Offentlig version av GSK:s bindande företagsregler

Inledning

GSK:s (**vi, oss, vår**) personalaktiviteter (**HR**) och aktiviteter inom forskning och utveckling (F&U) 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**) för internationella överföringar av personuppgifter inom företagsgruppen, för att följa EU:s och Storbritanniens dataskyddsregler, i synnerhet dataskyddsförordningen (förordning 2016/679) **(GDPR**) och Storbritanniens motsvarighet.

Vad är bindande företagsregler?

Våra bindande företagsregler omfattar ett antal dokument, bland annat vår policy och standard för behandling av personuppgifter, standarden för personuppgiftsbehandling inom F&U, ett avtal mellan företagen inom GSK-koncernen och det här offentliga dokumentet. De kompletteras med utbildning och revisioner. Det här offentliga dokumentet är avsett att beskriva de bindande företagsreglerna och se till att berörda individer (**du**), vars personuppgifter vi behandlar i samband med våra HR- och F&U-aktiviteter, är medvetna om sina rättigheter enligt våra bindande företagsregler och hur dessa rättigheter kan utövas.

Längst ned finns en lista med ord som används i det här dokumentet. Om du behöver ytterligare information kan du få en kopia av våra bindande företagsregler från vår EU-personuppgiftsansvariga på: EU.DPO@GSK.com.

Omfattningen av våra bindande företagsregler

Till följd av att Storbritannien upphört att vara en medlemsstat i EU har vi två uppsättningar av bindande företagsregler, våra bindande företagsregler för EU och våra bindande företagsregler för Storbritannien. Alla hänvisningar till GDPR i denna information ska, med avseende på våra bindande företagsregler för Storbritannien, avse motsvarande dataskyddslag i Storbritannien.

De bindande företagsreglerna för EU gäller för dina personuppgifter som insamlats under våra HR- och F&U-aktiviteter, enligt den noggrannare beskrivningen nedan där de överförs internationellt av ett GSK-företag som omfattas av EU-personuppgiftsskyddslagar, i de godkända EU-länderna; till ett land utanför Europeiska ekonomiska samarbetsområdet (EES) där lagarna inte ger tillräckligt skydd för personuppgifter.

EU-länder där godkännande har inhämtats: GSK:s bindande företagsregler 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 F&U), Schweiz, Slovakien, Slovenien, Spanien, Sverige, Tjeckien, Tyskland, Ungern och Österrike.

De bindande företagsreglerna för Storbritannien gäller dina personuppgifter som samlats in i samband med våra HR- och F&U-aktiviteter (så som dessa beskrivs nedan), där de överförs internationellt:

- Av ett GSK-företag som lyder under Storbritanniens dataskyddslagar;
- Till ett land utanför Storbritannien, där lagarna inte ger personuppgifter ett adekvat skydd.

Våra HR-aktiviteter: omfattar (i) hantering av rekryteringsprocessen, som omfattar all screening, bakgrunds- och brottsregisterkontroller; (ii) hantering av vår personal, som omfattar administration av löner och förmåner; hantering av hälso- och sjukvård, pensioner, medarbetarassistans, ledigheter, försäkrings- och sparplaner; hantering av sjukdom, hälsa och välbefinnande, inklusion och mångfald; hantering av medarbetarrelationer, disciplinärenden och uppsägningar; tillhandahållande av arbetsrelaterad logi eller hälso- och försäkringsförmåner, svar på förfrågningar eller begäranden; och hantering av register och aktiviteter efter avslutad anställning; (iii) affärsverksamhet inklusive allokering av tillgångar och resurser, genomförande av strategisk planering och projektledning, skapa budgetar och ekonomiska framställningar, upprätthålla

revisionsuppföljningar och register; (iv) analysera vår personal så att vi kan använda och fördela företagstillgångar och personal på ett bättre sätt; (v) hantera försäljningen av tillgångar, förvärv och omorganiseringar; (vi) kommunicera med vår personal, inklusive vid en nödsituation, och skapa innehåll, som t.ex. inspelningar, videor eller bilder för intern kommunikation eller utbildningssyften; (vii) hantera utbildning, utveckling, prestationer och kompetenshantering; (viii) hantera GSK:s IT-produkter, system, nätverk, och kommunikationskanaler, inklusive för att möjliggöra användning av dessa av personal, inklusive hantering av accessrättigheter och godtagbar användning, skapa säkerhetskopior och samla in statistiska data om deras användning; (ix) juridiska aktiviteter och compliancesaktiviteter som innefattar uppfyllnad av lagar, föreskrifter och andra krav som t.ex. lagar och föreskrifter avseende anställning, pensioner och företagshälsovård, avdrag för inkomstskatt och sociala avgifter; uppfyllnad av krav på registerföring och rapportering; genomföra övervakning och rapportering avseende jämställdhet; genomföra revisioner och riskhantering; uppfylla myndighetsinspektioner; svara på juridiska processer, verkställa juridiska rättigheter och ekonomisk kompensation, försvara sig vid rättsliga processer och hantera eventuella interna klagomål eller anspråk; uppfylla interna policyer och procedurer; och övervaka aktiviteter så som tillåtet eller erfordrat enligt lokala lagar; (x) övervaka användning av GSK:s IT-resurser och företagsundersökningar; (xi) hälso-, säkerhets- och skyddsaktiviteter; och (xii) drift av processen Speak Up så att problem kan uppmärksammas eller rapporteras internt.

