

Policy för hantering av personuppgifter

Beslutad av AÖS direktion 2018-05-21



Inledning

Dataskyddsförordningen syftar till att stärka och harmonisera den rättsliga säkerheten för enskilda och deras personliga integritet men även att öka flexibilitet och förutsägbarhet för myndigheter och ekonomiska operatörer inom unionen genom ett enhetligt regelverk för att därigenom kunna utveckla den digitala ekonomin över hela den inre marknaden.

Betydande vikt läggs vid att personuppgiftsansvarig kan visa att förordningen följs vilket medför ett ökat krav på dokumentation över de hanteringar inom förbundet som innefattar personuppgifter. För vad fall förbundet brister i sin hantering eller på annat sätt inte lever upp till de krav som ställs riskerar även förbundet komma att åläggas sanktionsavgift eller skadeståndsansvar.

Förordningen begränsar inte offentlighetsprincipen eller myndigheternas skyldigheter enligt arkivlagen.

Syfte och omfattning

Då hantering av personuppgifter av olika slag och för skilda ändamål sker inom en rad olika verksamheter inom förbundet finns ett behov av övergripande policydokument för att sätta de ramar som behöver iaktas vid personuppgiftshantering. Detta kompletteras av rutiner som på ett mer detaljerat sätt stödjer verksamheterna i de processer och hanteringsfrågor som uppkommer. Policyn tar sikte på sådan behandling av personuppgifter som helt eller delvis företas på automatiserad väg samt i övrigt vid behandling av personuppgifter som ingår eller kommer att ingå i ett register.

Med begreppet personuppgift avses all information som direkt eller indirekt kan hänföras till en levande person. Som exempel på personuppgifter kan nämnas namn, personnummer, telefonnummer, e-postadress, ip-adress, fotografier etc. Exempelen är inte tänkta att vara uttömmande utan det avgörande för om det är en personuppgift är om uppgiften, av slag det än månde vara, kan härledes till en fysisk levande person.

Personuppgiftshantering

I förbundet skall varje behandling av personuppgifter ske med iakttagande av den enskildes integritet och med beaktande av de rättigheter som tillkommer de registrerade. Utifrån detta skall:

Varje behandling av personuppgifter ske i enlighet med gällande lagstiftning.

Behandlingen skall vara laglig, korrekt och öppen gentemot den registrerade.

Innan behandling påbörjas – ska ett särskilt och uttryckt ändamål med behandlingen vara fastställt. Behandling av personuppgifter får inte ske för ett ändamål som är oförenligt med det ursprungliga ändamålet.

Insamling av personuppgifter får inte vara mer omfattande än nödvändigt. Detta innebär att endast uppgifter som är adekvata och relevanta får samlas in. Uppgifterna skall vara uppdaterade och korrekta.

Insamlade personuppgifter ska endast bevaras i identifierbar form så länge det är nödvändigt för ändamålet och inte annat följer av lag.

Åtkomst till personuppgifter begränsas till de som är behöriga.

Sådana organisatoriska och tekniska åtgärder för att skydda personuppgifterna som bedöms erforderliga vidtas.

Dataskyddsombud skall finnas utsett för förbundets samtliga verksamhetsområden.

Personuppgiftsansvar

Direktionen är personuppgiftsansvarig. Ansvar innebär att säkerställa bl.a. att:

Ändamål och syfte med behandling av personuppgifter fastställs innan behandlingen påbörjas.

Kännedom finns om var personuppgifter förekommer, hur de används och rutiner finns på plats att kunna informera berörda personer vid begäran.

Dataskyddsombud har utsetts.

Det finns tekniska och organisatoriska förutsättningar att behandla personuppgifter med erforderlig säkerhet.

Registerföring sker över personuppgiftsbehandlingen.

Personuppgiftsbiträdesavtal upprättas när biträden anlitas.

Rutiner finns på plats dels för att tillgodose de registrerades rättigheter dels i övrigt fullgöra skyldigheter som ankommer på personuppgiftsansvarig såsom t.ex. anmälningskyldighet vid personuppgiftsincidenter.

Genom dokumentation säkerställs att lagstiftningens krav är uppfyllda.