GSK:s bindande företagsregler

GSK:s offentliga policyuttalande

November 2022

Inledning

GSK:s (**vi, oss, vår**) personalaktiviteter (**HR**) och aktiviteter inom forskning och utveckling (**R&D**) inbegriper behandling av personuppgifter (se ordlistan), vilket omfattar internationell överföring av sådana uppgifter. Vi strävar efter att bibehålla en hög integritetsnivå vid all hantering av personuppgifter. Vi har infört bindande företagsregler (**BCR**) i syfte att få internationella överföringar av personuppgifter inom företagskoncernen att följa EU:s och Storbritanniens dataskyddsregler, i synnerhet dataskyddsförordningen (förordning 2016/679) (**GDPR**) och dess motsvarighet i Storbritannien.

Vad är bindande BCR?

Våra BCR omfattar ett antal dokument, bland annat vår sekretesspolicy och våra dataskyddsnormer, ett koncerninternt avtal mellan GSK-företagen och det här offentliga policyuttalandet. De kompletteras med utbildning och revisioner. Det här offentliga policyuttalandet är avsett att beskriva BCR och se till att berörda individer (**du**), vars personuppgifter vi behandlar i samband med våra HR- och R&D-aktiviteter, är medvetna om sina rättigheter enligt våra BCR och hur rättigheterna kan utövas.

Sist finns en lista med ord som används i det här dokumentet. Om du vill ha ytterligare information kan du kontakta vårt dataskyddsombud för EU/Storbritannien här: EU.DPO@GSK.com.

Omfattningen av våra BCR

Som ett resultat av Storbritanniens utträde ur EU har vi två uppsättningar BCR, våra **BCR för EU** och våra **BCR för Storbritannien**. Alla hänvisningar till BCR i detta uttalande ska avse BCR för både EU och Storbritannien. Alla hänvisningar till GDPR i detta uttalande ska, när det gäller våra BCR för Storbritannien, avse motsvarande dataskyddslagstiftning för Storbritannien inklusive den brittiska dataskyddslagen 2018 och GDPR, eftersom den utgör en del av brittisk lag.

BCR för EU gäller för dina personuppgifter som samlas in i samband med våra HR- och R&D-aktiviteter (som beskrivs närmare nedan), där de överförs internationellt:

- av ett GSK-företag som lyder under EES dataskyddslagar, i de EES-länder som anges nedan
- till ett land utanför Europeiska ekonomiska samarbetsområdet (**EES**), där lagarna inte ger tillräckligt skydd för personuppgifter.

EES-länder där godkännande har inhämtats: GSK:s BCR har godkänts i: Belgien, Bulgarien, Cypern, Danmark, Estland, Finland, Frankrike, Grekland, Irland, Island, Italien, Kroatien, Lettland, Litauen, Luxemburg, Malta, Nederländerna, Norge, Polen, Portugal, Rumänien (endast R&D), Schweiz, Slovakien, Slovenien, Spanien, Sverige, Tjeckien, Tyskland, Ungern och Österrike.

BCR för Storbritannien gäller för dina personuppgifter som samlas in i samband med våra HR- och R&D-aktiviteter (som beskrivs närmare nedan), där de överförs internationellt:

- av ett GSK-företag som omfattas av brittisk dataskyddslag
- till ett land utanför Storbritannien, där lagarna inte ger tillräckligt skydd för personuppgifter.

Våra HR-aktiviteter: Dessa inkluderar (i) hantering av rekryteringsprocessen som omfattar samtliga kontroller, bakgrundskontroller och brottsregister; (ii) ledning av vår personalstyrka som omfattar löne- och förmånsadministration, hantering av hälso- och sjukvård, pensioner, stödtjänster för anställda, ledighet, försäkringar och sparplaner; hantering av sjukdomar, hälsa och välbefinnande, inkludering och mångfald; hantering av anställdas relationer, disciplinära frågor och uppsägningar; tillhandahållande av arbetsrelaterat boende eller hälso- och försäkringsförmåner; svara på frågor eller förfrågningar; och hantering av register och aktiviteter efter avslutad anställning; (iii) upprätthålla affärsverksamhet som omfattar allokering av tillgångar och resurser, genomföra strategisk planering och projektledning, skapa budgetar och finansiella rapporter, upprätthålla en verifieringskedja för revision och föra register; (iv) analysera vår arbetsstyrka så att vi bättre kan använda och allokera företagets tillgångar och mänskliga resurser; (v) hantera försäljningen av tillgångar, fusioner, förvärv och omorganisationer; (vi) kommunicera med personal, inklusive i en nödsituation, och skapa innehåll, såsom inspelningar, videor eller bilder för intern kommunikation och utbildningsändamål; (vi) hantera utbildning, utveckling, prestation- och kompetenshantering; (vii) hantera GSK:s IT-produkter, system, nätverk och kommunikationskanaler, inklusive för att möjliggöra att dessa kan användas av personal, inklusive hantering av åtkomsträttigheter och acceptabel användning, skapa säkerhetskopior och samla in statistisk information om deras användning; (viii) juridisk verksamhet och regelefterlevnad som omfattar

