



HÖGSKOLAN
I SKÖVDE

Rektor

BESLUT

2021-06-01

Dnr HS 2021/158

Riktlinjer för personuppgiftsbiträdesavtal

Beslut

Härmed fastställs *Riktlinjer för personuppgiftsbiträdesavtal*. Riktlinjerna gäller från den 1 juni 2021.

Motivering

För såväl verksamhetsstödet som forsknings- och utbildningsverksamheten vid Högskolan i Skövde (Högskolan) föreligger ett behov av stöd gällande tecknande av personuppgiftsbiträdesavtal i samband med tecknande av ett huvudavtal. Krav på tecknande av personuppgiftsbiträdesavtal framgår av dataskyddsförordningen artikel 28.

Riktlinjerna ger stöd till medarbetare inom verksamheten som ska anlita en extern leverantör som ska behandla personuppgifter åt Högskolan.

Beslutet är fattat vid rektors beslutsmöte 1 juni 2021 efter föredragning av säkerhetsansvarig/informationssäkerhetssamordnare Emelie Dolfe. I bredningen av ärendet har högskolejuristen Christina Bjerke Versland samt dataskyddsombudet Anne Lindelöf deltagit. För att se vilka som närvarat vid föredragning och slutgiltig handläggning, utan att delta i avgörandet, hänvisas till aktuellt protokoll från rektors beslutsmöte.

Lars Niklasson

Emelie Dolfe

Sändlista

Rektorsfunktionen
Dekan
Prefekter
Avdelningschefer vid institution
Verksamhetsstödet chefer

Riktlinjer för personuppgiftsbiträdesavtal

1 Inledning

Högskolan är personuppgiftsansvarig för samtliga personuppgiftsbehandlingar som förekommer i verksamheten. Vid tecknande av avtal kan Högskolan behöva teckna skriftligt avtal mellan personuppgiftsansvarige (Högskolan) och personuppgiftsbiträde (leverantören) om denne komma att behandla av personuppgifter för Högskolans räkning. Dessa riktlinjer vänder sig till alla medarbetare och chefer på Högskolan i Skövde (Högskolan) som ska anlita en extern leverantör som ska behandla personuppgifter åt Högskolan.

Riktlinjerna besvarar följande frågor:

- När behövs personuppgiftsbiträdesavtal?
- Ansvar för att ingå avtal samt förvaring
- Innehåll i avtalet och krav på personuppgiftsbiträden

2 Förklaring av begrepp

2.1 Personuppgift

Med *personuppgifter* avses all slags information som direkt eller indirekt kan hänföras till en fysisk person som är i livet. Exempel på personuppgifter är namn, adress, personnummer, diarienummer, IP-adresser, kontouppgifter, e-postadress, telefonnummer, foton, filminspelningar och ljudupptagningar.

2.2 Behandling

Med *behandling* av personuppgifter menas i princip allt som görs med personuppgifter. Enligt definitionen i dataskyddsförordningen är behandling en åtgärd eller kombination av åtgärder beträffande personuppgifter, uppsättningar av personuppgifter – oberoende av om de utförs automatiserat eller inte. Exempel på åtgärder är insamling, registrering, organisering, strukturering, lagring, bearbetning, ändring, framtagning, sökning, läsning, användning, utlämning genom överföring, spridning eller tillhandahållande på annat sätt, justering, sammanförande, begräsning, radering eller förstöring.

2.3 Personuppgiftsbiträdesavtal

Ett personuppgiftsbiträdesavtal är ett skriftligt avtal mellan den personuppgiftsansvarige (Högskolan) och personuppgiftsbiträdet (leverantören) om behandling av personuppgifter för den personuppgiftsansvariges räkning. Syftet med ett personuppgiftsbiträdesavtal är bland annat att garantera att säkerhet och sekretess för personuppgifterna inte påverkas negativt till följd av att den personuppgiftsansvarige väljer att anlita ett personuppgiftsbiträde i stället för att själv utföra den aktuella personuppgiftsbehandlingen.

