

Offentlig erklæring om GSK's bindende selskabsregler

Introduktion

GSK's (**vi, os, vores**) aktiviteter inden for Human Resources (**HR**) samt forskning og udvikling (**R&D**) involverer behandlingen af "personlige oplysninger" (se ordlisten), herunder overførsel af disse personlige oplysninger til andre lande. Vi har forpligtet os til at holde en høj integritetsstandard i håndteringen af personlige oplysninger, og vi har implementeret bindende selskabsregler for at kunne foretage internationale overførsler af personlige oplysninger mellem vores koncernforbundne selskaber i henhold til EU's databeskyttelseslovgivning, især den generelle databeskyttelsesforordning (forordning 2016/679) (**GDPR**).

Hvad er bindende selskabsregler?

Vores bindende selskabsregler omfatter en række dokumenter, herunder vores (Privacy Standard) standard for beskyttelse af personoplysninger og vores privatlivspolitik, en intern koncernaftale mellem GSK-selskaber samt denne offentlige erklæring. De understøttes af uddannelse og inspektioner. Denne offentlige erklæring er udfærdiget for at forklare de bindende selskabsregler og sikre, at personer, hvis personlige oplysninger vi behandler i forbindelse med vores HR-aktiviteter samt forskning og udvikling (**du**), er klar over deres rettigheder i henhold til de bindende selskabsregler og ved, hvordan de udøver disse rettigheder.

Der findes en ordliste over termer, der bruges i dette dokument, i slutningen af dokumentet. Hvis du skal bruge flere oplysninger, kan du få fat i en kopi af vores bindende selskabsregler ved at kontakte vores databeskyttelsesansvarlige for EU her: EU.DPO@GSK.com.

Omfanget af vores bindende selskabsregler

De bindende selskabsregler gælder for dine personlige oplysninger, der indsamles i forbindelse med vores aktiviteter inden for HR samt forskning og udvikling, hvilket er yderligere beskrevet nedenfor, hvor de overføres til andre lande af et GSK-selskab, der er underlagt databeskyttelseslovgivningen i Storbritannien eller EU, i de godkendte EU-lande, til et land uden for EØS (Det Europæiske Økonomiske Samarbejdsområde), hvor lovgivningen ikke yder tilstrækkelig beskyttelse af personlige oplysninger.

EU-lande, hvor der er indhentet godkendelse: GSK har opnået godkendelse af vores bindende selskabsregler i: Belgien, Bulgarien, Cypern, Danmark, Estland, Finland, Frankrig, Grækenland, Holland, Irland, Island, Italien, Kroatien, Letland, Litauen, Luxembourg, Malta, Norge, Polen, Portugal, Rumænien (kun R&D), Schweiz, Slovakiet, Slovenien, Spanien, Storbritannien, Sverige, Tjekkiet, Tyskland, Ungarn og Østrig.

Vores HR-aktiviteter: Disse omfatter administration og håndtering af vores medarbejdere, rekrutterings- og screeningaktiviteter, indtrædelse i et ansættelsesforhold, administration af løn og personalegoder, uddannelse, udvikling og medarbejdervurdering, håndtering af disciplinærsager og klager, kommunikation med medarbejdere og indhentning af referencer, kommunikation med medarbejdere i nødstilfælde, rapportering af (alvorlige) forseelser eller mistanke herom t ([Speak Up](#)), vedligeholdelse af forretningsprocesser og sikring af, at medarbejderne kan få adgang til systemerne og udføre deres opgaver, screening og overvågning af medarbejderkommunikation, overholdelse af juridiske, regulatoriske og øvrige krav, som er gældende for GSK, inklusive krav i henhold til love og bestemmelser inden for skat, sundhed og sikkerhed, bekæmpelse af forskelsbehandling, databeskyttelse, ansættelse og immigration samt registrerings- og rapporteringskrav, revisionskrav samt offentlige tilsyn, og svar på retslige procedurer, håndhævelse af juridiske rettigheder og retsmidler, sagsanlæg og håndtering af interne klager eller krav. De behandlede personlige oplysninger omfatter oplysninger om nuværende, tidligere eller potentielle GSK-medarbejdere eller løst ansatte (se ordliste) samt ægtefæller og familiemedlemmer i relevant omfang.

