Gäller för: Västra Götalandsregionen
Innehållsansvar: Paulina Oscarsson, (pauos1), Regionutvecklare
Godkänd av: Johan Flarup, (johfl), Direktör

Giltig från: 2025-08-11
Giltig till: 2029-08-07

Personuppgiftsbiträdesavtal

Regional rutin 2025 – 2029
Ledningssystem för informationssäkerhet och dataskydd

VÄSTRA GÖTALANDSREGIONEN

Innehållsförteckning

Inledning

Mål: Vid användning av personuppgiftsbiträde ska ett skriftligt rättsligt bindande avtal tecknas mellan personuppgiftsansvarig och personuppgiftsbiträdet som uppfyller kraven i artikel 28 i dataskyddsförordningen (GDPR).

Syftet med rutinen är att beskriva vad som ska göras innan personuppgiftsbiträdesavtal upprättas, vid upprättandet och efter att personuppgiftsbiträdesavtal upprättats. Rutinen vänder sig till informationsägare, ägare IS/IT-tjänst och avtalsansvariga.

Personuppgiftsbiträdesavtalets syfte är att säkerställa att båda parter följer dataskyddsförordningen (GDPR) och att personuppgiftsansvarig bibehåller kontrollen över personuppgiftsbehandlingen.

Regional rutin för personuppgiftsbiträdesavtal är styrande för alla förvaltningar och bolag i Västra Götalandsregionen och ingår som en del i ledningssystemet för informationssäkerhet och dataskydd (LISD).

Termer och begrepp

Personuppgiftsansvarig

I Västra Götalandsregionen är personuppgiftsansvarig den styrelse, nämnd eller bolag som ensamt eller tillsammans med andra bestämmer ändamålen (varför) och medlen (hur) för behandlingen av personuppgifter. Varje nämnd, styrelse eller bolag är personuppgiftsansvarig för den behandling av personuppgifter som sker i nämndens verksamhet. De arbetsuppgifter som följer av ansvaret för personuppgifterna utförs av tjänstepersoner i nämndens, styrelsens eller bolagets verksamhet.

Informationsägare

En informationsägare ansvarar för att säkerställa att informationen inom sin verksamhet värderas, skyddas och används korrekt. Informationsägare äger de risker mot informationen som uppstår. Informationsägarskapet följer det ordinarie verksamhetsansvaret (VEP).

Personuppgiftsbiträde

Personuppgiftsbiträde är den som behandlar personuppgifter för den personuppgiftsansvariges räkning. Ett personuppgiftsbiträde kan vara en

fysisk eller juridisk person, offentlig myndighet, institution eller annat organ.

Personuppgiftsbehandling

Personuppgiftsbehandling innebär en åtgärd eller kombination av åtgärder beträffande personuppgifter eller uppsättningar av personuppgifter, oberoende av om de utförs automatiserat eller ej, såsom insamling, registrering, organisering, strukturering, lagring, bearbetning eller ändring, framtagning, läsning, användning, utlämning genom överföring, spridning eller tillhandahållande på annat sätt, justering eller sammanförande, begränsning, radering eller förstöring.

Personuppgift

All slags information som direkt eller indirekt kan knytas till en (fysisk) person som är i livet.

Underbiträde

Ett underbiträde är den som behandlar personuppgifter för personuppgiftsbiträdets räkning.

Reglering av förhållanden inom Västra Götalandsregionen

Personuppgiftsbiträdesavtal upprättas inte mellan myndigheter inom Västra Götalandsregionen. Vid tillhandahållande av IS/IT-tjänst av koncernstab digitalisering regleras ansvarsförhållandena genom ledningssystem för informationssäkerhet och dataskydd (LISD) samt IS/IT-styrmodell.

Innan avtal upprättas

Identifiera nödvändiga säkerhetsåtgärder

Innan avtal upprättas ska informationsägare ha genomfört de grundläggande informationssäkerhets- och dataskyddsanalyserna (informationsklassning, riskhantering, tröskelanalys avseende dataskydd och eventuell konsekvensbedömning avseende dataskydd).

Informationsägaren ansvarar för att ta ställning till om de säkerhetsåtgärder för personuppgiftsbehandlingen som beslutats vid de

grundläggande informationssäkerhets- och dataskyddsanalyserna ska följa med till personuppgiftsbiträdesavtalet som krav. I så fall ska dessa krav ställas på personuppgiftsbiträdet genom att de anges i instruktionerna till personuppgiftsbiträdet. Informationsägaren är ansvarig för att så sker.

I *Informationssäkerhet för extern molntjänst – Regional rutin 2024–2028* fastställs och beskrivs de säkerhetsåtgärder som ska vidtas när extern molntjänst anskaffas, förvaltas och när VGR lämnar eller avslutar informationsbehandling i en extern molntjänst. Informationsägaren ansvarar för att bedöma vilka säkerhetsåtgärder i rutinen som ska anges i instruktionen för personuppgiftsbiträdet.

