Haninge kommun

Riktlinjer för behandling av personuppgifter

Dokumenttyp	Dokumentnamn	Beslutat datum	Gäller från datum
Styrdokument	Riktlinjer för behandling av personuppgifter	2018-06-12 2018-06-13	2018-06-13

Beslutat av	Ansvarig förvaltning och avdelning	Diarienummer
Grund- och förskolenämnden Gymnasie- och vuxenutbildningsnämnden	Kansliavdelningen, utbildningsförvaltningen	GFN 2018/87 GVN 2018/33

Ämnesord	Ersätter tidigare beslut
Behandling av personuppgifter, GDPR, Dataskyddsförordningen	

Dokumentinformation

Riktlinjerna reglerar hur utbildningsförvaltningen ska hantera personuppgifter för att leva upp till kraven i Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning)som träder i kraft 2018-05-25. Förordningen ersätter den svenska personuppgiftslagen (1998:204), PuL.

Inledning

Från och med den 25 maj 2018 gäller EU:s dataskyddsförordning för hantering av personuppgifter. Förordningen reglerar under vilka förutsättningar personuppgifter får behandlas. Det är förbjudet att behandla personuppgifter i strid med dataskyddsförordningen och brister på området kan leda till omfattande sanktionsavgifter för den personuppgiftsansvarige.

Grund- och förskolenämnden respektive gymnasie- och vuxenutbildningsnämnden är personuppgiftsansvariga för sina respektive verksamhetsområden. Ansvaret innebär en yttersta skyldighet att tillse att gällande lagstiftning efterlevs genom att bl.a. fastställa ändamål och syfte med behandling av personuppgifter innan behandling påbörjas, säkerställa att det finns tekniska och organisatoriska förutsättningar att behandla personuppgifter med erforderlig säkerhet, kunna visa att kraven i lagstiftningen är uppfyllda och föra register över behandlingar av personuppgifter. Dessa riktlinjer syftar till att konkretisera hur det ansvaret ska uppfyllas.

Omfattning

Riktlinjerna gäller för alla anställda inom grund- och förskolenämnden samt gymnasie- och vuxenutbildningsnämnden och ska tillämpas vid 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.

Definitioner

Med *personuppgifter* avses all slags information som direkt eller indirekt kan hänföras till en fysisk person som är i livet, till exempel namn, adress och personnummer. Även information som beskriver någon eller på annat sätt kan härledas till en enskild individ såsom till exempel ”läraren i 2B”, filmer, bilder, pseudonymer och krypterade uppgifter kan vara personuppgifter. Indirekta uppgifter är också personuppgifter om det går att härleda till en enskild individ.

Behandling av personuppgifter omfattar alla åtgärder som vidtas beträffande sådana uppgifter (insamling, lagring, bearbetning etc). Exempel på behandling av personuppgifter:

- Sammanställa en lista med personuppgifter för eget bruk
- Lagra personuppgifter i form av bild eller text
- Skicka eller ta emot ett mejl som innehåller personuppgifter
- Elevadministration i kommunens IT-system

Ett *personuppgiftsbiträde* är den som hanterar personuppgifter för den personuppgiftsansvariges räkning, till exempel en systemleverantör. Ett särskilt avtal, *personuppgiftsbiträdesavtal*, upprättas mellan den personuppgiftsansvarige och personuppgiftsbiträdet för att reglera hur personuppgifterna får behandlas.

Särskilda kategorier av personuppgifter (känsliga personuppgifter) och integritetskänsliga personuppgifter

Särskilda kategorier av personuppgifter (känsliga personuppgifter) är uppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening, uppgifter om lagöverträdelser samt genetiska uppgifter, biometriska uppgifter för att entydigt identifiera en fysisk person, uppgifter om hälsa eller uppgifter om en fysisk persons sexualliv eller sexuell läggning.

Integritetskänsliga personuppgifter är uppgifter som omfattas av sekretess eller som annars rör någons personliga förhållanden, till exempel lärares omdömen eller värderingar om elever.

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. Samtycke används inte om någon av nedanstående punkter är tillämplig.
- Behandlingen är nödvändig för att fullgöra ett avtal
- Behandlingen är nödvändig för att fullgöra en rättslig förpliktelse
- Behandlingen är nödvändig för att skydda ett grundläggande intresse för den registrerade eller annan fysisk person
- Behandlingen är nödvändig för att utföra uppgift av allmänt intresse eller som ett led i den personuppgiftsansvariges myndighetsutövning

Allmänna principer för behandling av personuppgifter

När personuppgifter behandlas ska hänsyn alltid tas till den personliga integriteten. För varje behandling ska ett ändamål fastställas. Endast uppgifter som behövs för att uppnå ändamålet med behandlingen får behandlas. Uppgifterna som behandlas ska alltid vara sakliga och relevanta. Vid behandling av personuppgifter ska följande gälla:

- Uppgifterna ska behandlas på ett lagligt, korrekt och öppet sätt i förhållande till den registrerade (laglighet, korrekthet och öppenhet).
- De ska samlas in för särskilda, uttryckligt angivna och berättigade ändamål och inte senare behandlas på ett sätt som är oförenligt med dessa ändamål. Ytterligare behandling för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål ska inte anses vara oförenlig med de ursprungliga ändamålen (ändamålsbegränsning).
- De ska vara adekvata, relevanta och inte för omfattande i förhållande till de ändamål för vilka de behandlas (uppgiftsminimering).
- De ska vara korrekta och om nödvändigt uppdaterade. Alla rimliga åtgärder måste vidtas för att säkerställa att personuppgifter som är felaktiga i förhållande till de ändamål för vilka de behandlas raderas eller rättas utan dröjsmål (korrekthet).
- De får inte förvaras i en form som möjliggör identifiering av den registrerade under en längre tid än vad som är nödvändigt för de ändamål för vilka personuppgifterna behandlas. Personuppgifter får lagras under längre perioder i den mån som personuppgifterna enbart behandlas för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål under förutsättning att de lämpliga tekniska och organisatoriska åtgärder som krävs enligt GDPR genomförs för att säkerställa den registrerades rättigheter och friheter (lagringsminimering).