efterlevnad av lagar, regler och andra krav, såsom lagar och förordningar för anställning, socialförsäkring och företagshälsovård, inkomstskatt och allmänna försäkringsavdrag; uppfylla registerförings- och rapporteringsskyldigheter; slutföra övervakning och rapportering av lika möjligheter; genomföra revisioner och riskhantering; efterleva statliga inspektioner; svara på rättsprocesser, utöva juridiska rättigheter och rättsmedel för att försvara rättstvister och hantera eventuella interna klagomål eller anspråk; följa interna policyer och förfaranden; och övervakning av aktiviteter som tillåts eller krävs enligt lokal lagstiftning; (ix) övervaka GSK:s IT-resursanvändning och företagsutredningar; x) hälso-, trygghets- och säkerhetsverksamhet, och (xi) driva Speak Up-processen för att möjliggöra att problem tas upp eller rapporteras internt.

Våra R&D-aktiviteter: Dessa inbegriper interventionsbaserade och icke-interventionsbaserade kliniska studier som initieras enskilt eller i samarbete, leds eller finansieras av oss och tillhörande regelefterlevnad som exempelvis säkerhetsövervakning och biverkningsrapportering. Personuppgifterna som behandlas består av information om ”externa forskare” och ”forskningspersoner” (se ordlistan).

Detta ingår inte: Våra BCR styr inte våra kommersiella divisioners behandling och överföring av personuppgifter (exempelvis personuppgifter kopplade till kunder eller enskilda personer som är kopplade till leverantörer till våra kommersiella divisioner). De uppgifterna skyddas av olika lagstadgade mekanismer. Våra BCR för EU täcker inte in överföring av personuppgifter från GSK-företag utanför EES, där de inte skyddas av EU:s dataskyddslagar. Våra BCR för Storbritannien täcker inte överföring av personuppgifter från GSK-företag utanför Storbritannien, där de inte skyddas av brittiska dataskyddslagar.

GSK-företag som omfattas av BCR: Våra BCR är bindande för alla företag i koncernen som har undertecknat det koncerninterna avtal som anges ovan. Dessa koncernföretag ska på begäran tillhandahålla uppgifter om revisioner i samband med personuppgifter som behandlas enligt dessa BCR till relevanta tillsynsmyndigheter, och tillåta tillsynsmyndigheter att granska dem för att visa att dessa BCR följs.

För BCR för EU: GlaxoSmithKline (Ireland) Limited, ett irländskt företag, har det övergripande ansvaret för att säkerställa att övriga företag i koncernen i världen följer BCR för EU, inklusive att åtgärda överträdelser av dessa EU-regler.
För BCR för Storbritannien: GlaxoSmithKline plc, ett brittiskt företag, har det övergripande ansvaret för att säkerställa att övriga företag i koncernen i världen följer BCR för Storbritannien, inklusive att åtgärda överträdelser av dessa regler för Storbritannien.

Våra regler (som återspeglas i våra dataskyddsnormer)

1. Vi behandlar personuppgifter på ett korrekt och lagenligt sätt

Vi följer gällande lagar avseende behandling av personuppgifter. I händelse av en konflikt mellan dessa BCR och gällande lagar, som sannolikt kommer att ha en väsentlig negativ effekt, inklusive alla juridiskt bindande begärande om utlämnande av personuppgifter från en brottsbekämpande myndighet eller statligt säkerhetsorgan, ska detta rapporteras till (för BCR för EU) GlaxoSmithKline (Ireland) Limited, eller (för BCR för Storbritannien) GlaxoSmithKline plc, och den behöriga tillsynsmyndigheten. Om tillämplig lag förbjuder det aktuella koncernföretaget från att göra en sådan anmälan till den behöriga tillsynsmyndigheten kommer vi att göra vårt bästa för att få ett undantag från detta förbud.

Om dessa ansträngningar misslyckas kommer koncernföretaget att för varje 12-månadersperiod tillhandahålla behörig tillsynsmyndighet allmän information om de förfrågningar som företaget har mottagit från sådana myndigheter, inklusive antalet ansökningar om utlämnande, typ av begärda uppgifter och, om möjligt, identiteten på det organ som begärde uppgifterna.

Inte vid något tillfälle kommer något koncernföretag att tillhandahålla personuppgifter till statliga organ i något land urskillningslöst, oproportionerligt eller i stor skala på ett sätt som går utöver vad som är nödvändigt i ett demokratiskt samhälle.

Syfte med behandling: Vi behandlar endast personuppgifter om det föreligger legitima affärsändamål och databehandlingen är nödvändig för det ändamålet. All behandling sker enligt lämplig rättslig grund för GDPR.

Rättslig grund för behandling: Vi förlitar oss på följande rättsliga grunder vid behandling av personuppgifter. Databehandlingen måste vara nödvändig:

- för att uppfylla ett avtal där du är en av parterna eller för att vidta åtgärder på din begäran innan ett avtal ingås
- för att uppfylla våra rättsliga förpliktelser
- för att vi ska kunna utföra en uppgift som ligger i allmänhetens intresse
- för att skydda dina väsentliga intressen
- för våra eller tredje mans berättigade intressen ifall dessa intressen inte åsidosätts av dina egna intressen, rättigheter och friheter.