Vores aktiviteter inden for forskning og udvikling: Disse omfatter interventionelle og ikke-interventionelle kliniske forsøg, der er helt eller delvist igangsat, styret eller finansieret af os, og relateret overholdelse af lovgivningen som f.eks. sikkerhedsovervågning og rapportering af uønskede hændelser. De behandlede personlige oplysninger omfatter oplysninger om eksterne forskere og forskningspersoner (se ordliste).

Uden for omfanget: Vores bindende selskabsregler omfatter ikke behandling og overførsel af personlige oplysninger fra vores kommercielle divisioner (f.eks. personlige oplysninger om kunder eller enkeltpersoner, der er knyttet til

leverandører til vores kommercielle divisioner). Disse oplysninger er beskyttet i henhold til forskellige retsgyldige mekanismer. De dækker ikke overførsler af personlige oplysninger fra GSK-selskaber uden for EØS, hvor de ikke er underlagt databeskyttelseslovgivningen i Storbritannien eller EU.

GSK-selskaber, der er dækket af de bindende selskabsregler: Vores bindende selskabsregler er bindende for alle vores koncernforbundne selskaber, der har underskrevet ovennævnte interne koncerntaftale. GlaxoSmithKline plc, der er en virksomhed registreret i Storbritannien, har det overordnede ansvar for at sikre, at andre koncernselskaber rundt omkring i verden overholder de bindende selskabsregler, herunder afhjælpning af overtrædelser af de bindende selskabsregler.

Vores regler (som afspejles i vores standard for beskyttelse af personoplysninger)

1. Vi behandler personlige oplysninger retfærdigt og i henhold til lovgivningen

Vi overholder den gældende lovgivning vedrørende behandling af personlige oplysninger. I tilfælde af en konflikt mellem disse bindende selskabsregler og den gældende lovgivning, hvor konflikten forventes at have en markant negativ effekt, skal dette rapporteres til databeskyttelsesmyndigheden.

Årsag til behandling: Vi behandler kun personlige oplysninger, hvis vi har et legitimt forretningsmæssigt formål med det, og hvis behandlingen er nødvendig i forhold til dette formål. Al behandling sker med et relevant retsgrundlag i henhold til GDPR.

Retsgrundlag for behandling: vi bruger følgende retsgrundlag til at behandle personlige oplysninger. Behandlingen skal være nødvendig:

- (i) i forhold til at opfylde en kontrakt, som du er part i, eller for at udføre handlinger på din opfordring før indgåelse af en kontrakt
- (ii) for at kunne opfylde vores juridiske forpligtelser
- (iii) for at vi kan udføre en opgave, der gennemføres i offentlighedens interesse
- (iv) for at beskytte dine vitale interesser eller
- (v) i forhold til legitime interesser, der varetages af os eller tredjepart under forudsætning af, at disse interesser ikke tilsidesættes af personens egne interesser, rettigheder og friheder.

Særlige kategorioplysninger: På grund af "særlige kategorioplysningers" (se ordliste) karakteristika er der ekstra sikkerhedsforanstaltninger, der er gældende. Vi behandler kun særlige kategorioplysninger, hvor:

- (i) det er nødvendigt, for at vi kan overholde vores juridiske forpligtelser og udøve vores juridiske rettigheder i henhold til ansættelseslovgivningen
- (ii) det er nødvendigt for at beskytte dine vitale interesser, hvis du fysisk eller juridisk ikke er i stand til at give samtykke
- (iii) behandlingen involverer personoplysninger, der åbenlyst er gjort offentlige af dig
- (iv) det er nødvendigt for at kunne etablere, udøve eller forsvare erstatningskrav
- (v) det er nødvendigt af grunde, der i væsentligt omfang er i offentlighedens interesse eller
- (vi) det er relevant med hensyn til præventiv medicin eller arbejdsmedicin, vurdering af arbejdsevnen hos en af GSK's medarbejdere, medicinsk diagnose, forsyning af sundhedspleje eller social omsorg eller behandling eller administration af sundhedssystemer og -tjenester samt sociale systemer og tjenester, enten i henhold til gældende lovgivning eller i henhold til en kontrakt med sundhedsfagligt personale. Under disse omstændigheder forestås behandlingen af en sundhedsfaglig person, der har professionel tavshedspligt, eller af en anden person, der har en passende tavshedspligt.

Vi indhenter kun dit utvetydige samtykke til at behandle personlige oplysninger og særlige kategorioplysninger, hvis dette er et lovkrav, eller hvis vi ikke kan anvende et af ovennævnte retsgrundlag.

