Fördjupad kontroll

Personuppgiftsbiträdesavtal

Bakgrund

Den fördjupade kontrollen av personuppgiftsbiträdesavtalen syftar till att se om organisationen uppfyller kraven i artikel 28.3 dataskyddsförordningen att relationen mellan personuppgiftsansvarig och personuppgiftsbiträde ska regleras skriftligen. Kontrollen har genomförts i två delar, del ett har bestått av ett antal frågor som besvarats av organisationen och del två har bestått av att dataskyddsombudet slumpvis valt ut tre avtal och kontrollerat om dessa uppfyller kraven.

Iakttagelser från kontrollen

Del 1

Boplats har bifogat en lista med de aktörer som de har identifierat som personuppgiftsbiträden. Till alla de angivna aktörerna finns det upprättade personuppgiftsbiträdesavtal, som också har bifogats till dataskyddsombudet. Av de presenterade svaren gör dataskyddsombudet bedömningen att Boplats inte har en framtagen rutin för att hantera personuppgiftsbiträden och tillhörande avtal. Bolaget har inte heller särskilt många personuppgiftsbiträden vilket kan vara anledningen till att man inte prioriterat att ta fram någon rutin för ändamålet. Att ha en rutin kan underlätta för bolaget att se till så att alla krav enligt förordningen säkerställs i avtalsförhållandet. Underlaget som presenterats för dataskyddsombudet visar inte på vilket sätt bolaget säkerställer så att kraven på personuppgiftsbiträdesavtal enligt förordningen uppfylls.

Bolaget uppger att de till tre av fyra aktörer har lämnat instruktioner enligt artikel 28.3 i dataskyddsförordningen. Syftet med instruktioner är att säkerställa så att det är den personuppgiftsansvarige, och inte personuppgiftsbiträdet, som bestämmer vad som sker med personuppgifterna. Det innebär att om personuppgiftsbiträdet agerar utanför instruktionerna genom att själv bestämma ändamål och medel, kan biträdet istället ses som ansvarig och åläggas samma ansvar som en personuppgiftsansvarig. Instruktionerna kan följas direkt av avtalet eller ges skriftligen på annat sätt, men måste sparas så att de finns dokumenterade. Kravet enligt artikel 28.3 är att det i personuppgiftsbiträdesavtalet ska framgå att personuppgiftsbiträdet enbart får behandla personuppgifter på dokumenterade instruktioner från personuppgiftsansvarige, vilket har uppfyllts i de angivna avtalen. Däremot kan dataskyddsombudet inte hitta några ytterligare instruktioner om vad behandlingen egentligen innebär. Därmed vill dataskyddsombudet uppmärksamma bolaget på att det finns risker med att inte tydligt instruera biträdena hur personuppgiftsbehandlingen ska behandlas, eftersom det då inte är lika tydligt när personuppgifterna behandlas felaktigt.

Vidare uppger bolaget att det inte finns någon särskild rutin för att avgöra om en leverantör anses vara personuppgiftsbiträde, men att frågor rörande personuppgiftsbehandling ska hanteras av ansvarig chef vid införande, förändring eller avveckling av process eller informationssystem i enlighet med den därtill hörande

rutinen. I övrigt så konsulterar Boplats sitt dataskyddsombud eller vid behov externa jurister för att göra bedömningen huruvida en aktör ska ses som ett personuppgiftsbiträde. Dataskyddsombudet vill i sammanhanget påpeka att bolaget som personuppgiftsansvarig har en skyldighet för behandlingen i alla led och även för det som utförs av biträdena, således ligger det i bolagets intresse att ha kontroll över vad som föreskrivs i avtalen.

