Hälsinglands
Utbildningsförbund

INFORMATIONSSÄKERHETSPOLICY

Inom Hälsinglands Utbildningsförbund ska varje behandling av personuppgifter ske med hänsyn till den enskildes personliga integritet och rättssäkerhet.

Ovanstående policy är antagen av Hälsinglands Utbildningsförbunds direktion 2018-04-23.

POSTADRESS Hälsinglands Utbildningsförbund, 821 80 Bollnäs **BESÖKSADRESS** Kulturhuset, Collinigatan 12, 821 43 Bollnäs **TELEFON** 010-454 10 00 **E-POST** info@hufb.se **WEBB** www.hufb.se

Hälsinglands
Utbildningsförbund

Informationssäkerhetspolicy - tillämpning

Information är en av utbildningsförbundets viktigaste tillgångar och hanteringen av den är en mycket viktig del i arbetet. Med informationstillgångar avses all information oavsett om den behandlas manuellt eller automatiserat och oberoende av dess form eller miljön den förekommer i. Informationssäkerheten omfattar förbundets alla informationstillgångar.

Denna informationssäkerhetspolicy gäller för informationssäkerhet inom förbund, inklusive de bolag, stiftelser och ekonomiska föreningar där förbundet utövar ett rättsligt bestämmande inflytande. Policyn ska även tillämpas av dem som har beroenden till förbundets gemensamma informationstillgångar.

Informationssäkerhet

Med informationssäkerhet avses att följande krav säkerställs och upprätthålls:

- Konfidentialitet - att informationen kan åtkomstbegränsas (benämndes tidigare sekretess)
- Riktighet - att informationen ska vara tillförlitlig, korrekt och fullständig
- Tillgänglighet - att informationen ska kunna nyttjas efter behov, i förväntad utsträckning samt av rätt person med rätt behörighet
- Spårbarhet - att specifika aktiviteter som rör informationen kan spåras

Dataskydd för hantering av personuppgifter

- Varje behandling av personuppgifter ska ske med hänsyn till den enskildes personliga integritet och rättigheter.

- Varje behandling av personuppgifter ska ske i enlighet med gällande lagstiftning

Vid behandling av personuppgifter ska följande grundläggande principer tillämpas:

- Behandlingen ska vara laglig, korrekt och öppen gentemot den registrerade

- Ändamålsbegränsning - innan behandling påbörjas ska ett särskilt och uttryckligt samt berättigat ändamål med behandlingen vara fastställt. Hantering utöver detta ändamål kan vara otillåtet då det kan vara oförenligt med det ursprungliga ändamålet

POSTADRESS Hälsinglands Utbildningsförbund, 821 80 Bollnäs **BESÖKSADRESS** Kulturhuset, Collinigatan 12, 821 43 Bollnäs **TELEFON** 010-454 10 00 **E-POST** info@hufb.se **WEBB** www.hufb.se

- Insamling av uppgifter - endast de uppgifter som är adekvata och relevanta för ändamålet får samlas in. Insamlingen får inte vara mer omfattande än nödvändigt - insamlade personuppgifter ska vara korrekta och uppdaterade
- Lagringsminimering - insamlade personuppgifter får bara bevaras i identifierbar form så länge det är nödvändigt för ändamålet
- Åtkomstbegränsning – endast behöriga ska få åtkomst till personuppgifter
- Integritet och konfidentialitet – lämpliga tekniska och organisatoriska åtgärder baserade på informationssäkerhetsklassningar och riskanalyser ska skydda personuppgifterna
- Ansvar - den personuppgiftsansvarige ska kunna visa att behandlingen sker med följsamhet till principerna
- Verksamhet i förbundet ska vara representerat av ett dataskyddsombud
- Vid varje behandling av personuppgifter ska ett sådant förhållningssätt iakttas att risken för skada för den registrerade minimeras.

Struktur

I detta dokument, *Informationssäkerhetspolicy - tillämpning,* fastställs synen på informationssäkerhet, övergripande mål och organisationens intention med informationssäkerhetsarbetet.