Uppgift av särskild kategori: Vid hantering av uppgifter av särskild kategori (se ordlistan) vidtas ytterligare skyddsåtgärder. Vi behandlar bara uppgifter av särskild kategori om:

- den är nödvändig för att vi ska kunna uppfylla våra rättsliga förpliktelser och utöva våra juridiska rättigheter enligt anställningslagarna
- den är nödvändig för att skydda dina väsentliga intressen ifall du är fysiskt eller juridiskt oförmögen att ge ditt medgivande
- behandlingen omfattar personuppgifter som du uppenbart själv har offentliggjort
- den är nödvändig för att fastställa, utöva eller försvara rättsanspråk
- den är nödvändig på grund av stort allmänintresse
- den behövs för preventiv medicin eller yrkesmedicin, bedömning av arbetsförmågan hos någon av våra medarbetare, medicinsk diagnos, tillhandahållande av hälsovård eller social vård eller behandling eller administration av system och tjänster för hälsovård eller socialvård enligt gällande lag eller enligt avtal med vårdpersonal. I de här situationerna behandlas uppgifterna av vårdpersonal som är bunden av tystnadsplikt eller en annan person som är bunden av lämplig sekretessplikt.

Vi kommer att söka ditt otvetydiga samtycke till att behandla dina personuppgifter om så krävs enligt lag eller om vi inte kan åberopa någon av ovan nämnda rättsliga grunder. När vi behandlar uppgifter av särskild kategori kommer vi endast att göra det där sådant samtycke uttryckligen ges. Om du ger oss ditt samtycke kan du när som helst återkalla det. Om du vill återkalla ditt samtycke meddelar du det genom att kontakta oss enligt vår information om behandling av personuppgifter som finns tillgängliga här.

2. Vi samlar in och lagrar ett minimum av personuppgifter som krävs för att genomföra specifika, uttryckligt angivna och legitima affärsändamål

Vi samlar in och lagrar ett minimum av personuppgifter som krävs för att genomföra varje specifikt, uttryckligen angivna och legitima affärsändamål. Vi ser till att personuppgifter är adekvata, relevanta och begränsade för de syften i vilka vi samlar in och/eller behandlar dem. Om vi får veta att några personuppgifter är felaktiga, vidtar vi alla rimliga åtgärder för att radera eller korrigera dem utan dröjsmål. Om så är möjligt använder vi oss av ”anonymiserade uppgifter” (se ordlistan), i stället för personuppgifter, för att uppnå våra syften. Vi säkerställer att personuppgifterna är korrekta och – vid behov – hålls aktuella.

Vi för ett register över all behandling som vi utför på dina personuppgifter, som vi på begäran gör tillgängligt för tillsynsmyndigheter. Detta register innehåller kontaktuppgifterna för alla GSK-företag som behandlar personuppgifter, syftena med behandlingen av dina personuppgifter (dvs. varför vi använder dina personuppgifter), kategorierna av enskilda personer, typerna av personuppgifter, kategorierna av mottagare som vi delar dina personuppgifter med, internationella överföringar av dina personuppgifter och det relevanta juridiska verktyg vi använder för det ändamålet, och där så är möjligt de planerade lagringsgränserna och en allmän beskrivning av de säkerhetsåtgärder som tillämpas på behandlingen.

Där vår användning av personuppgifter sannolikt kommer att resultera i en hög risk för dina rättigheter och friheter, genomför vi innan behandlingen en bedömning av behandlingens inverkan på skyddet av dina personuppgifter. Vi genomför bedömningar av behandlingens inverkan på skyddet av dina personuppgifter med stöd från dataskyddsombudet för EU/Storbritannien för att hantera eventuella risker i behandlingen och för att identifiera säkerhetsåtgärder och andra mekanismer för att säkerställa skyddet av dina personuppgifter.

Vi lagrar personuppgifter endast så länge som det behövs för att uppnå ett legitimt affärsändamål. Sedan raderar, förstör eller anonymiserar vi personuppgifterna.

3. Vi meddelar hur personuppgifter används och dina rättigheter

Transparens: Vi är transparenta med våra aktiviteter för behandling av personuppgifter. Vi säkerställer att du får information om vår behandling, i enlighet med gällande lagar, normalt vid tidpunkten för insamlingen av personuppgifterna. För information om hur GSK använder dina personuppgifter, se vår information om behandling av personuppgifter som finns här. Som ett minimum tillhandahåller eller säkerställer vi tillhandahållandet av följande.

Uppgifter om GSK:

- identiteten och kontaktuppgifterna för det GSK-företag som fungerar som ”personuppgiftsansvarig” (se ordlista) för dina personuppgifter och, i förekommande fall, den personuppgiftsansvariges företrädare
- kontaktuppgifterna till vårt dataskyddsombud (dataskyddsombudet för EU/Storbritannien).