3 När behövs personuppgiftsbiträdesavtal?

Om Högskolan ska anlita en extern leverantör, t.ex. en myndighet eller enskilda leverantörer av tjänster, som ska behandla personuppgifter för Högskolans räkning blir dessa leverantörer personuppgiftsbiträden. Högskolan ska ta fram och teckna ett personuppgiftsbiträdesavtal (PUBA) med den externa leverantören.

Kravet på att det ska finnas ett personuppgiftsbiträdesavtal framgår av artikel 28 i dataskyddsförordningen.

Om Högskolan åtar sig att behandla personuppgifter för en annan personuppgiftsansvarigs räkning innebär det att Högskolan är personuppgiftsbiträde. Den som åtar sig ett sådant uppdrag behöver också säkerställa att ett personuppgiftsbiträdesavtal ingås mellan parterna.

En förutsättning för att Högskolan ska kunna anlita ett personuppgiftsbiträde är att behandlingen av aktuella personuppgifter har stöd i författning, exempelvis att Högskolan upprättar register över studenter som genomför utbildning på lärosätet. En annan förutsättning är att sekretess inte hindrar ett utlämnande av uppgifterna till ett personuppgiftsbiträde. Högskolan bör dokumentera sitt ställningstagande i dessa rättsliga frågor för varje enskilt avtal innan ett personuppgiftsbiträde anlitas för behandling av Högskolans uppgifter. Här bör särskilt behandling av känsliga personuppgifter beaktas. För stöd bör Högskolans informationssäkerhets- och dataskyddsgrupp kontaktas som också vid behov kan tillhandahålla mall för ändamålet.

3.1 Att bedöma om personuppgiftsbiträdesavtal

Den grundläggande utgångspunkten är att det ska vara fråga om en utomstående fysisk eller juridisk person som inom ramen för ett uppdrag eller en tjänsteleverans ska behandla personuppgifter för Högskolans räkning.

Det kan ibland vara svårt att avgöra om en personuppgiftsbiträdessituation föreligger. Några exempel:

- En leverantör som inom ramen för ett uppdrag *självständigt avgör för vilka ändamål och med vilka medel personuppgifter behandlas*, är inte ett personuppgiftsbiträde utan en personuppgiftsansvarig.
- Omvänt, en leverantör bör ses som personuppgiftsbiträde om *leverantören är osjälvständig i fråga om vilka personuppgifter som ska behandlas*, för vilka ändamål och på vilka sätt som behandling ska göras.

4 Ansvar för att ingå avtal samt förvaring

På Högskolan är det den medarbetare på respektive avdelning/institution som ska genomföra en planerad aktivitet (exempelvis upphandling/teckna avtal) som måste bedöma om aktiviteten medför att personuppgifter kommer att behandlas och ansvarar för att den upphandlade tjänsten kommer att utföras i enlighet med dataskyddslagstiftningen.

Det är den medarbetare som har rätt att teckna avtal gällande en tjänst eller ett uppdrag, som ska bedöma om en leverantör – eller eventuella andra externa personer som tar del av personuppgifter – utgör ett personuppgiftsbiträde och därmed om ett personuppgiftsbiträdesavtal behöver ingås. Vem som får teckna avtal framgår i *Prefekternas delegationsordning* samt *Högskoledirektörens delegationsordning*.

Bedömningen av om ett personuppgiftsbiträdesavtal behövs och vad detta ska innehålla kan vara komplicerad. Stöd i bedömningen kan fås från informationssäkerhets- och dataskyddsgruppen. Kontaktuppgifter finns på medarbetarportalen.

Personuppgiftsbiträdesavtal upprättas i samband med huvudavtalets upprättande. Underskrivet personuppgiftsbiträdesavtal ska omgående lämnas till registrator för diarieföring.