Boplats saknar rutin för att säkerställa och följa upp att personuppgiftsbiträdena uppfyller de garantier som lämnats avseende tekniska och organisatoriska åtgärder, men hänvisar till att det skrivs in i själva avtalen istället. Bolaget har i avtalen lagt in klausuler om tester och kontroller för att säkerställa detta. Det är positivt att bolaget är måna om att säkerställa kontroll av lämnade garantier i avtalet, då det också gör att biträdet är medveten om hur kontroller sker och vad som kontrolleras. Det behövs inte en separat rutin så länge bolaget har kontroll över att detta sker vid varje avtalstecknande. I avtalen skrivs det också in vad som sker när tjänsten avslutas, därför finns ingen generell rutin utan det beror på avtal. Samma sak gäller här, att så länge det skrivs in i varje avtal så kan bolaget säkerställa att man vet vad man gör när ett avtal avslutas.

Bolaget har inte heller någon rutin eller arbetssätt för att säkerställa att personuppgiftsbiträdesavtalen är aktuella och uppdaterade vilket är en förutsättning för att kunna efterleva dataskyddsförordningen, precis som ovanstående iakttagelse. Däremot framkommer det i alla avtal vad som ska ske när tjänsten avslutas, vilket är positivt. Det kan också noteras att om en tjänst avslutas ska den leverantören inte längre ha personuppgifterna hos sig utan personuppgiftsansvarige måste då ha kontroll över vad som händer med uppgifterna.

Dataskyddsombudet konstaterar att det även saknas rutin för att säkerställa att avtalen tecknas i behörig ordning, utan att man vid behov hör med dataskyddsombud, konsult eller annan för att avgöra detta. Bolaget uppger efter kontroll att det är VD som är behörig att teckna personuppgiftsbiträdesavtal. Det kan vara av betydelse för bolaget att ha beslutat vem inom organisationen det är som får ingå personuppgiftsbiträdesavtal, så att inga obehöriga gör det, samt att dokumentera detta. Det är därför också av vikt att avtalet föregåtts av en kontroll av insatta medarbetare för att säkerställa att innehållet i avtalet är lämpat för personuppgiftsbehandlingen och att sådan kontroll eller genomläsning förmedlas till VD.

Del 2

Dataskyddsombudets stickprovskontroll har omfattat följande tre avtal: Altiva AB, Oops AB och PIN Sweden AB. Utifrån de minimikrav som anges i artikel 28.3 har dataskyddsombudet enbart kontrollerat så att dessa uppfylls.

- Altiva AB: Inga större avvikelser noterade. Dataskyddsombudet saknar särskilda instruktioner som Boplats uppger finns till avtalet. Under punkten som anger att biträdet ska bistå den personuppgiftsansvariga i fråga om dennes skyldigheter enligt artikel 32-36 saknas information gällande hantering av incidenter, information till registrerade om incidenter, konsekvensbedömning samt förhandssamråd. Vidare framkommer det inte hur biträdet uppfyller sina skyldigheter att kunna vidta åtgärder för att bistå personuppgiftsansvarige att svara på begäran från de registrerade att utöva sina rättigheter enligt kapitel 3

Dataskyddsförordningen, utöver i förhållande till registerutdrag och rättelse. Det saknas alltså information om vad som gäller angående de andra rättigheterna. Slutligen framkommer att personuppgiftsansvarige har möjlighet att utföra kontroller, men på egen bekostnad. Biträdet har en skyldighet att enligt förordningen gå med på och bistå vid granskning och inspektioner. Eftersom avtalet är ifrån 2016 och innan dataskyddsförordningen trädde i kraft, kan det vara av värde för bolaget att se över så att det stämmer överens med förordningen.