Information om hur vi använder dina personuppgifter:

- hur och varför vi enligt tillämpliga lagar får samla in och använda dina personuppgifter, inklusive ändamålen med behandlingen som personuppgifterna är avsedda för
- om vi använder dina personuppgifter för ett legitimt affärsändamål, information om det berättigade intresset
- information om vem vi delar dina personuppgifter med, inklusive mottagare eller kategorier av mottagare, om sådana förekommer
- i vilka fall vi överför vi dina personuppgifter utanför ditt hemland? (eller utanför EES, om du befinner dig inom EES)
- om vi förlitar oss på dessa BCR, eller någon annan juridisk mekanism för att överföra dina personuppgifter internationellt (till ett land eller en organisation som inte anses adekvat enligt tillämplig lag), information om dessa BCR eller juridiska mekanismer, och hur du kan få en kopia av BCR eller annan juridisk mekanism
- hur länge vi behåller dina personuppgifter inklusive den period som personuppgifterna kommer att lagras under, eller om det inte är möjligt, de kriterier som används för att fastställa den perioden.

Information om vilka rättigheter du har avseende dina personuppgifter:

- information om dina rättigheter, inklusive rätten att begära åtkomst, rättelse eller radering av dina personuppgifter, eller att begränsa eller invända mot behandlingen av personuppgifter, eller rätten att begära att GSK överför dina uppgifter till en annan organisation
- hur du när som helst kan dra tillbaka ditt samtycke avseende vår behandling av dina personuppgifter
- din rättighet att framföra ett klagomål till behörig tillsynsmyndighet.

Information om särskilda behandlingsaktiviteter:

- om det är nödvändigt för oss att använda dina personuppgifter enligt lag eller för att fullgöra ett avtal med dig, och konsekvenserna för dig om du inte tillhandahåller oss de uppgifterna
- huruvida vi fattar beslut om dig med hjälp av dina personuppgifter genom automatiserade processer utan mänsklig inblandning (även kallat ”automatiserat beslutsfattande”), inklusive för att förutsäga beteende eller utvärdera egenskaper hos en person (kallat ”profilering”)
- om vi genomför automatiserat beslutsfattande eller profilering, information om vårt tillvägagångssätt, vilken betydelse denna behandling har och behandlingens konsekvenser för dig som enskild person
- om vi avser att använda dina personuppgifter för ytterligare ändamål (andra än de som meddelats dig), information om dessa ytterligare ändamål.

Om vi får dina personuppgifter från tredje man – inte direkt från dig – kan vi (enligt gällande lag) inte tillhandahålla ovan nämnda uppgifter till dig om detta är omöjligt eller innebär en orimlig ansträngning.

Tillämpning av individuella rättigheter: Vi låter dig utöva rättigheter enligt dataskyddsförordningen, inklusive de rättigheter som beskrivs nedan (vilka kan vara föremål för vissa begränsningar baserat på dina omständigheter:

(i) **rätten att begära åtkomst till dina personuppgifter** – specifikt rätten att få bekräftelse från oss om huruvida dina personuppgifter behandlas eller inte, och i så fall, åtkomst till dina personuppgifter och följande information:
   - ändamålen med behandlingen
   - kategorierna av personuppgifter som behandlas

- mottagare eller kategorier av mottagare till vilka dina personuppgifter har lämnats eller kommer att lämnas ut, särskilt mottagare i tredjeländer eller internationella organisationer
- där det är möjligt, den planerade lagringsperioden för dina personuppgifter, eller om det inte är möjligt, de kriterier som används för att fastställa den perioden
- förekomsten av din rätt att av oss begära rättelse eller radering av dina personuppgifter eller begränsning av behandlingen av dina personuppgifter eller att invända mot sådan behandling
- din rättighet att framföra ett klagomål till behörig tillsynsmyndighet
- om dina personuppgifter inte samlas in från dig, all tillgänglig information om deras källa
- förekomsten av automatiserat beslutsfattande, inklusive profilering och åtminstone i dessa fall, betydelsefull information om använd logik, samt betydelsen och de förväntade konsekvenserna för dig av sådan behandling
- om dina personuppgifter överförs till ett tredjeland eller till en internationell organisation har du rätt att få information om lämpliga skyddsåtgärder.

Vi ska tillhandahålla en kopia av dina personuppgifter som behandlas. För ytterligare kopior som du begär, eller där en begäran är uppenbart ogrundad eller överdriven, särskilt på grund av dess repetitiva karaktär, kan vi ta ut en rimlig avgift baserad på administrativa kostnader. Om du gör en sådan begäran på elektronisk väg ska uppgifterna tillhandahållas till dig i en vanlig elektronisk form. Din rätt att få en kopia av dina personuppgifter ska inte påverka andras rättigheter och friheter negativt.

(ii) **rätt att rätta (korrigera) dina personuppgifter –** du har rätt att utan onödigt dröjsmål få felaktiga personuppgifter om dig rättade. Med hänsyn till ändamålen med behandlingen ska du ha rätt att få ofullständiga personuppgifter kompletterade, inklusive genom att lämna ett kompletterande uttalande.

(iii) **rätt att radera dina personuppgifter –** du har rätt att utan onödigt dröjsmål få dina personuppgifter raderade och vi är skyldiga att radera dina personuppgifter utan onödigt dröjsmål om något av följande skäl föreligger:
- personuppgifterna inte längre är nödvändiga för de ändamål för vilka de har samlats in eller på annat sätt behandlats
- du återkallar ditt samtycke på vilket behandlingen baseras och det inte finns någon annan rättslig grund för behandlingen
- du invänder mot behandlingen och det inte finns några berättigade skäl för behandlingen som väger tyngre
- dina personuppgifter har behandlats på ett olagligt sätt
- dina personuppgifter måste raderas för att uppfylla en rättslig skyldighet som vi är föremål för
- dina personuppgifter har samlats in i samband med ett erbjudande av informationssamhällets tjänster.