2. Vi indsamler og opbevarer den minimale mængde personlige oplysninger, der er nødvendig for at kunne varetage specifikke og legitime forretningsformål

Vi indsamler den minimale mængde personlige oplysninger, der er nødvendig for at kunne varetage hvert enkelt legitimt forretningsformål. Vi sikrer, at de personlige oplysninger er tilstrækkelige, relevante og ikke for

omfangsrige i forhold til de formål, vi indsamler og/eller derefter behandler dem til. Hvis det er muligt, bruger vi anonymiserede oplysninger i stedet for at bruge personlige oplysninger til at opfylde det mål, de er indsamlet til. Vi sørger for, at personlige oplysninger er nøjagtige og holdes opdaterede i nødvendigt omfang.

Vi opbevarer kun personlige oplysninger i det nødvendige tidsrum i forhold til legitime forretningsmæssige formål. Derefter sletter, destruerer eller anonymiserer vi de personlige oplysninger.

3. Vi forklarer, hvordan personlige oplysninger bliver brugt, og gør opmærksom på dine rettigheder

Åbenhed: Vi er åbne omkring vores behandling af personlige oplysninger. Vi giver de oplysninger, der kræves i henhold til gældende lovgivning, på det tidspunkt, hvor de personlige oplysninger indsamles. Vi angiver som minimum de oplysninger, som er mindstegrænsen ifølge kravene i artikel 13 og 14 i GDPR. Når vi indsamler personlige oplysninger fra tredjepart i stedet for direkte fra dig, må vi (i henhold til den gældende lovgivning) ikke stille disse oplysninger til rådighed for dig, hvis dette vil være umuligt eller kræve en uforholdsmæssigt stor indsats.

Administration af individuelle rettigheder: Vi giver dig mulighed for at udøve rettigheder i henhold til GDPR, inklusive retten:

- (i) til at få adgang til dine personlige oplysninger
- (ii) til at rette dine personlige oplysninger
- (iii) til at slette dine personlige oplysninger
- (iv) til at begrænse eller stoppe behandlingen af dine personlige oplysninger
- (v) til at stille en kopi af dine personlige oplysninger til rådighed for dig eller en tredjepart
- (vi) til ikke at foretage automatiserede afgørelser om dig (se nedenfor)
- (vii) til at trække dit samtykke tilbage og
- (viii) til at fravælge at modtage markedsføringshenvendelser.

Vi overholder også den gældende lovgivning i de lande, der giver dig andre rettigheder med hensyn til dine personlige oplysninger. Vi kan begrænse din ret til at få adgang til dine personlige oplysninger for at beskytte andre (f.eks. en anden persons ret til privatliv).

Automatiserede afgørelser: Vi gør begrænset brug af automatiserede beslutningstagningsprocedurer i forbindelse med behandling af personlige oplysninger. Vi bruger kun automatiseret beslutningstagningsprocedurer, hvis:

- (i) det er nødvendigt for at indgå eller håndhæve en kontrakt mellem os og dig
- (ii) det er godkendt i henhold til en specifik lov i EU eller et medlemsland, og de sikkerhedsforanstaltninger, som den pågældende lov kræver implementeret, er blevet implementeret eller
- (iii) du har givet udtrykkeligt samtykke.

4. Vi bruger ikke personlige oplysninger til yderligere formål, der ikke er kompatible med det formål, de oprindeligt blev indsamlet til.

Begrænsning af formål: Vi behandler kun personlige oplysninger på en måde, der er kompatibel med det legitime forretningsformål, de oprindeligt blev indsamlet til. Vi underretter dig om eventuelle nye formål med at behandle dine personlige oplysninger.

5. Vi bruger passende sikkerhedsforanstaltninger

Beskyttelse af dit privatliv: Vi implementerer passende tekniske og organisatoriske sikkerhedsforanstaltninger for at forhindre utilsigtet eller ulovlig destruktion, tab, ændring, uautoriseret videregivelse af eller adgang til personlige oplysninger. Disse foranstaltninger er passende i forhold til de risici, der er forbundet med at bruge personlige oplysninger og implementere moderne teknologier.