- Oops: Är också ett avtal ifrån 2016 och upprättat utifrån PuL:s regler vilket innebär att flera av de obligatoriska kraven i 28.3 DSF saknas. Inte heller i detta avtal finns några bifogade instruktioner även om det uppges att biträdet enbart får handla på sådana instruktioner. I avtalet återfinns ett stycke med villkor för annan uppdragstagare som biträdet använder sig av, men ej med benämningen underbiträden. Det saknas också information om att relationen mellan biträde och underbiträde ska regleras i avtal och att personuppgiftsansvarige måste godkänna underbiträden genom särskilt eller allmänt tillstånd. Avtalet saknade information om biträdes skyldighet att vidta åtgärder för att bistå den personuppgiftsansvarige i frågan om att uppfylla begäran gällande de registrerades rättigheter. Det saknades också information angående biträdets skyldighet att bistå den personuppgiftsansvariga i fråga om dennes skyldigheter enligt artikel 32-36 - här saknades alla förutom artikel 32 om säkerhet. Slutligen reglerade avtalet inte biträdets skyldighet att gå med på och bistå vid granskning och inspektioner.
- PIN: Även i detta avtal uppges behandling enbart få ske på instruktioner ifrån personuppgiftsansvarig men det saknas sådana särskilda instruktioner. Utöver det saknas det enbart information om biträdes skyldighet att bistå den personuppgiftsansvariga i fråga om dennes skyldigheter enligt artikel 36 som berör förhandssamråd. Eftersom detta avtal är från 2020 och ser ut att vara Boplats egen mall, ser dataskyddsombudet det som positivt att man för den egna verksamheten tagit fram en mall som uppfyller de ställda kraven.

Sammanfattning

- Bolaget behöver utreda vilket behov som finns för att skapa rutiner för ett mer konsekvent arbetssätt avseende ingående av personuppgiftsbiträdesavtal, kontroll av att de obligatoriska kraven är uppfyllda, att instruktioner lämnas samt att rätt aktör är biträde.
- Om rutin för uppföljning och kontroll av biträdena inte behövs, säkerställ att detta skrivs in i alla biträdesavtal
- Bolaget bör göra en översyn över gamla biträdesavtal eftersom de skrevs innan nuvarande Dataskyddsförordning trädde i kraft
- Den mall som bolaget själva tagit fram uppfyller kraven enligt förordningen och bör användas vid ingående av nya personuppgiftsbiträdesavtal
- Dokumentera vem inom organisationen som är behörig att teckna personuppgiftsbiträdesavtal
- Säkerställ att det finns instruktioner till personuppgiftsbiträdesavtalen och att man i framtiden har rutin för att lämna sådana instruktioner

Bilagor

1. Kontrollfrågor om personuppgiftsbiträdesavtal

Fördjupad kontroll 2021

Biträdesavtal

Del 1

Vänligen besvara frågorna så utförligt och detaljerat som möjligt. Bifoga även relevanta dokument, underlag och aktuella rutiner som ni har tagit fram. Svaren skall ha inkommit till dataskyddsombudet **senast den 5 april 2021**.
Har du frågor, kontakta ditt dataskyddsombud.

1. Ange/bifoga lista över vilka ni har identifierat som personuppgiftsbiträden.
    a. Ange för vilka personuppgiftsbiträden som det finns personuppgiftsbiträdesavtal med.
    b. Har ni gett instruktioner till de personuppgiftsbiträden som ni har avtal med (enligt art. 28.3 a dataskyddsförordningen)?
2. Finns det rutiner för bedömningen av om en leverantör eller annan motpart ska anses vara personuppgiftsbiträde?
    a. Om ja, bifoga rutinen/rutinerna.
    b. Om nej, ange hur ni går tillväga för att annars göra den bedömningen.
3. Finns det rutiner för att säkerställa och följa upp att personuppgiftsbiträden uppfyller de garantier som de har lämnat avseende tekniska och organisatoriska åtgärder?
    a. Om ja, bifoga rutinen/rutinerna.
    b. Om nej, ange hur ni annars går tillväga för att göra den bedömningen.
4. Finns det rutiner för regelbunden avtalsuppföljning (t.ex. om tjänsten ändras eller avslutas) för personuppgiftsbiträdesavtalen?
    a. Om ja, bifoga rutinen/rutinerna.
    b. Om nej, ange hur ni säkerställer att era personuppgiftsbiträdesavtal är aktuella och uppdaterade?
5. Ange hur ni säkerställer att tecknande av personuppgiftsbiträdesavtal sker i behörig ordning.