I *Riktlinjer för informationssäkerhet* beskrivs vad som måste etableras för att uppfylla informationssäkerhetspolicyn. Utifrån detta upprättas sedan instruktioner, som detaljerat redogör för hur exempelvis rutiner och säkerhets-lösningar ska utformas och tillämpas, för att informationssäkerhetspolicyn och riktlinjerna ska följas.

Sammantaget är detta förbundets regelverk för informationssäkerhet.

Mål

Förbundets informationssäkerhetsarbete har som mål:

- att informationssäkerhet är en naturlig och integrerad del i verksamheten,
- att kunskap finns om hur informationssäkerheten säkerställs,
- att alla informationstillgångar klassificeras,
- att hotbilden mot informationstillgångar fortlöpande analyseras,

POSTADRESS Hälsinglands Utbildningsförbund, 821 80 Bollnäs **BESÖKSADRESS** Kulturhuset, Collinigatan 12, 821 43 Bollnäs **TELEFON** 010-454 10 00 **E-POST** info@hufb.se **WEBB** www.hufb.se

- att händelser som kan leda till negativa konsekvenser förebyggs, och
- att krishanteringsförmågan fortlöpande analyseras och upprätthålls.

Organisation av informationssäkerhetsarbetet

- *Direktionen* uttrycker sin viljeinriktning i denna policy och har det yttersta ansvaret för kommunens informationssäkerhetsarbete.
- *Informationssäkerhetssamordnaren* har det övergripande och strategiska ansvaret att leda, utveckla och samordna informationssäkerhetsarbetet.
- *Informationsägarna* har det övergripande och yttersta ansvaret för den information som används av ett eller flera system. Informationsägaren fattar avgörande beslut om hur, av vem och vilken information som får hanteras.
- *Systemägarna* har övergripande ansvar för respektive system och dess användning. System ska uppfylla informationssäkerhetskraven i förhållande till verksamhetens behov dess innehåll klassificeras.
- *Systemförvaltarna* har det funktionella (dagliga) helhetsansvaret för ett system. Systemförvaltaren fungerar i hög grad som systemägarens utförare och ser till att systemets funktionalitet samt planerade och beslutade aktiviteter genomförs och upprätthålls. De har även rollen som registerförare.
- *Alla* som hanterar informationstillgångar har ett ansvar att informationssäkerheten upprätthålls.

Efterlevnad

Förbundet ska följa lagar, författningar, avtalsförpliktelser, samt andra säkerhetskrav.
Chefer inom förbundet ska säkerställa att alla säkerhetsrutiner inom deras respektive ansvarsområde utförs korrekt för att uppnå efterlevnad av förbundets informationssäkerhetsregelverk.

Ytterligare information

För vidare information se *Riktlinjer för informationssäkerhet*

POSTADRESS Hälsinglands Utbildningsförbund, 821 80 Bollnäs **BESÖKSADRESS** Kulturhuset, Collinigatan 12, 821 43 Bollnäs **TELEFON** 010-454 10 00 **E-POST** info@hufb.se **WEBB** www.hufb.se

Hälsinglands
Utbildningsförbund

Riktlinje för hantering av personuppgifter i Hälsinglands Utbildningsförbund

Inledning

Följande riktlinje syftar till att konkretisera policyn för informationssäkerhet samt ge vägledning och råd vid hantering av personuppgifter i Hälsinglands Utbildningsförbund.
Riktlinjen, som grundar sig på bestämmelserna i lagstiftningen och kan komma att justeras vid förändringar av gällande rätt, antas av förbundschef.

Omfattning

Denna riktlinje gäller för Hälsinglands Utbildningsförbunds hela verksamhet samt i förekommande fall i styrelser i sådana organisationer där förbundet har det rättsligt bestämmande inflytandet. Riktlinjen avser hantering av personuppgifter som helt eller delvis företas på automatisk väg samt på annan än automatisk behandling av personuppgifter som ingår eller kommer att ingå i ett register. Med ett register avses en strukturerad samling uppgifter som är tillgängliga för sökning eller sammanställda enligt särskilda kriterier.