Våra F&U-aktiviteter: De 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 bindande företagsregler 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 bindande företagsregler för EU täcker inte in överföring av personuppgifter från GSK-företag utanför EES, där de inte skyddas av EU:s dataskyddslagar. Våra bindande företagsregler för Storbritannien täcker inte in överföring av personuppgifter från GSK-företag utanför Storbritannien där de inte skyddas av Storbritanniens dataskyddslagar.

GSK-företag som omfattas av de bindande företagsreglerna: Våra bindande företagsregler är bindande för alla företag i gruppen som har undertecknat det gruppinterna avtalet som anges ovan. GlaxoSmithKline (Ireland) Limited, ett irländskt företag, har det övergripande ansvaret för att säkerställa att övriga företag i gruppen i världen följer de bindande företagsreglerna för EU, inklusive att åtgärda överträdelser av de bindande företagsreglerna för EU. GlaxoSmithKline plc, ett brittiskt företag, har det övergripande ansvaret för att säkerställa att övriga företag i gruppen i världen följer de bindande företagsreglerna för Storbritannien, inklusive att åtgärda överträdelser av de bindande företagsreglerna för Storbritannien.

Våra regler (som återspeglas i vår Privacy Standard)

1. Vi behandlar personuppgifter på ett korrekt och lagenligt sätt

Vi följer gällande lagar som för behandling av personuppgifter. Om dessa bindande företagsregler är i strid med gällande lagar och konflikten kan ha betydande negativa effekter, inklusive eventuella rättsligt bindande krav på utlämnande av personuppgifter av en brottsbekämpande myndighet eller ett statligt säkerhetsorgan, ska detta anmälas till den behöriga tillsynsmyndigheten. Om tillämplig lag förbjuder det berörda koncernföretaget från att göra en sådan anmälan till behörig tillsynsmyndighet, kommer vi att göra vårt bästa för att få ett undantag från detta förbud.

I händelse av att dessa åtgärder inte lyckas kommer koncernföretaget att ge den behöriga tillsynsmyndigheten allmän information avseende de begäranden som har mottagits från sådana myndigheter, inklusive antalet ansökningar om yppande, typen av data som har begärts och, om möjligt, identiteten på det organ som har begärt dem. Uppdateringen sker var 12:e månad.

Under inga omständigheter kommer ett koncernföretag att tillhandahålla personuppgifter till statliga organ i ett land godtyckligt, oproportionerligt eller i stor skala på ett sätt som överskrider vad som är nödvändigt i ett demokratiskt samhälle.

Syfte för behandling: Vi behandlar bara personuppgifter om det finns legitima affärssyften 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

(i) för att uppfylla ett avtal där du är en av parterna eller för att vidta åtgärder på din begäran innan ett avtal ingås
(ii) för att uppfylla våra juridiska skyldigheter
(iii) för att vi ska kunna utföra en uppgift som ligger i allmänhetens intresse
(iv) för att skydda dina väsentliga intressen
(v) för våra eller tredje mans legitima intressen ifall dessa intressen inte åsidosätts av dina egna intressen, rättigheter och friheter.

Känsliga personuppgifter: Vid hantering av känsliga personuppgifter (se ordlistan) vidtas ytterligare skyddsåtgärder. Vi behandlar bara känsliga personuppgifter om

(i) den är nödvändig för att vi ska kunna uppfylla våra juridiska åtaganden och utöva våra juridiska rättigheter enligt arbetslagstiftning
(ii) den här nödvändig för att skydda dina vitala intressen ifall du är fysiskt eller juridiskt oförmögen att ge ditt medgivande
(iii) behandlingen omfattar personuppgifter som du uppenbart själv har offentliggjort
(iv) den är nödvändig för att fastställa, utöva eller försvara rättsanspråk
(v) den är nödvändig på grund av stort allmänintresse
(vi) 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.