Fördjupad kontroll

Personuppgiftsbehandlingsregistret

Bakgrund

Den fördjupade kontrollen av personuppgiftsbehandlingsregistret syftar till att se om organisationen uppfyller kraven om att systematiskt dokumentera alla behandlingar i form av ett register enligt artikel 30 i dataskyddsförordningen och att rutiner finns för att säkerställa att registerförteckningen hålls aktuell. Kontrollen har genomförts i två delar, del ett har bestått av ett antal frågor som besvarats av organisationen och del två har bestått av att dataskyddsombudet slumpvis valt ut fem behandlingar från registret och kontrollerat om dessa uppfyller kraven.

Iakttagelser från kontrollen

Boplats har angett att man har ett personuppgiftsbehandlingsregister där alla behandlingar är registrerade. Bolaget använder sig av Draftit. All information enligt artikel 30 i GDPR ska vara komplett för varje behandling och har dubbelkollats gentemot den checklista som verksamheten fick ta del av. I dagsläget finns 54 behandlingar registrerade. Dataskyddsombudet utförda stickprovskontroll visade inga avvikelser, utan alla obligatoriska fält var ifyllda på de tre behandlingar som kontrollerades. Dataskyddsombudet gjorde dock en observation gällande den lagliga grunden. Att ange den lagliga grunden på en behandling i registret är inget krav enligt artikel 30, men något som dataskyddsombudet ändå kontrollerat då det trots allt är en förutsättning för att en behandling ska vara laglig. På vissa behandlingar anges flera lagliga grunder, och där är dataskyddsombudets uppmaning till verksamheten att de ser över vilken grund som är den lämpligaste. Om fler lagliga grunder skulle kunna vara tillämpliga så bör ändå enbart en väljas. Det går inte att under en behandlings gång välja en annan laglig grund och det är viktigt att bolaget i sin informationsplikt ger rätt information till de registrerade om vilken laglig grund som används. Det är viktigt att bolaget även framöver säkerställer så korrekt laglig grund anges.

En annan observation som gjordes vid stickprovskontrollen är att det framkommer i behandlingen ”Publicering bilder” att ingen överföring av personuppgifter till tredjeland förekommer. Boplats uppger att dessa bilder främst publiceras i Boplats marknadsföringsmaterial och på webbplatsen, och vanligtvis inte i sociala medier. Där är det viktigt att bolaget säkerställer så att i de fall bilderna publiceras på sociala medier, att man tänker på reglerna gällande tredjelandsöverföringar. Detta särskilt efter domen i Schrems II-målet som kom förra året. Bolaget har sedan tidigare rekommenderats att kartlägga vilka behandlingar som innebär en överföring av personuppgifter till tredjeland. Det ska då också uppges i registret om en sådan överföring sker.

Boplats anger vidare att det finns en rutin för införande, förändring eller avveckling av process eller informationssystem där det ingår att kontrollera om personuppgiftsregistret behöver kompletteras eller ändras. Översyn av denna rutin gjordes i juli 2019. Huruvida någon översyn av registret annars sker, även när det inte sker förändringar eller införande av process/informationssystem framkommer inte av svaren som bolaget lämnat. Det kan vara av värde för Boplats att även årligen se över registret för att minska risken för att det finns behandlingar som blivit inaktuella eller är felaktiga finns kvar i systemet, vilket i

förlängningen innebär risk för att registrerades personuppgifter behandlas felaktigt. Dataskyddsombudets rekommendation är att bolaget ser över huruvida det är en uppgift som dataskyddsgruppen skulle kunna åta sig i framtiden.