Bakgrund

Från och med den 25 maj 2018 gäller EU:s dataskyddsförordning (679/2016) för hantering av personuppgifter. Förordningen ersätter personuppgiftslagen, PuL (1998:204). Förordningen behöver inte implementeras i svensk rätt genom svensk lag utan är direkt tillämplig.
Genom den nya lagstiftningen ska den tillit som behövs för att utveckla den digitala ekonomin över hela den inre marknaden uppnås. Det är av stor vikt att fysiska personer har kontroll över sina egna personuppgifter. Målet med dataskyddsförordningen anges vara att stärka och harmonisera den rättsliga säkerheten och smidigheten för fysiska personer, ekonomiska operatörer och myndigheter i unionen.

Övergångsregler

All pågående behandling ska vara anpassad till förordningen den 25 maj 2018. Om pågående behandling grundar sig på samtycke enligt direktiv 95/46/EG, är det inte nödvändigt att den registrerade på nytt ger sitt samtycke för att den personuppgiftsansvarige ska kunna fortsätta med behandlingen i fråga efter det att denna förordning börjar tillämpas, om det sätt på vilket samtycket gavs överensstämmer med villkoren i denna förordning. Beslut av kommissionen som

POSTADRESS Hälsinglands Utbildningsförbund, 821 80 Bollnäs BESÖKSADRESS Kulturhuset, Collinigatan 12, 821 43 Bollnäs TELEFON 010-454 10 00 E-POST info@hufb.se WEBB www.hufb.se

antagits och tillstånd från tillsynsmyndigheterna som utfärdats på grundval av direktiv 95/46/EG ska fortsatt vara giltiga tills de ändras, ersätts eller upphävs.

Materiellt tillämpningsområde

Förordningen ska tillämpas på all hantering av personuppgifter som helt eller delvis företas på automatisk väg samt på annan än automatisk behandling av personuppgifter som ingår eller kommer att ingå i ett register.

Personuppgiftsansvar

Samtliga nämnder samt styrelser i sådana organisationer där xx kommun/förbund har det rättsligt bestämmande inflytandet, är personuppgiftsansvariga för sina respektive verksamhetsområden. Ansvaret innebär en yttersta skyldighet att se till att gällande lagstiftning följs genom att bl.a.

- Fastställa ändamål och syfte med behandling av personuppgifter, innan behandling påbörjas.
- Utse dataskyddsombud som har förutsättningar för uppdraget och har nödvändig kunskap för att fullgöra sitt uppdrag.
- Säkerställa att det finns tekniska och organisatoriska förutsättningar att behandla personuppgifter med nödvändig säkerhet.
- Kunna visa att kraven i lagstiftningen är uppfyllda genom noggrann dokumentation samt verifierande tester.
- Föra register över behandlingar av personuppgifter.

Laglig behandling av personuppgifter

Personuppgifter får endast behandlas om det finns laglig grund för behandlingen. Den lagliga grunden ska fastställas innan behandling påbörjas enligt någon av nedan punkter:

- Samtycke – ska vara informerat, frivilligt och specifikt samt kunna visas.
- Behandlingen är nödvändig för att fullgöra ett avtal.
- Behandlingen är nödvändig för att fullgöra en rättslig förpliktelse som den personuppgiftsansvarige har.
- Behandlingen är nödvändig för att skydda ett grundläggande intresse för den registrerade eller annan fysisk person

POSTADRESS Hälsinglands Utbildningsförbund, 821 80 Bollnäs **BESÖKSADRESS** Kulturhuset, Collinigatan 12, 821 43 Bollnäs **TELEFON** 010-454 10 00 **E-POST** info@hufb.se **WEBB** www.hufb.se

- Behandlingen är nödvändig för att utföra uppgift av allmänt intresse eller som ett led i den personuppgiftsansvariges myndighetsutövning.

Innan behandling av personuppgifter påbörjas krävs följande:

1. Dokumentera ändamål och syfte samt under hur lång tid behandlingen beräknas pågå.

2. Fastställ rättslig grund.

3. Inhämta samtycke vid behov.

4. Säkerställ att behandlingen sker i enlighet med de grundläggande principerna och denna policy och riktlinje.

5. Vid behov, rådgör med dataskyddsombudet.

6. Klassificera personuppgifterna utifrån informationssäkerhetsnivå och genomföra en riskanalys av den planerade behandlingen. Dataskyddsombudet ska involveras i riskanalysen.