Om vi har gjort personuppgifterna och är skyldiga att radera personuppgifterna ska vi, med hänsyn till tillgänglig teknik och kostnaden för genomförandet, vidta rimliga åtgärder, inbegripet tekniska åtgärder, för att informera andra personuppgiftsansvariga som behandlar personuppgifterna att du har begärt radering från dessa personuppgiftsansvariga av eventuella länkar till, eller kopiering eller reproduktioner av dina personuppgifter.

Rätten till radering ska inte gälla om behandling är nödvändig:
- för att utöva rätten till yttrande- och informationsfrihet
- för efterlevnad av en rättslig skyldighet som kräver behandling enligt lag som vi är föremål för eller för att utföra en uppgift som utförs i allmänhetens intresse
- av allmänt intresse av folkhälsoskäl
- för arkiveringsändamål i allmänhetens intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål eller för att fastställa, utöva eller försvara rättsanspråk.

(iv) **rätt att begränsa eller invända mot behandlingen av dina personuppgifter.** Specifikt ska du ha rätt att få behandlingen av dina personuppgifter begränsad av oss om något av följande gäller:
- personuppgifternas riktighet bestrids av dig, under en period som gör det möjligt för oss att verifiera personuppgifternas riktighet
- behandlingen är olaglig och du motsätter dig radering av personuppgifterna och begär istället begränsning av deras användning

- vi behöver inte längre personuppgifterna för behandlingens ändamål, men den registrerade kräver det av oss för att fastställa, utöva eller försvara rättsanspråk
- du har invänt mot behandling i avvaktan på verifieringen om huruvida våra berättigade skäl åsidosätter dina.

Om behandlingen har begränsats ska sådana personuppgifter, med undantag för lagring, endast behandlas med ditt samtycke eller för att fastställa, utöva eller försvara rättsanspråk eller för att skydda en annan fysisk eller juridisk persons rättigheter eller av skäl av viktigt allmänt intresse enligt EU:s eller EES-medlemsstats lagstiftning (för EES-överföringar), eller enligt brittisk lag (för brittiska överföringar). Om du har erhållit begränsning av behandlingen ska du informeras av oss innan begränsningen av behandlingen hävs.

(v) **rätt till dataportabilitet –** få en kopia av dina personuppgifter överlämnade till dig eller en tredje man, specifikt: du har rätt att få de personuppgifter om dig som du har lämnat till oss i ett strukturerat, vanligt och maskinläsbart format och har rätt att överföra dessa uppgifter till en annan personuppgiftsansvarig utan hinder från oss, om:
- behandlingen baseras på ditt samtycke
- behandlingen utförs automatiserat.

När du utövar din rätt till dataportabilitet ska du ha rätt att få personuppgifterna överförda direkt från en personuppgiftsansvarig till en annan, där det är tekniskt möjligt. Denna rättighet som avses ska inte påverka andras rättigheter och friheter negativt.

(vi) **rätt för oss att inte fatta beslut automatiskt om dig.** Specifikt har du rätt att inte bli föremål för ett beslut baserat enbart på automatiserad behandling, inklusive profilering, som ger rättsverkningar för dig eller som på liknande sätt väsentligt påverkar dig. Detta ska inte gälla om beslutet:
- krävs för att ingå, eller fullgöra, avtal mellan dig, den registrerade, och oss
- är auktoriserat enligt lag som vi lyder under och som även fastställer lämpliga åtgärder för att skydda dina rättigheter och friheter och berättigade intressen
- baseras på ditt uttryckliga samtycke.

Vi ska genomföra lämpliga åtgärder för att skydda dina rättigheter och friheter och berättigade intressen, åtminstone rätten att få till stånd mänskligt medverkande från vår sida och för att du ska kunna uttrycka din åsikt och bestrida beslutet.

(vii) **rätt att dra tillbaka ditt samtycke**– där du tidigare har lämnat samtycke till oss för att vi ska behandla dina personuppgifter.

(viii) **rätt att invända mot behandling som utförs utifrån ett berättigat intresse.** Specifikt har du rätt att när som helst invända mot behandlingen av dina personuppgifter baserat på den personuppgiftsansvariges eller tredje parts berättigade intressen, eller om behandlingen är nödvändig för att utföra en uppgift som ligger i allmänhetens intresse eller vid utövande av myndighet som tillkommer den personuppgiftsansvarige.

(ix) **rätt att invända mot, och avstå från att ta emot marknadskommunikation**. Specifikt ska du ha rätt att när som helst invända mot behandlingen av dina personuppgifter för marknadsföringsändamål.

Vi följer även gällande lagar i de länder som tillhandahåller dig andra rättigheter till dina personuppgifter. Vi kan komma att begränsa din rätt till dina personuppgifter i syfte att skydda andra (exempelvis en annan individs rätt till sekretess) eller för att uppfylla våra rättsliga förpliktelser.