Om så krävs enligt lag eller om vi inte kan åberopa någon av ovan nämnda rättsliga grunder för att behandla dina personuppgifter kommer vi att fråga om ditt uttalade samtycke. När vi behandlar känsliga personuppgifter kommer vi endast att göra det om sådant samtycke uttryckligen ges. Om du har givit ett samtycke, kan du när som helst dra tillbaka det. Vänligen kontakta oss såsom beskrivs i våra integritetsmeddelanden, som är tillgängliga här, om du vill dra tillbaka ditt samtycke.

2. Vi samlar in och sparar ett minimum av personuppgifter som krävs för att genomföra specifika, explicita och legitima verksamhetssyften

Vi samlar in och sparar ett minimum av personuppgifter som krävs för att uppfylla ett specificerat, explicit och legitimt verksamhetssyfte. Vi ser till att personuppgifter är adekvata, relevanta och begränsas till vad som är nödvändigt för de syften vi samlar in och/eller behandlar dem. Om vi får kännedom om att personuppgifter är felaktiga, vidtar vi utan dröjsmål alla rimliga åtgärder för att radera eller rätta dem. Om så är möjligt använder vi oss av anonymiserade uppgifter, i stället för personuppgifter, för att uppnå våra syften. Vi säkerställer att personuppgifterna är korrekta och – vid behov – hålls aktuella.

Vi sparar personuppgifter endast så länge som det behövs för att uppnå legitima affärssyften. 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 tillhandahåller information som krävs enligt de lagar som gäller när personuppgifterna insamlas. Vi tillhandahåller åtminstone den information som krävs enligt artikel 13 och 14 i dataskyddsförordningen. Om vi får personuppgifter från tredje man – inte direkt från dig – kan vi (enligt gällande lag) inte tillhandahålla dessa uppgifter till dig om det skulle visa sig vara omöjligt eller innebära en orimlig ansträngning.

Tillämpning av individuella rättigheter: Vi låter dig hävda dina rättigheter enligt dataskyddsförordningen, inklusive rätten att

(i) komma åt dina personuppgifter
(ii) få rättelse av dina personuppgifter
(iii) radera dina personuppgifter
(iv) begränsa eller protestera mot behandlingen av dina personuppgifter
(v) få en kopia av dina personuppgifter överlämnade till dig eller en tredje man
(vi) beslut om dig inte ska fattas automatiskt (se nedan)
(vii) ta tillbaka ditt samtycke
(viii) avstå från att få marknadsföring skickad till dig.

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 juridiska skyldigheter.

Automatiskt beslutsfattande: Vi kan i begränsad utsträckning använda oss av automatiserat beslutsfattande vid behandling av personuppgifter. Vi använder oss av automatiserat beslutsfattande endast om

(i) det krävs för att ingå, eller fullgöra, avtal mellan oss och dig
(ii) det har godkänts enligt EU:s eller medlemsstaternas lagstiftning (avseende bindande företagsregler i EU) eller enligt Storbritanniens lagstiftning (avseende bindande företagsregler i Storbritannien), och de skyddsåtgärder som krävs enligt gällande lag har vidtagits
(iii) du uttryckligen har lämnat ditt samtycke.

Om du vill utöva någon av dina rättigheter, vänligen meddela oss genom att kontakta oss så som beskrivs i vårt integritetsmeddelande. Om du väljer att utöva någon rättighet, kommer vi att försöka ge dig information om de åtgärder vi har vidtagit inom en kalendermånad. Beroende på komplexiteten i din begäran och antalet andra förfrågningar vi behandlar, kan vi behöva ytterligare två månader för att tillhandahålla denna information. Vi meddelar dig om eventuell försening inom en månad från att ha mottagit din begäran.

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

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

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 modern teknik.

Hantering av incidenter och överträdelser: Vi rapporterar personuppgiftsöverträdelser till datatillsynsmyndigheter ifall det är sannolikt att överträdelserna 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 loggar personuppgiftsöverträdelser med detaljer om personuppgiftsöverträdelsen, eventuella effekter för dig och oss eller andra parter samt den åtgärd som vidtagits för att åtgärda överträdelsen. Vi kommer att tillgängliggöra registret för behöriga datatillsynsmyndigheter på begäran.

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

Sekretesshantering för tredje man: Vi lämnar ut personuppgifter utanför vår företagsgrupp 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 företagsgrupp 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: I de fall vi överför personuppgifter internationellt till tredje män i länder där dataskyddslagarna inte ger tillräckligt skydd för personuppgifter, så tillämpar vi godkända standardavtalsklausuler (se här).