7. Samråd med tillsynsmyndighet om hög risk inte kan åtgärdas inför behandling av personuppgifter.

8. Se till att det finns tillräckliga tekniska och organisatoriska säkerhetsåtgärder utifrån genomförd informationssäkerhetsklassning och resultat från riskanalys.

9. Klargör om, och i så fall vilken, kommunikation med den registrerade som är nödvändigt.

10. Upprätta personuppgiftsbiträdesavtal vid behov.

11. Se till att dataskyddsombudet godkänner behandlingen.

12. Anteckna ny behandling av personuppgifter i det system som kommunen/förbundet använder.

Säkerhet
Behandling av personuppgifter får ske om lämplig teknisk och organisatorisk säkerhet vidtagits för behandlingen. Säkerheten ska baseras på genomförda informationssäkerhetsklassningar och riskanalyser.

Säkerhet utgörs av:
Inbyggt dataskydd och dataskydd som standard vilket för personuppgiftshanteringen bl.a. innebär:

POSTADRESS Hälsinglands Utbildningsförbund, 821 80 Bollnäs **BESÖKSADRESS** Kulturhuset, Collinigatan 12, 821 43 Bollnäs **TELEFON** 010-454 10 00 **E-POST** info@hufb.se **WEBB** www.hufb.se

- att säkerställandet av personuppgiftshanteringen ska finnas med redan från den initiala planeringen och täcka såväl tekniska som organisatoriska åtgärder.
- säkerställa att xx kommunen/förbundet grundsäkerhetsnivå för informationssäkerhet föreligger samt om möjligt använda åtgärder som pseudonymisering, anonymisering eller kryptering.
- säkerställa att xx kommunen/förbundet förhöjda säkerhetsnivå för informationssäkerhet föreligger avseende särskilda personuppgifters konfidentialitet och riktighet vilket för elektronisk hantering bl.a. innebär att använda kryptering samt stark autentisering motsvarande tillitsnivå 3 för e-legitimation.
- använda åtgärder som uppgiftsminimering, lagringsminimering, fritextfältsminimering och åtkomstbegränsning.

- Införande och tillämpning av rutiner för att:
  - Kontinuerligt testa, undersöka och visa på effektiviteten av införda säkerhetsåtgärder.
  - Anmäla personuppgiftsincident till tillsynsmyndighet.
  - Vid behov kunna ge incidentinformation till berörda registrerade.
  - Vid behov kunna involvera och rådgöra med dataskyddsombudet.

Personuppgiftsbiträde

Den som behandlar personuppgifter på uppdrag av annan personuppgiftsansvarig blir personuppgiftsbiträde i förhållande till den personuppgiftsansvarige. Vid anlitandet av ett personuppgiftsbiträde ska säkerställas att denne kan ge tillräckliga garantier om att upprätthålla lämplig teknisk och organisatorisk säkerhet i enlighet med gällande rätt.

Personuppgiftsbiträdesavtal

Personuppgiftsbiträdets (biträdet) behandling av personuppgifter ska regleras av personuppgiftsbiträdesavtal mellan biträdet och den personuppgiftsansvarige (ansvarige). I avtalet ska anges:

- Vem som är personuppgiftsansvarig respektive personuppgiftsbiträde.
- Vad behandlingen avser, dess varaktighet, art, ändamål, typ av personuppgifter samt kategori av registrerade.

POSTADRESS Hälsinglands Utbildningsförbund, 821 80 Bollnäs **BESÖKSADRESS** Kulturhuset, Collinigatan 12, 821 43 Bollnäs **TELEFON** 010-454 10 00 **E-POST** info@hufb.se **WEBB** www.hufb.se