Automatiskt beslutsfattande: Vi kan i begränsad utsträckning använda oss av automatiserat beslutsfattande vid behandling av personuppgifter. Vi använder oss endast av automatiserat beslutsfattande om:
- det krävs för att ingå, eller fullgöra, avtal mellan oss och dig
- det har godkänts enligt EU:s eller medlemsstaternas lagstiftning (avseende BCR för EU) eller enligt brittisk lagstiftning (avseende BCR för Storbritannien) och de skyddsåtgärder som krävs enligt gällande lag har vidtagits
- du uttryckligen har lämnat ditt samtycke.

Om du vill utöva någon av dina rättigheter meddelar du det genom att kontakta oss enligt vår information om behandling av personuppgifter. Om du väljer att utöva någon av dina rättigheter kommer vi att försöka lämna information om de åtgärder vi har vidtagit som svar inom en kalendermånad. Beroende på hur komplex din begäran är och antalet andra förfrågningar vi hanterar, kan vi behöva ytterligare två månader för att lämna denna information. Vi kommer att meddela dig inom en månad efter att vi mottagit din begäran om vårt svar kommer att bli försenat.

4. Vi använder inte personuppgifter för andra ändamål som inte är i linje med eller som går emot det ändamål för vilket de ursprungligen insamlades

Ändamålsbegränsning: Vi behandlar bara personuppgifter på sätt som motsvarar det specificerade, uttryckliga och legitima affärsändamålet för vilket de ursprungligen insamlades. Vi meddelar dig om andra ändamål för att behandla dina personuppgifter tillkommer.

5. Vi använder oss av lämpliga skyddsåtgärder

Skydd av din sekretess: Vi tillämpar lämpliga tekniska och organisatoriska säkerhetsåtgärder för att förhindra oavsiktlig eller olaglig destruktion, förlust, ändring, obehörigt yppande eller åtkomst av personuppgifter. Dessa åtgärder är anpassade till de risker som är förknippade med användning av personuppgifter och tar hjälp av moderna tekniker.

Hantering av incidenter och överträdelser: Vi rapporterar personuppgiftsöverträdelser (se ordlista) till tillsynsmyndigheter utan onödigt dröjsmål och i alla händelser inom 72 timmar efter att vi blivit medvetna om dem, såvida inte det är osannolikt att dessa överträdelser kan utsätta dina rättigheter och friheter för risk. Vi rapporterar personuppgiftsöverträdelser till dig ifall överträdelsen sannolikt kan utsätta dina rättigheter och friheter för stora risker samt i vissa andra situationer enligt vårt gottfinnande. Vi för ett register över personuppgiftsöverträdelser med detaljer om personuppgiftsöverträdelsen, eventuella effekter på dig samt den åtgärd som vidtagits för att åtgärda överträdelsen. På begäran kommer vi att tillgängliggöra registret för behöriga tillsynsmyndigheter.

6. Vi kontrollerar mycket noggrant utlämnande av personuppgifter till tredje man

Sekretesshantering för tredje man: Vi lämnar ut personuppgifter utanför vår företagskoncern om det krävs enligt gällande lag, i samband med rättsliga förfaranden och i vissa andra begränsade och lagenliga syften. Vi kan även komma att överföra personuppgifter utanför vår företagskoncern till: (a) tredje män som agerar på vårt uppdrag eller (b) andra oberoende tredje män, exempelvis partner inom forskning och handel eller övervakningsmyndigheter.

I de fall tredje män anlitas för att behandla personuppgifter för vår räkning tillämpar vi lämpliga avtalsbaserade, organisatoriska och operativa kontroller för att säkerställa sekretess och skydd av dina personuppgifter. Vi kräver att dessa tredje män godkänner alla bestämmelser i artikel 28 i dataskyddsförordningen. Om vi upptäcker att en tredje man behandlar personuppgifter på ett sätt som inte är förenligt med våra krav eller gällande lagstiftning kommer vi att vidta alla rimliga åtgärder för att säkerställa att bristerna åtgärdas så snabbt som möjligt.

Senare överföring till tredje män: När vi överför personuppgifter internationellt från EES eller Storbritannien till tredje part i länder där dataskyddslagarna i det landet inte erbjuder en adekvat skyddsnivå för personuppgifter, inför vi standardavtalsklausuler med mottagaren av personuppgifterna. Dessa är avtalsskydd i en föreskriven form godkänd av Europeiska kommissionen (för överföringar från EES) eller av ministern eller ICO (för överföringar från Storbritannien), beroende på vad som är tillämpligt (detaljer om vilka finns här: https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en och https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-data-transfer-agreement-and-guidance/). Du har rätt att få en kopia av dessa standardavtalsklausuler och kan begära dem via e-post till EU.DPO@GSK.com. Dessa standardavtalsklausuler kräver att både GSK som avsändare, och tredje part som mottagare, av dina personuppgifter samtycker till att följa stränga avtalskrav avseende hanteringen av dina personuppgifter för att säkerställa att de är korrekt skyddade. Du, som den enskilda registrerade, kan göra anspråk enligt relevanta standardavtalsklausuler om GSK eller mottagaren bryter mot dessa krav.

