Offentligt uttalande om 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)** i syfte att få internationella överföringar av personuppgifter inom företagsgruppen att följa EU:s dataskyddsregler, i synnerhet dataskyddsförordningen (förordning 2016/679) **(GDPR).**

Vad är bindande företagsregler?

Våra bindande företagsregler omfattar ett antal dokument, bland annat standarden och policyer för sekretess, ett avtal mellan företagen inom GSK-företag i gruppen och det här offentliga uttalandet. De kompletteras med utbildning och revisioner. Det här offentliga uttalandet är avsett att beskriva de bindande företagsreglerna och se till att berörda individer vars personuppgifter vi behandlar i samband med våra HR- och F&U-aktiviteter **(du)** är medvetna om sina rättigheter enligt våra bindande företagsregler och rättigheterna kan utövas.

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

Omfattningen av våra bindande företagsregler

De bindande företagsreglerna 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 brittiska eller andra 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, Storbritannien, Sverige, Tjeckien, Tyskland, Ungern och Österrike.

Våra HR-aktiviteter: omfattar administration och ledning av vår personal; rekryterings- och urvalsaktiviteter; inledande av anställningsförhållande; administration av lön och förmåner; utbildning, utveckling och prestationer; hantering av disciplin- och klagomålsärenden; kommunikation med medarbetare och givande av referenser; kommunikation med medarbetare i akuta situationer; drift av processen Speak Up så att problem kan uppmärksammas eller rapporteras internt; underhåll av affärsverksamhet och säkerställande att medarbetarna kan komma åt system och utföra sina arbetsuppgifter; kontroll och övervakning av medarbetarkommunikation; efterlevnad till juridiska, regulatoriska och andra krav som gäller för oss, inklusive de som beror på lagstiftning rörande moms, hälsa och säkerhet, antidiskriminering, datasekretess, anställnings- och immigrationslagar och -förordningar, arkiverings- och rapporteringsansvar, revisionsansvar och myndighetsinspektioner; och svar i juridiska processer, utövande av lagstadgade rättigheter och rättsmedel, försvar i rättstvister och hantering av interna klagomål eller anspråk. Personuppgifterna som bearbetas omfattar information som rör nuvarande, tidigare eller blivande anställda på GSK eller visstidsanställda (se ordlistan) samt äkta makar och underhållsberättigade personer i förekommande fall.

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. De täcker

inte in överföring av personuppgifter från GSK-företag utanför EES, där de inte skyddas av brittiska lagar eller EU-lagar.

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 plc, ett brittiskt företag, har det övergripande ansvaret för att säkerställa att övriga företag i gruppen i världen följer de bindande företagsreglerna, inklusive att åtgärda överträdelser av dessa regler.

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 konflikt med gällande lagar och konflikten kan ha betydande negativa effekter så ska situationen rapporteras till dataskyddsmyndigheten.

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.

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

(i) den är nödvändig för att vi ska kunna uppfylla våra juridiska åtaganden och utöva våra juridiska rättigheter enligt anställningslagarna
(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.

Vi kommer att söka ditt otvetydiga samtycke till att behandla personuppgifter och uppgifter av särskild kategori om så krävs enligt lag eller om vi inte kan åberopa någon av ovan nämnda rättsliga grunder.

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

Vi samlar in och sparar ett minimum av personuppgifter som krävs för att uppfylla varje legitimt verksamhetssyfte. Vi ser till att personuppgifter är adekvata, relevanta och inte mer omfattande än nödvändigt för de syften i vilka vi samlar in och/eller behandlar 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 för dig om det skulle visa sig vara omöjligt eller innebära en orimlig ansträngning.

Tillämpning av individuella rättigheter: Vi låter dig tillvarata 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 upphöra med behandlingen av dina personuppgifter
(v) få en kopia av dina personuppgifter överlämnade till dig eller en tredje man
(vi) inte beslut om dig 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).

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 och de skyddsåtgärder som krävs enligt gällande lag har vidtagits
(iii) du uttryckligen har lämnat ditt samtycke.

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 legitima affärssyftet i 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 moderna tekniker.

Hantering av incidenter och överträdelser: Vi rapporterar personuppgiftsöverträdelser till dataskyddsmyndigheter 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 på dig och oss eller andra parter samt den åtgärd som vidtagits för att åtgärda överträdelsen. Vi kommer att tillgängliggöra registret för behöriga dataskyddsmyndigheter 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 utanför EES där dataskyddslagarna inte ger tillräckligt skydd för personuppgifter, så tillämpar vi godkända standardavtalsklausuler (se här) eller använder andra lagenliga undantag för överföring av personuppgifterna.

Registreringar hos tillsynsmyndigheter: Där så krävs enligt gällande dataskyddslagar i någon medlemsstat meddelar vi eller inhämtar godkännande från den relevanta dataskyddsmyndigheten 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 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 Privacy Center of Excellence. De 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 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 – 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-dataskyddsombud på EU.DPO@GSK.com. EU:s dataskyddsombud 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-dataskyddsombud direkt.

Lämna in ett klagomål till en dataskyddsmyndighet eller domstol: Du kan lämna in ett klagomål till någon av följande: (i) den behöriga dataskyddsmyndigheten i det land där du huvudsakligen är bosatt, arbetar eller där den påstådda överträdelsen skedde, (ii) den behöriga tillsynsmyndigheten eller en domstol i Storbritannien (där GlaxoSmithKline plc har sitt säte), (iii) domstolarna i det EES-land varifrån personuppgifterna överfördes av oss

eller (d) domstolarna i det EES-land där du huvudsakligen är bosatt. 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 våra bindande företagsregler behöver vi bevisa att våra bindande företagsregler inte har överträtts. Om en dataskyddsmyndighet ger ett föreläggande till ett GSK-företag utanför EES, 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.

”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.

”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.

[Juni 2018]

.