- Den ansvariges skyldigheter och rättigheter.
- Att biträdet endast får behandla personuppgifter i enlighet med den ansvariges instruktion.
- Att biträdet iakttar nödvändig konfidentialitet och tystnadsplikt.
- Att biträdet vidtar alla lämpliga tekniska och organisatoriska åtgärder för att säkerställa adekvat skydd för personuppgifterna samt att detta kan visas genom att ge ansvarige tillgång till vederbörlig information.
- Att biträdet ska bistå den ansvarige i att uppfylla sina förpliktelser enligt förordningen.
- Att biträdet inte får anlita underleverantör för behandling av den ansvariges personuppgifter utan den ansvariges skriftliga medgivande till detta. Om biträdet anlitar underleverantör ska personuppgiftsbiträdesavtal upprättas även mellan dessa parter.
- Att överföring till tredje land inte får ske utan att adekvata säkerhetsåtgärder är uppfyllda.
- Reglering om inom vilken tid radering eller överflyttning av personuppgifter sker vid avtals upphörande.

Register över behandling

Varje personuppgiftsansvarig ska föra ett register över behandling som utförs under dess ansvar. Registret ska minst innehålla:

- Namn och kontaktuppgifter till den personuppgiftsansvarige samt dataskyddsombudet.
- Ändamålet med behandlingen.
- Laglig grund.
- Kategori av registrerade, personuppgifter samt behandlingar.
- Mottagare av personuppgifter, i förekommande fall.
- Eventuell överföring till tredje land med tillhörande säkerhetsåtgärder.
- Uppskattad tidsfrist för radering.

POSTADRESS Hälsinglands Utbildningsförbund, 821 80 Bollnäs **BESÖKSADRESS** Kulturhuset, Collinigatan 12, 821 43 Bollnäs **TELEFON** 010-454 10 00 **E-POST** info@hufb.se **WEBB** www.hufb.se

- Beskrivning av tekniska och organisatoriska säkerhetsåtgärder för behandlingen om inte detta hindras av exempelvis sekretessbestämmelser.

Dataskyddsombud

Den personuppgiftsansvarige ska utse ett dataskyddsombud att representera den ansvariges verksamhet. Det kan vara en person för flera verksamheter och det kan vara en anställd eller extern konsult. Dataskyddsombudet ska utses på grundval av sina yrkesmässiga kvalifikationer och i synnerhet sakkunskap om lagstiftning och praxis avseende dataskydd. Dataskyddsombudet ska anmälas till tillsynsmyndigheten. Dataskyddsombudet ska minst ha följande uppgifter:

- Informera och ge råd till den personuppgiftsansvarige och anställda om skyldigheterna enligt dataskyddsförordningen.
- Övervaka efterlevnad av förordningen avseende fungerande rutiner och åtgärder, ansvarstilldelning, information, utbildning och granskning.
- Ge råd vid riskanalysen.
- Samarbeta med tillsynsmyndigheten.
- Vara kontaktpunkt för tillsynsmyndigheten i alla frågor som rör behandling av personuppgifter.
- Vara kontaktperson till den registrerade.
- Delta i frågor som rör skyddet av personuppgifter.
- Får även ha andra uppgifter om dessa inte leder till intressekonflikt.

Den personuppgiftsansvarige ska säkerställa att dataskyddsombudet:

- På ett korrekt sätt och i god tid deltar i alla frågor som rör skyddet av personuppgifter.
- Tillhandahålls de resurser och det stöd som krävs för att fullgöra sina uppgifter.
- Upprätthålla ombudets sakkunskap.
- Inte blir föremål för sanktioner eller avsätts på grund av att ombudet utför sitt uppdrag.
- Inte bli föremål för otillbörlig påverkan i utövande av sitt uppdrag.

POSTADRESS Hälsinglands Utbildningsförbund, 821 80 Bollnäs **BESÖKSADRESS** Kulturhuset, Collinigatan 12, 821 43 Bollnäs **TELEFON** 010-454 10 00 **E-POST** info@hufb.se **WEBB** www.hufb.se

- Rapporterar direkt till den personuppgiftsansvarige eller dennes högsta förvaltningsnivå.

POSTADRESS Hälsinglands Utbildningsförbund, 821 80 Bollnäs **BESÖKSADRESS** Kulturhuset, Collinigatan 12, 821 43 Bollnäs **TELEFON** 010-454 10 00 **E-POST** info@hufb.se **WEBB** www.hufb.se