Håndtering af hændelser og sikkerhedsbrud: Vi underretter databeskyttelsesmyndighederne om sikkerhedsbrud på personlige data, medmindre det er usandsynligt, at disse brud udgør en risiko med hensyn til dine rettigheder og friheder. Vi underretter dig om et sikkerhedsbrud på personlige data, hvis det er sandsynligt, at et sådant sikkerhedsbrud fører til høj risiko for dine rettigheder og friheder samt (efter vores skøn) under visse andre

omstændigheder. Vi vedligeholder en optegnelse over sikkerhedsbrud på personlige data, der indeholder oplysninger om det enkelte sikkerhedsbrud på de personlige data, de eventuelle følgevirkninger på dig, på os selv eller på eventuelle andre parter samt de afhjælpende handlinger, der er udført for at rette op på sikkerhedsbruddet. Vi stiller disse optegnelser til rådighed for kompetente databeskyttelsesmyndigheder på opfordring.

6. Vi kontrollerer omhyggeligt videregivelsen af personlige oplysninger til tredjepart

Tredjeparts beskyttelse af personlige oplysninger: Vi videregiver personlige oplysninger til tredjeparter uden for vores concernforbundne selskaber, hvis der er lovkrav herom i forbindelse med retssager samt under andre begrænsede og retsgyldige omstændigheder. Vi kan også overføre personlige oplysninger til parter uden for vores concernforbundne selskaber til: (a) tredjeparter, der handler på vores vegne, herunder leverandører; eller (b) andre uafhængige tredjeparter, f.eks. forskningspartnere og kommercielle partnere eller kontrolorganer.

I det omfang vi bruger tredjeparter til at behandle personlige oplysninger på vores vegne, etablerer vi passende kontraktmæssige, organisatoriske og operationelle kontroller med dem for at sikre dine personlige oplysningers anonymitet og sikkerhed. Vi kræver, at disse tredjeparter accepterer alle forskrifter i artikel 28 i GDPR. Hvis vi finder ud af, at en tredjepart behandler personlige oplysninger på en måde, der ikke lever op til de krav, der stilles fra vores side eller i den gældende lovgivning, tager vi alle rimelige skridt for at sikre, at disse mangler adresseres så hurtigt som muligt.

Videreoverførsler til tredjeparter: Hvis vi overfører personlige oplysninger på tværs af landegrænser til tredjeparter, der befinder sig i lande uden for EØS, hvor databeskyttelseslovgivningen ikke yder tilstrækkelig beskyttelse af personlige oplysninger, implementerer vi godkendte standardkontraktklausuler, hvis detaljer kan ses [her](#), eller bruger en anden retsgyldig undtagelse til at overføre de personlige oplysninger.

Regulatoriske indberetninger: Hvis der er krav herom i henhold til den gældende databeskyttelseslovgivning i et medlemsland, underretter vi eller indhenter godkendelse fra den relevante databeskyttelsesmyndighed med hensyn til behandling af personlige oplysninger (inklusive internationale overførsler af personlige oplysninger) og sikrer, at underretningerne eller indberetningerne til godkendelse ajourføres i tilfælde af ændringer.

7. Vi har en klageprocedure og respekterer din ret til at få afhjulpet en fejl

Indgivelse af en klage til os: Hvis du mener, at vi ikke har overholdt de regler, der er anført i vores bindende selskabsregler, har du mulighed for at gøre indsigelser direkte til os og få vurderet din klage som led i vores interne klageprocedure. Vi opfordrer dig til at anmelde klager vedrørende anonymitet via vores [Speak Up-tjeneste](#).

HR-aktiviteter: I forbindelse med medarbejdere og andre personer, hvis oplysninger bliver behandlet som led i HR-aktiviteter, kan en anonymitetsklage blive registreret hos din leder (for GSK-medarbejdere), en compliance officer på landeniveau, en lokal HR-ansvarlig eller juridisk ansvarlig eller det regionale modstykke til nogen af disse, som alle anmelder anonymitetsklagen via klageinstansen, og herved videresendes klagen til forretningsenhedens compliance-team og Privacy Centre of Excellence. De foretager en uafhængig vurdering af det passende handlingsforløb som reaktion på din klage.

Aktiviteter inden for forskning og udvikling: For personer, hvis personlige oplysninger bliver behandlet som led i aktiviteter inden for forskning og udvikling: Hvis du er forskningsperson (se ordliste), skal du kontakte den kliniker eller forsker, der udfører undersøgelsen, og som kan videresende klagen til vores Privacy Centre of Excellence. Hvis du er ekstern forsker (se ordliste), kan en anonymitetsklage registreres hos GSK's compliance officer på landeniveau eller juridisk ansvarlige eller det regionale modstykke, som alle anmelder anonymitetsklagen via klageinstansen i GSK. De foretager en uafhængig vurdering af det passende handlingsforløb som reaktion på din klage.