Säkerställa en väsentligen likvärdig skyddsnivå: Vi kan komma att lämna ut personuppgifter inom vår företagskoncern och till tredje parter som är belägna i länder utanför EES och Storbritannien där dataskyddslagarna inte anses ge en adekvat skyddsnivå av Europeiska kommissionen (för EES-överföringar) eller ministern (för brittiska överföringar). Före utlämnandet av personuppgifter till mottagare i dessa länder genomför vi en bedömningsprocess i flera steg för att överväga om våra avtalsskydd (inklusive BCR och eventuella standardavtalsklausuler för senare överföringar) ger tillräckliga garantier för att säkerställa ett lämpligt skydd av personuppgifter:

- Vi tar hänsyn till om mottagarlandets lagar och praxis försvagar befintliga dataskyddsåtgärder, inklusive om mottagarna av personuppgifter kan uppfylla sina skyldigheter att skydda personuppgifterna. Detta omfattar att bedöma om landets lagar och praxis innefattar att mottagaren lämnar ut personuppgifter till, eller ger åtkomst till personuppgifter genom, offentliga myndigheter i en omfattning som överstiger vad som är nödvändigt och proportionerligt.
- Om denna bedömning indikerar en risk för att BCR inte ger lämpligt skydd för personuppgifter, beaktar vi huruvida vi kan införa ytterligare åtgärder för överföringen av personuppgifter för att säkerställa en väsentligen likvärdig skyddsnivå. Detta kan innebära att ytterligare tekniska säkerhetsåtgärder tillämpas.
- Dataskyddsombudet för EU/Storbritannien, tillsammans med GlaxoSmithKline (Ireland) Limited (för EES-överföringar) och GlaxoSmithKline plc (för brittiska överföringar), kommer att vara involverade i denna bedömning.
- Vi kommer att informera andra GSK-företag om resultatet från denna bedömning, och kräva att GSK-företagen tillämpar dessa ytterligare säkerhetsåtgärder för liknande överföringar.
- Om vi anser att vi inte kan identifiera lämpliga ytterligare säkerhetsåtgärder för att tillhandahålla en väsentligen likvärdig skyddsnivå för personuppgifter, eller om vi uppmanas av en behörig tillsynsmyndighet, kommer vi att informera andra GSK-företag och avsluta eller avbryta överföringen av sådana personuppgifter.

Registreringar hos tillsynsmyndigheter: Där så krävs enligt gällande dataskyddslagar i någon EES-medlemsstat eller i Storbritannien meddelar vi eller inhämtar godkännande från den relevanta tillsynsmyndigheten avseende behandling av personuppgifter (inklusive internationella överföringar av personuppgifter) och säkerställer att meddelanden eller inlagor för godkännande hålls aktuella vid eventuella ändringar.

7. Vi tillämpar ett klagomålsförfarande och respekterar din rätt till åtgärd

Lämna klagomål till oss: Om du anser att vi inte har följt de regler som anges i våra BCR är du välkommen att vända dig direkt till oss och få ditt klagomål bedömt enligt vår interna process för att åtgärda klagomål. Vi uppmuntrar dig att lämna in sekretessklagomål via vår Speak Up-linje.

HR-aktiviteter: Anställda och andra enskilda individer vars uppgifter behandlas i samband med HR-aktiviteter kan lämna in sekretessklagomål till sin närmaste chef (gäller GSK-medarbetare), den compliance-ansvarige i landet, en lokal HR-representant eller ett juridiskt ombud eller den regionala motsvarigheten till någon av dessa. Alla kommer att rapportera sekretessklagomålet till klagomålskanalen som vidarebefordrar klagomålet till affärsenhetens compliance-grupp och sekretessteamet. De bedömer självständigt vilka åtgärder som bör vidtas som svar på ditt klagomål.

R&D-aktiviteter: Personer vars personuppgifter behandlas i samband med R&D-aktiviteter: Om du är en ”forskningsperson” (se ordlistan) bör du kontakta klinikern eller forskaren som genomför studien. Han eller hon vidarebefordrar klagomålet till sekretessteamet. Om du är en ”extern forskare” (se ordlistan) kan du lämna in klagomål till GSK:s compliance-ansvarige i landet, ett av företagets juridiska ombud eller den regionala motsvarigheten. Dessa kommer att vidarebefordra sekretessklagomålet till GSK:s klagomålskanal. De bedömer självständigt vilka åtgärder som bör vidtas som svar på ditt klagomål.

Eskalering: Oavsett varifrån vi får sekretessklagomål kommer de att eskaleras: (i) till GSK:s sekretesskontakt vars kontaktuppgifter finns på vår webbplats här, eller (ii) till GSK:s dataskyddsombud för EU/Storbritannien på EU.DPO@GSK.com. Dataskyddsombudet för EU/Storbritannien är den sista möjligheten inom GSK för att åtgärda ett klagomål på våra BCR. Vi bemödar oss om att lösa klagomål snabbt. Förutom vid exceptionella omständigheter kontaktar GSK dig skriftligt inom en månad. Skrivelsen kommer antingen att: (a) redogöra för vårt ställningstagande i frågan avseende klagomålet och eventuella åtgärder vi har vidtagit eller kommer att vidta som svar på klagomålet eller (b) ange när du får besked om vårt ställningstagande, vilket kommer att vara högst två månader därefter. Om du vill kan du kontakta vårt dataskyddsombud för EU/Storbritannien direkt.