När personuppgifter behandlas av leverantör (personuppgiftsbiträde) i en regionalt förvaltad IS/IT-tjänst

När personuppgiftsbiträde används för IS/IT-tjänst eller licenser som förvaltas, eller kommer att förvaltas, av koncernstab digitalisering ska en ägare för IS/IT-tjänsten utses. Ägaren av IS/IT-tjänst ansvarar för att, utifrån de krav på säkerhetsåtgärder som informationsägaren ställer på tjänsten, att införa, förvalta, följa upp och utvärdera säkerhetsåtgärder i IS/IT-tjänsten så att adekvat skydd uppnås för personuppgifterna.

Vid upprättande av avtal

Mall för personuppgiftsbiträdesavtal

Västra Götalandsregionen ska använda den mall för personuppgiftsbiträdesavtal som anges på organisationens intranätssidor om informationssäkerhet och dataskydd. I de undantagsfall leverantörens mall för personuppgiftsbiträdesavtal eller instruktioner ska användas ska innehållet granskas med stöd av jurist.

I personuppgiftsavtalet ska samtliga personuppgiftsansvariga i VGR som omfattas av avtalet anges.

Instruktion till personuppgiftsbiträdet

Personuppgiftsbiträdet får endast behandla personuppgifter på dokumenterade instruktioner från den personuppgiftsansvariga.

Informationsägaren ansvarar för instruktionen till personuppgiftsbiträdet.

Instruktionerna är en obligatorisk bilaga till personuppgiftsbiträdesavtalet och ska minst innehålla följande information:

- Föremålet för behandlingen (huvudsakliga syftet med personuppgiftsbiträdets behandling av personuppgifter åt den personuppgiftsansvarige, ändamålet med personuppgiftsbiträdets behandling av personuppgifter åt den personuppgiftsansvarige och vilka behandlingsåtgärder som personuppgiftsbiträdet ska utföra åt den personuppgiftsansvarige).
- Vilka typer av personuppgifter som personuppgiftsbiträdet har rätt att behandla.
- Vilka kategorier av registrerade som behandlingen omfattar.
- Vilka särskilda hanteringskrav som gäller vid behandlingen av personuppgifter som utförs av personuppgiftsbiträdet.
- Vilka särskilda tekniska och organisatoriska säkerhetsåtgärder som gäller för personuppgiftsbiträdets behandling av personuppgifter. Detta framgår av de grundläggande informationssäkerhets- och dataskyddsanalyserna som informationsägare ansvarar för att ha genomförts.
- Vilka särskilda krav på loggning som gäller vid behandling av personuppgifter samt vilka som ska ha tillgång till dem.
- Vilka krav personuppgiftsbiträdet ska iaktta avseende lokalisering och överföring av personuppgifter till tredjeland (land utanför EU/EES).
- Behandlingens varaktighet.
- Vid behov ytterligare instruktioner angående behandling av personuppgifter som utförs av personuppgiftsbiträdet (t.ex. förfarandet vid personuppgiftsansvarigs granskningar och inspektioner av personuppgiftsbiträdets behandling av personuppgifter enligt avsnitt 9 i personuppgiftsbiträdesavtalet).

Instruktionerna från den personuppgiftsansvariga kan följa direkt av avtalet eller ges skriftligen på annat sätt. Instruktionerna ska diarieföras tillsammans med personuppgiftsbiträdesavtalet.

Huvudavtal – avtalsansvarigs ansvar

Med huvudavtal menas det avtal som avser den ursprungliga orsaken till att personuppgiftsbiträdet anlitas.

Inköpare, avtalsansvarig eller annan som enligt delegeringsordning har rätt att ingå avtal ansvarar för huvudavtalet och för att personuppgiftsbiträdesavtal upprättas när leverantör behandlar personuppgifter på VGR:s vägnar.

Personuppgiftsbiträdesavtal är en bilaga till ett huvudavtal.

Kontaktperson för parternas samarbete om dataskydd

I personuppgiftsbiträdesavtalet ska kontaktpersoner för parternas samarbete om dataskydd anges för bägge parter. Kontaktpersonen ska vara väl insatt i varför huvudavtalet har tecknats och vad huvudavtalet gäller samt vilka instruktioner som getts till personuppgiftsbiträdet.

Om personuppgiftsbiträdesavtalet gäller en molntjänst, IS/IT-tjänst, licenser eller andra tjänster som förvaltas av koncernstab digitalisering ska ägare av IS/IT-tjänsten vara VGR:s kontaktperson för parternas samarbete om dataskydd.

Vid övriga situationer ska informationsägaren eller annan av informationsägaren utsedd person stå som kontaktperson.