Boplats uppger vidare att personuppgiftsbehandlingsregistret används som en naturlig del i arbetet, genom att det vid införande eller ändring av en ny process eller nytt informationssystem är ansvarig chef som ansvarar för att se till så att personuppgifter behandlas riktigt, vilket också innebär ansvar för att föra in nya behandlingar, eller ändringar, i registret. Boplats dataskyddsgrupp uppger att medvetenheten om registrets utformning, vilka uppgifter som ska anges och varför, kan förbättras hos ansvariga chefer. Därför planerar bolaget att ha genomgång av alla existerande behandlingar med varje avdelningschefer under 2021. Att ansvarig chef också ska se över personuppgiftsbehandlingsregistret innebär att det finns ett tydligt utpekat ansvar. Det betyder att kunskapen om vad varje behandling innebär och vilka krav som ställs för registret måste finnas hos var och en som påbörjar nya behandlingar för att på ett korrekt sätt kunna ange bland annat laglig grund, ändamål och vilka personuppgifter som kommer att behandlas. Risken om denna kunskap inte finns hos medarbetarna är att man påbörjar en ny behandling som inte är följsam gentemot dataskyddslagstiftningen vilket kan leda till klagomål från enskild eller vite från tillsynsmyndighet. Bolaget har uppgett att man avser att öka medvetenheten hos de chefer som ansvarar för införandet och ändringar i registret för att säkerställa att kunskap finns om vilka uppgifter som ska anges och varför. Detta anser dataskyddsombudet vara mycket positivt, då det sprider kunskap inom verksamheten och i förlängningen också förenklar dataskyddskontakternas jobb gällande efterlevnaden av dataskyddsförordningen i verksamheten. Skulle bolaget ge ansvaret till dataskyddsgruppen att årligen följa upp registret är det positivt om grundarbetet redan är gjort på ett korrekt sätt av de som ansvarar för behandlingarna.

Kontrollen visar på att Boplats både arbetar aktivt med registret samt har en framtagen rutin där registret ingår vilket dataskyddsombudet anser positivt. Eftersom det är ett krav enligt förordningen att personuppgiftsansvarig ska ha ett korrekt och uppdaterat register är det naturligt att vid påbörjandet av en ny behandling även föra in denna behandling i registret. Att verksamheten har en rutin bidrar till ett följsamt arbetssätt och minskar risken för att registret blir utdaterat och sannolikt inte uppfyller kraven i dataskyddsförordningen.

Personuppgiftsbehandlingsregistret är också ett verktyg för att få en förståelse för sin verksamhet och kunna överblicka var processer och aktiviteter härrör. Registret är ett ypperligt sätt att avgöra exempelvis vilken laglig grund som kan vara lämplig, om behandlingen verkligen ska anses utgöra en ny behandlingen eller kan täckas in av en annan behandling och för att avgöra vem som bör och kan ha ansvar. Bolaget är medvetna om att visst arbete framåt behöver göras vilket också är positivt då det pekar på en medvetenhet inom verksamheten.

Sammanfattande rekommendationer

- Bolaget bör i sin rutin för kontroll av personuppgiftsbehandlingsregistret också införa att kontroll av de obligatoriska kraven enligt dataskyddsförordningen uppfylls.

- Bolaget bör fundera på om en mer regelbunden översyn av registret är av värde, och inte bara vid införande, ändring eller avslutande av process eller behandling.
- Bolaget bör förtydliga vem eller vilka inom organisationen som skulle ha ansvar. för en sådan regelbunden översyn.
- Bolaget bör, som de själva konstaterat, öka medvetenheten om registret inom verksamheten för att säkerställa så att nya/ändrade behandlingar dokumenteras korrekt.

Bilagor

2. Kontrollfrågor om personuppgiftsbehandlingsregistret

Fördjupad kontroll 2021

Personuppgiftsbehandlingsregistret

Del 1

Vänligen besvara frågorna så utförligt och detaljerat som möjligt. Bifoga även relevanta dokument, underlag och aktuella rutiner som ni har tagit fram. Svaren skall ha inkommit till dataskyddsombudet **senast den 11 mars 2021**.
Har du frågor, kontakta ditt dataskyddsombud.

1. Har verksamheten ett personuppgiftsbehandlingsregister där alla behandlingar är dokumenterade?
2. Är all information enligt artikel 30 i GDPR komplett för varje behandling (obligatoriska fälten)? Om inte, vilka obligatoriska fält har inte fyllts i och varför?
3. Finns det en rutin för att kontinuerligt uppdatera registret med behandlingar som tillkommit eller förändrats? När gjorde ni senast en översyn av registrets innehåll?
4. Använder dataskyddsorganisationen personuppgiftsbehandlingsregistret som en naturlig del i arbetet? Beskriv hur och när det används.