Lämna in ett klagomål till en tillsynsmyndighet eller domstol:
För BCR för EU: Du kan lämna in ett klagomål avseende våra BCR för EU till någon av följande: (i) den behöriga tillsynsmyndigheten i det EES-land där du huvudsakligen är bosatt, arbetar eller där den påstådda överträdelsen skedde, (ii) Data Protection Commissioner eller domstol i Irland (där GlaxoSmithKline (Ireland) Limited har sitt säte), (iii) domstolarna i det EES-land varifrån personuppgifterna överfördes av oss eller (iv) domstolarna i det EES-land där du är bosatt.
För BCR för Storbritannien: Du kan lämna in ett klagomål angående våra BCR för Storbritannien till Information Commissioner för eller domstol i Storbritannien (där GlaxoSmithKline plc har sitt säte).

Att följa våra interna förfaranden för klagomål kommer inte på något sätt att påverka din rätt att använda dessa möjligheter.

Du kan ha rätt att få upprättelse och, under vissa omständigheter, kompensation när vi bryter mot BCR. Om du lämnar in ett klagomål och kan visa att du har lidit materiell eller immateriell skada som mest sannolikt beror på en överträdelse av antingen den ena uppsättningen eller båda uppsättningarna av BCR för EU och Storbritannien, behöver vi bevisa att relevanta BCR inte har överträtts.

Om en EES-tillsynsmyndighet eller domstol i ett EES-land utfärdar ett föreläggande mot ett GSK-företag utanför EES avseende våra BCR för EU och GSK-företaget av någon anledning är oförmöget eller ovilligt att betala skadeståndet eller följa föreläggandet inom en eventuell respitperiod, kommer GlaxoSmithKline (Ireland) Limited att betala skadeståndet som tilldelas dig direkt, eller säkerställa att det relevanta GSK-företaget följer föreläggandet.

Om Information Commissioner för Storbritannien (eller dess efterträdare eller ersättare) eller brittisk domstol utfärdar ett föreläggande mot ett GSK-företag utanför Storbritannien avseende våra BCR för Storbritannien och GSK-företaget av någon anledning är oförmöget eller ovilligt att betala skadeståndet eller följa föreläggandet inom en eventuell respitperiod, kommer GlaxoSmithKline plc att betala skadeståndet som tilldelas dig direkt, eller säkerställa att det relevanta GSK-företaget följer föreläggandet.

Ordlista

- ”Tillräckligt skydd” eller ”tillräcklig skyddsnivå” avser en dataskyddsnivå i ett land utanför EES (för EES-överföringar) eller Storbritannien (för överföringar i Storbritannien) som enligt dataskyddslagstiftning anses ge tillräckligt skydd för enskilda personers rättigheter och friheter för deras personuppgifter.
- ”Anonymiserade uppgifter” är uppgifter som har gjorts anonyma på ett sådant sätt att den enskilda personen inte längre identifieras eller kan identifieras.
- ”Visstidsanställd” avser en enskild person som inte är medarbetare hos GSK men som tillhandahåller tjänster för eller åt GSK, inklusive interna eller externa villkorsanställda, konsulter, tillfälligt anställda, underleverantörer och koncessionsinnehavare.
- ”Personuppgiftsansvarig” avser en fysisk eller juridisk person som bestämmer ändamålen och medlen för behandling av personuppgifter, antingen ensam eller tillsammans med andra.
- ”Dataskyddsombud för EU/Storbritannien” avser dataskyddsombudet som övervakar efterlevnaden av våra BCR och ansvarar för att övervaka efterlevnaden av EU:s och Storbritanniens dataskyddslagstiftning. Dataskyddsombudet för EU/Storbritannien kan kontaktas på EU.DPO@GSK.com.
- ”Extern forskare” avser läkare eller annan hälso- eller sjukvårdspersonal som deltar eller kan delta i R&D.
- ”Personuppgiftsöverträdelse” avser varje säkerhetsöverträdelse som leder till oavsiktlig eller olaglig förstörelse, förlust, ändring, obehörigt utlämnande av eller åtkomst till personuppgifter.
- ”Personuppgift” är en uppgift som rör en identifierad eller identifierbar enskild person.
- ”Forskningsperson” är kandidater för eller deltagare i forskningsaktiviteter eller personer som behandlas med våra produkter eller behandlingar och vars personuppgifter vi behandlar av farmakovigilansskäl. Forskningspersoner inbegriper deltagare både inom och utanför GSK.
- ”Uppgifter av särskild kategori” är ett urval av personuppgifter relaterat till en individs etniska ursprung, politiska åsikter, religiösa eller filosofiska övertygelse, fackföreningsmedlemskap, genetiska uppgifter, biometriska uppgifter som behandlas i syfte att unikt identifiera en fysisk person, uppgifter om hälsa eller uppgifter om en fysisk persons sexualliv eller sexuella läggning.

November 2022