Eskalering: Uanset hvor vi modtager klager om dataanonymitet, bliver de eskaleret på følgende måde, hvis de ikke kan løses: (i) til en databeskyttelsesrådgiver på landeniveau i GSK, hvis kontaktoplysninger er offentliggjort på vores website her; eller (ii) derefter til GSK's databeskyttelsesansvarlige for EU på EU.DPO@GSK.com. Den databeskyttelsesansvarlige for EU er den sidste instans i GSK-regi i forhold til løsning af klager i forbindelse

med vores bindende selskabsregler. Vi bestræber os på at løse klager hurtigt, og GSK vil – medmindre usædvanlige omstændigheder gør sig gældende – kontakte dig skriftligt inden for en måned. Denne skrivelse vil enten: (a) indikere vores holdning vedrørende klagen og eventuelle handlinger, vi har foretaget eller vil foretage som reaktion på klagen; eller (b) anføre, hvornår du vil blive underrettet om vores holdning, hvilket senest vil ske to måneder derefter. Du kan kontakte vores databeskyttelsesansvarlige for EU, hvis du ønsker det.

Indgivelse af en klage til en databeskyttelsesmyndighed eller til en domstol: Du kan indgive en klage til en hvilken som helst af følgende: (i) den kompetente databeskyttelsesmyndighed i det land, hvor du har primær bopæl eller arbejder, eller hvor det påståede sikkerhedsbrud fandt sted; (ii) informationskommisæreren i Storbritannien eller de kompetente domstole i Storbritannien (hvor GlaxoSmithKline plc har hovedkontor); (iii) domstolene i det EØS-land, som dine personlige oplysninger er blevet overført fra af os; og (iv) domstolene i det EØS-land, hvor du har primær bopæl. Hvis vores interne klageprocedure følges, går det på ingen måde ud over din ret til at gøre brug af nogen af disse muligheder.

Hvis du indgiver en klage og kan påvise, at du har lidt materiel eller ikke-materiel skade, der med al sandsynlighed er opstået som følge af en overtrædelse af de bindende selskabsregler, skal vi bevise, at der ikke har været nogen overtrædelse af vores bindende selskabsregler. Hvis en databeskyttelsesmyndighed eller domstol afsiger en kendelse mod et GSK-selskab uden for EØS, og GSK-selskabet af en hvilken som helst årsag ikke kan eller vil betale bøden eller overholde kendelsen inden for den gældende tidsfrist, skal GlaxoSmithKline plc betale den sum, som du er blevet tilkendt, direkte eller sikre, at det relevante GSK-selskab overholder den relevante kendelse.

Ordliste

"Anonymiserede oplysninger" henviser til personlige oplysninger, der er gjort anonyme på en sådan måde, at det ikke længere er muligt at identificere en person.

"Ekstern forsker" refererer til eksterne læger eller andet sundhedsfagligt personale, der deltager eller potentielt kan deltage i forskning og udvikling.

"Forskningsperson" refererer til kandidater til eller personer, der deltager i forskningsaktiviteter, eller personer, der benytter vores produkter eller behandlinger, og hvis personlige oplysninger bliver behandlet af os i forbindelse med lægemiddelovervågning. Forskningspersoner inkluderer deltagere, der både har eksterne og interne roller i GSK.

"Løst ansat" forstås i GSK-regi som en person, der ikke er GSK-medarbejder, og som leverer tjenester for eller på vegne af GSK, herunder løst ansatte på virksomhedens område eller udenfor, professionelle konsulenter, midlertidigt personale, leverandører og serviceleverandører.

"Personlige oplysninger" refererer til oplysninger, der er relateret til en identificeret eller identificerbar person.

"Særlige kategorioplysninger" refererer til et undersæt af personlige oplysninger relateret til en persons race eller etnicitet, politiske synspunkter, religiøse eller filosofiske overbevisninger, medlemskab af fagforening, genetiske data, biometriske data, der er behandlet for at kunne foretage entydig identifikation af en fysisk person, oplysninger om helbred eller oplysninger om en fysisk persons sexliv eller seksuelle observans.

[Juni 2018]