Registreringar hos tillsynsmyndigheter: Där så krävs enligt gällande dataskyddslagar i någon medlemsstat eller Storbritannien meddelar vi eller inhämtar godkännande från den relevanta datatillsynsmyndigheten 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 besvärsförfarande och respekterar din rätt till åtgärd

Lämna klagomål till oss: Om du anser att vi inte har följt gällande regler enligt våra bindande företagsregler är du välkommen att vända dig direkt till oss och få ditt klagomål utvärderat enligt vår interna process för att åtgärda klagomål. Vi uppmuntrar dig att lämna in klagomål på personuppgiftsbehandling via vår Speak Up-linje.

HR-aktiviteter: Anställda och andra enskilda individer vars uppgifter behandlas i samband med HR-aktiviteter kan lämna in klagomål på personuppgiftsbehandling till sin närmaste chef (gäller GSK-medarbetare), den compliance-ansvarige i landet, en lokal HR-representant eller ett juridiskt ombud eller den regionala motsvarigheten för någon av dessa. Alla kommer att rapportera klagomålet om personuppgiftsbehandlingen till ”Speak Up” systemet, vilket i sin tur vidarebefordrar klagomålet till affärsenhetens compliance-grupp och Privacy Center of Excellence. Dessa bedömer självständigt vilka åtgärder som bör vidtas som svar på ditt klagomål.

F&U-aktiviteter: Personer vars personuppgifter behandlas i samband med F&U-aktiviteter: Om du är en forskningsperson (se ordlistan) bör du kontakta klinikern eller forskaren som genomför studien. Han eller hon vidarebefordrar klagomålet till Privacy Center of Excellence. 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 klagomålet om personuppgiftsbehandlingen till GSK:s klagomålskanal. De bedömer självständigt vilka åtgärder som bör vidtas som svar på ditt klagomål.

Eskalering: Oavsett varifrån vi får klagomål om personuppgiftsbehandling kommer de – om de inte kan åtgärdas – att eskaleras (i) till GSK:s Country Privacy Advisor vars kontaktuppgifter publiceras på vår webbplats här eller (ii) därefter till GSK:s EU/Storbritannien-dataskyddsombud på EU.DPO@GSK.com. EU/Storbritannien-dataskyddsombudet är den sista möjligheten inom GSK för att åtgärda ett klagomål på våra bindande affärsregler. 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 vi når efter högst två månader därefter. Om du vill kan du kontakta vårt EU/Storbritannien-dataskyddsombud direkt.

Lämna in ett klagomål till en datatillsynsmyndighet eller domstol: Du kan lämna in ett klagomål avseende våra bindande företagsregler för EU till någon av följande: (i) den behöriga datatillsynsmyndigheten i det land där du är bosatt, arbetar eller där den påstådda överträdelsen skedde, (ii) den irländska dataskyddskommissionären eller en domstol i Irland (där GlaxoSmithKline (Ireland) Limited har sitt säte), (iii) domstolarna i det EES-land varifrån personuppgifterna överfördes av oss eller (d) domstolarna i det EES-land där du bosatt. Du kan lämna in ett klagomål avseende våra bindande företagsregler för Storbritannien till Storbritanniens informationskommissionär eller till domstolarna i England och Wales (där GlaxoKlineSmith plc har sitt säte). Att följa våra interna förfaranden för klagomål kommer inte på

något sätt att påverka din rätt att använda dessa möjligheter.

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 en av eller båda våra bindande företagsregler för EU och Storbritannien behöver vi bevisa att de relevanta bindande företagsreglerna inte har överträtts. Om en datatillsynsmyndighet ger ett föreläggande till ett GSK-företag utanför EES avseende våra bindande företagsregler för EU, och GSK-företaget av något skäl är oförmöget eller ovilligt att ersätta skadorna eller följa föreläggandet inom en eventuell respittid, så kommer GlaxoSmithKline (Ireland) Limited att betala skadeståndet direkt till dig eller se till att det aktuella GSK-företaget följer föreläggandet. Om Storbritanniens informationskommissionär eller domstolarna i England och Wales ger ett föreläggande till ett GSK-företag utanför Storbritannien avseende våra bindande företagsregler för Storbritannien, och GSK-företaget av något skäl är oförmöget eller ovilligt att ersätta skadorna eller följa föreläggandet inom en eventuell respittid, så kommer GlaxoSmithKline plc att betala skadeståndet direkt till dig eller se till att det aktuella GSK-företaget följer föreläggandet.

Ordlista

”Anonyma uppgifter” är uppgifter som har gjorts anonyma på ett sådant sätt att individen inte längre identifieras eller kan identifieras.
”Extern forskare” avser läkare eller annan hälso- eller sjukvårdspersonal som deltar eller kan delta i F&U.
”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.
”Personuppgift” är en uppgift som rör en identifierad eller identifierbar individ.
”Känsliga personuppgifter” 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.
”Visstidsanställd” avser en individ 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.

[December 2020]