5 Innehåll i avtalet och krav på personuppgiftsbiträden

Bestämmelser om vad ett personuppgiftsbiträdesavtal ska innehålla finns i artikel 28 dataskyddsförordningen. Ett grundläggande krav är att den personuppgiftsansvarige endast får anlita personuppgiftsbiträden som ger tillräckliga garantier om att genomföra lämpliga och organisatoriska åtgärder som säkerställer att den registrerades rättigheter skyddas. Det krävs således en bedömning av att personuppgiftsbiträden är lämpliga ur ett dataskyddsperspektiv.

Enligt dataskyddsförordningen ska bl.a. följande framgå av personuppgiftsbiträdesavtalet.

- Föremålet för behandlingen
- Behandlingens varaktighet, art och ändamål
- Typen av personuppgifter och kategorier av registrerade
- Den personuppgiftsansvariges skyldigheter och rättigheter
- Att biträdet endast får behandla personuppgifter på dokumenterade instruktioner från den personuppgiftsansvarige
- Att personer med behörighet att behandla personuppgifterna har åtagit sig att iaktta konfidentialitet eller omfattas av en lämplig lagstadgad tystnadsplikt
- Att biträdet ska vidta alla åtgärder som krävs enligt artikel 32 dataskyddsförordningen (säkerhetsåtgärder)
- Att biträdet ska respektera Högskolans villkor för anlitaandet av ett annat personuppgiftsbiträde

- Att biträdet ska hjälpa den personuppgiftsansvarige genom lämpliga tekniska och organisatoriska åtgärder så att den personuppgiftsansvarige kan fullgöra sin skyldighet att ansvara på begäran om utövande av den registrerades rättigheter i enlighet med dataskyddsförordningen
- Att biträdet ska bistå den personuppgiftsansvarige med att se till att skyldigheterna enligt artiklarna 32 - 36 dataskyddsförordningen fullgörs
- Att biträdet, beroende på vad den personuppgiftsansvarige väljer, ska radera eller återlämna alla personuppgifter till den personuppgiftsansvarige efter att uppdraget har avslutats, och radera befintliga kopior såvida inte lagring av personuppgifterna krävs enligt unionsrätten eller medlemsstaternas nationella rätt
- Att biträdet ska ge den personuppgiftsansvarige tillgång till all information som krävs för att visa att de skyldigheter som fastställs i artikel 28 dataskyddsförordningen har fullgjorts samt möjliggöra och bidra till granskningar som genomförs av den personuppgiftsansvarige

Vilka ytterligare instruktioner som Högskolan behöver lämna i personuppgiftsbiträdes-avtalet får avgöras i det enskilda fallet.

För mer information se:

- Högskolans portal för säkerhet på medarbetarportalen
- Integritetsskyddsmyndighetens hemsida, imy.se

5.1 Molntjänstlösningar

I vissa fall kan det vara svårt att hitta en leverantör av en viss tjänst och enda möjligheten är att anlita en leverantör av en s.k. publik molntjänst som är bunden av bestämmelser i annat land.

Med publik molntjänst menas en IT-tjänst som levereras över internet och där en leverantör erbjuder möjlighet till t.ex. lagring eller processkraft i servrar som kontrolleras av leverantören och där servrarna finns utspridda på olika geografiska platser. De som använder en molntjänst för lagring av personuppgifter förlorar den faktiska kontrollen över de personuppgifter som lagras. Till detta kommer att molntjänstleverantörer ofta använder sig av standardavtal, det vill säga i förväg definierade användarvillkor, och anlitar underleverantörer. Det är därför viktigt att den som tänker använda en molntjänst i sin verksamhet är medveten om de krav som ställs enligt dataskyddsförordningen och praxis från EU-domstolen.

Den som använder en molntjänst för sin personuppgiftsbehandling är personuppgiftsansvarig för behandlingen även om den utförs av molntjänstleverantören eller dess underleverantörer.

6 Riktlinjerna gäller från

Dessa riktlinjer gäller från 1 juni 2021.