eventuali violazioni delle norme vincolanti d'impresa.

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 norme vincolanti d'impresa e le leggi applicabili, soprattutto se tale conflitto può avere un sostanziale effetto negativo, è necessario segnalare il problema all'autorità garante per la protezione dei dati.

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:

(i) 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;
(ii) per adempiere ai nostri obblighi legali;
(iii) per l'esecuzione da parte di GSK di un compito svolto nell'interesse pubblico;
(iv) per tutelare gli interessi chiave del soggetto che fornisce i dati personali; o
(v) 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.

Dati di categoria speciale: data la natura dei "dati di categoria speciale" (vedere il Glossario), si applicano ulteriori misure di salvaguardia. Trattiamo i dati di categoria speciale solo se:

(i) è necessario per consentirci di rispettare i nostri obblighi giuridici e di esercitare i nostri diritti giuridici nell'ambito delle normative sul lavoro;
(ii) è necessario per proteggere gli interessi chiave del soggetto che fornisce i dati personali qualora il soggetto sia fisicamente o legalmente incapace di dare il consenso;
(iii) il trattamento riguarda dati personali che sono manifestamente resi pubblici dal soggetto che li fornisce;
(iv) è necessario per accertare, esercitare o difendere diritti o procedimenti giuridici;
(v) è necessario per motivi di interesse pubblico effettivo; o
(vi) 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.

Cerchiamo di ottenere il consenso inequivocabile al trattamento dei dati personali e dei dati di categoria speciale laddove previsto dalla legge o laddove non possiamo fare affidamento su una delle basi giuridiche di cui sopra.

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

Raccogliamo la quantità minima di dati personali necessaria per perseguire ogni legittimo scopo aziendale. Garantiamo che i dati personali siano adeguati, pertinenti e non eccessivi in relazione agli scopi per i quali li raccogliamo e/o li trattiamo ulteriormente. Ove possibile, facciamo affidamento su dati anonimizzati piuttosto che sull'uso di dati personali per raggiungere i nostri obiettivi. Garantiamo che i dati personali siano accurati e, laddove necessario, aggiornati.

Conserviamo i dati personali solo per il tempo necessario a raggiungere i legittimi scopi aziendali. 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. Forniamo i dati richiesti dalle leggi applicabili, al momento della raccolta dei dati personali. Di minima, forniamo i dati minimi necessari ai sensi degli Articoli 13 e 14 del GDPR. Laddove otteniamo i dati personali da terze parti invece che direttamente dall'interessato, potremmo (in base alla legge applicabile) non fornire questi dati se ciò fosse impossibile o implicasse uno sforzo sproporzionato.

Gestione dei diritti individuali: consentiamo ai soggetti che forniscono i dati personali di esercitare i propri diritti ai sensi del GDPR, incluso il diritto di:

(i) accedere ai dati personali;
(ii) correggere i dati personali;
(iii) cancellare i dati personali;
(iv) limitare o interrompere il trattamento dei dati personali;
(v) ricevere una copia dei dati personali o richiedere di fornirne una ad una terza parte;
(vi) non prendere decisioni basandosi esclusivamente sul trattamento automatico (vedere di seguito);
(vii) ritirare il consenso al trattamento; e
(viii) opporsi a ricevere comunicazioni 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).

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:

(i) è necessario per stipulare un contratto fra noi e il soggetto che fornisce i dati personali oppure per renderlo efficace;
(ii) è autorizzato nell'ambito della legge UE o di uno stato membro e le misure di salvaguardia previste dalla legge sono state implementate; o
(iii) il soggetto ha fornito il proprio consenso esplicito.

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 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 le violazioni dei dati personali alle autorità garanti per la protezione dei dati, 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. Manteniamo un registro delle violazioni dei dati personali che include dettagli sulle violazioni dei dati personali, le conseguenze (laddove applicabile) per il soggetto che fornisce tali dati, per noi o per eventuali terze parti e le azioni correttive intraprese per risolvere la violazione. Su richiesta, metteremo tali registri a disposizione delle autorità garanti per la protezione dei dati.

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 trasferiamo dati personali a livello internazionale a terze parti situate in paesi al di fuori dello Spazio economico europeo (SEE), dove le leggi sulla protezione dei dati non offrono un livello adeguato di protezione dei dati personali, implementiamo clausole contrattuali standard approvate, i cui dettagli sono disponibili qui, oppure facciamo affidamento su specifiche deroghe previste dal GDPR per il trasferimento dei dati personali.

Registrazioni normative: laddove necessario secondo le leggi sulla protezione dei dati applicabili in qualsiasi stato membro, 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 ad azioni correttive

Presentare un reclamo presso GSK: se si ritiene che non abbiamo rispettato le regole stabilite nelle nostre norme vincolanti d'impresa, si è liberi di sollevare i propri dubbi 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 Centre of Excellence, dove verranno esaminate in modo indipendente le azioni appropriate in risposta al reclamo stesso.

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 Centre of Excellence. 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 stesso.

Escalation: indipendentemente da dove riceviamo reclami relativi alla privacy, se non possono essere risolti,

verranno segnalati come segue: (i) a un Country Privacy Advisor di GSK, i cui dettagli di contatto sono pubblicati sul nostro sito Web qui; quindi (ii) all'EU Data Protection Officer di GSK all'indirizzo EU.DPO@GSK.com. L'EU Data Protection Officer rappresenta l'ultimo livello all'interno di GSK per la risoluzione dei reclami relativi alle nostre norme vincolanti d'impresa. 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 EU Data Protection Officer.

Presentare un reclamo presso un'autorità garante della protezione dei dati o un tribunale: è possibile presentare un reclamo a uno dei seguenti enti: (i) l'autorità garante per la protezione dei dati competente nel paese in cui si risiede o si lavora o in cui è avvenuta la presunta violazione; (ii) l'UK Information Commissioner o i tribunali del Regno Unito (la sede di GlaxoSmithKline plc); (iii) i tribunali del paese SEE dal quale abbiamo trasferito i dati personali; e (iv) i tribunali del paese SEE in cui si ha la residenza principale. Seguire la nostra procedura interna per i reclami non pregiudica in alcun modo il diritto di utilizzare queste opzioni.

Se si presenta un reclamo e si può dimostrare di aver subito danni materiali o immateriali a causa di una violazione delle nostre norme vincolanti d'impresa, saremo tenuti a dimostrare che non si è verificata alcuna violazione delle nostre norme vincolanti d'impresa. Se un'autorità garante per la protezione dei dati o un tribunale emette un'ingiunzione contro un'azienda GSK al di fuori dello Spazio economico europeo (SEE) e l'azienda 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

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 "dati anonimizzati" si intendono dati personali resi anonimi in modo tale che una persona non sia o non sia più identificata o identificabile.
Per "dati di categoria speciale" si intende un sottoinsieme di dati personali relative 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.
Per "dati personali" si intendono dati relativi a una persona identificata o identificabile.
Per "ricercatori esterni" si intendono medici esterni o altri operatori sanitari che partecipano o possono partecipare ad attività R&D.
Per "soggetti di ricerca" si intendono persone che partecipano ad attività di ricerca o candidati alla partecipazione a tali attività, oppure persone 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.

[Giugno 2018]