Kontaktperson för administration av personuppgiftsbiträdesavtalet

I personuppgiftsbiträdesavtalet ska kontaktpersoner för administration av personuppgiftsbiträdesavtalet anges för bägge parter. För VGR:s del ska kontaktpersonen vara samma som undertecknar huvudavtalet.

Vid anlitande av underbiträde

Informationsägaren ska ta ställning till om ett visst underbiträde kan anlitas, om man ska lämna ett generellt godkännande eller om man ska neka att överhuvud taget anlita ett underbiträde. Detta ska anges i instruktionen till personuppgiftsbiträdet.

Om personuppgiftsbiträdet anlitar ett underbiträde ansvarar personuppgiftsbiträdet för att underbiträdet uppfyller sina skyldigheter i fråga om dataskydd.

Samtliga aktuella underbiträden ska anges i underbiträdesbilagan (lista över godkända underbiträden). Om personuppgiftsbiträdet har rätt att anlita nya underbiträden efter att avtal upprättats ska bilagan ska uppdateras när så sker av personuppgiftsbiträdet och skickas till personuppgiftsansvarig.

Efter att personuppgiftsbiträdesavtal upprättats

Diarieföring och registrering av personuppgiftsbehandlingen

Personuppgiftsbiträdesavtal, tillhörande instruktion och eventuell underbiträdesbilaga (lista över godkända underbiträden) ska diarieföras tillsammans med huvudavtalet och namnges på ett tydligt sätt som möjliggör kontroll och uppföljning, t.ex. personuppgiftsbiträdesavtal för [det huvudavtalet avser], instruktion för behandling [namn på personuppgiftsuppbehandling] och underbiträdesbilaga (lista över godkända underbiträden) [namn på personuppgiftsuppbehandling].

Avtalsansvarig ansvarar för att både huvudavtal och dess bilagor diarieförs.

Informationsägaren ansvarar för att uppgift om personuppgiftsbehandlingen och eventuella biträden förtecknas i register över personuppgiftsbehandlingar.

Uppföljning av personuppgiftsbiträdesavtalet

Vid förändring eller förlängning av huvudavtal

Avtalsansvarig ska kontakta den som står som kontaktperson för parternas samarbete om dataskydd innan huvudavtal förlängs eller förändras för kontroll av uppgifterna i biträdesavtalet och instruktionerna till personuppgiftsbiträdet.

Vid förändring i verksamheten

Innehåll i instruktionen kan behöva uppdateras vid förändringar i verksamheten som resulterar i förändringar av de personuppgifter som leverantören ska behandla, t.ex. när arbetsuppgifter utförs på annat sätt och nya personuppgifter tillkommer eller tvärtom, att behov av att behandla vissa personuppgifter försvinner. Informationsägaren ansvarar för att instruktionen uppdateras vid behov.

Vid personuppgiftsincidenter

Det kan finnas behov av att följa upp personuppgiftsbiträdesavtal och instruktion till personuppgiftsbiträdet vid personuppgiftsincidenter eller andra händelser som indikerar brister i personuppgiftsbehandlingen. Informationsägaren ansvarar för att personuppgiftsavtalet och instruktionen uppdateras vid behov.

Relaterade dokument

Termbank för informationssäkerhet - nationell terminologi för informations- och cybersäkerhetsområdet https://termbanken.informationssakerhet.se/

Policy - säkerhet och beredskap i Västra Götalandsregionen (dnr RS 2018-00129)

Informationssäkerhet och dataskydd - Regional riktlinje 2023–2027 (dnr RS 2023-02811)

Informationsklassning - Regional rutin 2024 – 2028 (dokument-id: RS10162-1596316381-102)

Riskhantering för informationssäkerhet - Regional rutin 2024 – 2028 (dokument-id: RS10162-1596316381-118)

Tröskelanalys avseende dataskydd - Regional rutin 2024–2028 (dokument-id: RS10162-1596316381-258)

Konsekvensbedömning avseende dataskydd - Regional rutin 2024–2028 (dokument-id: RS10162-1596316381-259)

Säker utveckling - Informationssäkerhet och dataskydd vid verksamhetsutveckling - Regional rutin 2024–2028 (dokument-id: RS10162-1596316381-136)

Informationssäkerhet för extern molntjänst - Regional rutin 2024 – 2028 (dokument-id: RS10162-1596316381-126)

Register över personuppgiftsbehandlingar – Regional rutin 2024 – 2028 (dokument-id: RS10162-1596316381-301)

Information om handlingen

Handlingstyp: Rutin

Gäller för: Västra Götalandsregionen

Innehållsansvar: Paulina Oscarsson, (pauos1), Regionutvecklare

Godkänd av: Johan Flarup, (johfl), Direktör

Dokument-ID: RS10162-1596316381-157

Version: 2.0

Giltig från: 2025-08-11

Giltig till: 2029-08-07