- De ska behandlas på ett sätt som säkerställer lämplig säkerhet för personuppgifterna, inbegripet skydd mot obehörig eller otillåten behandling och mot förlust, förstöring eller skada genom olyckshändelse, med användning av lämpliga tekniska eller organisatoriska åtgärder (integritet och konfidentialitet).

Inför att en behandling påbörjas

Redan innan man påbörjar en behandling måste man fundera på vilka personuppgifter som kommer att behandlas, vad ändamålet med behandlingen är samt vilken laglig grund man har för att behandla personuppgifterna. Det gäller oavsett om det handlar om ett större verksamhetssystem, en app, en excellista eller något annat. Till hjälp finns kommunens handbok för behandling av personuppgifter som nås via intranätet. Vid behov rådgör i första hand med förvaltningens dataskyddskoordinator eller i andra hand med dataskyddsombudet (nås på dataskyddsombud@haninge.se). Processen kan beskrivas i följande steg.

1. Identifiera och dokumentera vilka personuppgifter som kommer att behandlas
2. Formulera ändamålet med behandlingen.
3. Fastställ den lagliga grunden för behandlingen
4. Genomför en informationssäkerhetsklassning
5. Genomför eventuell risk- och konsekvensanalys. Dataskyddsombudet ska involveras i denna.
6. Fastställ behov av säkerhetsåtgärder och kontrollera att dessa finns på plats.
7. Om ett nytt verksamhetssystem ska införskaffas för behandlingen ta ställning till hur systemet ska förvaltas, vem blir objektsspecialist?
8. Fastställ hur de registrerade ska få information om behandlingen
9. Fastställ hur och när gallring av personuppgifterna ska ske
10. Upprätta personuppgiftsbiträdesavtal vid behov
11. Om ett nytt verksamhetssystem införskaffas för behandlingen ta fram skriftliga instruktioner för användarna som beskriver hur personuppgifter får behandlas i systemet samt hur dessa gallras.
12. Fyll i en registerförteckning i Draftit samt Mall för rutiner för behandlingen. En länk skickas av förvaltningens dataskyddskoordinator

Vid införskaffande av nytt eller uppgraderat IT-stöd för behandling av personuppgifter ska alltid kommunens Riktlinjer för anskaffning av IT-stöd tillämpas. Dessa nås via intranätet.

Om någon form av social media ska användas ska alltid kommunens Riktlinjer för sociala medier tillämpas. Dessa nås via intranätet.

Konsekvensbedömning

En risk- och konsekvensbedömning ska göras för ”högrisk”-behandlingar, dvs. behandlingar som sannolikt leder till en hög risk för integritetsskyddet. Konsekvensbedömningen ska genomföras innan behandlingen påbörjas. Syftet är att komma fram till om en behandling ska genomföras och vilka säkerhetsåtgärder som krävs.

För alla informationstillgångar ska en informationssäkerhetsklassning genomföras. Har en sådan genomförts behöver man inte genomföra en konsekvensbedömning. Konsekvensbedömningen bör innehålla syfte med behandlingen, behovet av behandlingen jämfört med risken för den personliga integriteten, utvärdering av risker och åtgärder för att minimera riskerna.

Kommunens dataskyddsombud ska rådfrågas vid genomförandet av en konsekvensbedömning.

Säkerhet

Behandling av personuppgifter får ske om lämplig teknisk och organisatorisk säkerhet vidtagits för behandlingen. Säkerheten ska baseras på genomförd informationssäkerhetsklassning. Allmänna principer för dataskydd är att nyttja åtgärder som uppgiftsminimering, lagringsminimering, fritextfältsminimering och åtkomstbegränsning.

Nedan säkerhetskrav gäller i Haninge kommun för behandling av personuppgifter i IT-system.

Typ av information	**Krav**
Känsliga personuppgifter till exempel uppgifter om ras, etniskt ursprung, religion, hälsa, sexualliv Integritetskänslig information till exempel lärares omdömen eller värderingar om elever.	Höga säkerhetskrav (två-faktorsinloggning): BankID, sms, säkerhetsdosa eller annan säker metod för identifiering vid åtkomst till informationen. Vid kommunikation över öppna nät krävs krypterad förbindelse.
Personuppgifter som inte omfattas av sekretess eller som annars kan anses känsliga.	Grundläggande säkerhetskrav (användarnamn och lösenord).

Lagring

Uppgifter som omfattas av sekretess ska i princip bara lagras i verksamhetssystem. Om behov uppstår i samband med framställan/under arbetsprocess kan sekretessbelagda uppgifter förvaras på hemkatalogen W.

Om man behandlar personuppgifter som omfattas av sekretess och det inte finns ett verksamhetssystem för dessa uppgifter kan man lagra dessa på hemkatalogen W. En förutsättning är givetvis att kraven i dessa riktlinjer i övrigt är uppfyllda. Om ett sådant behov uppstår bör man alltid överväga att införskaffa ett IT-stöd. Om det finns behov av att dela uppgifterna med andra kan man skapa en särskild mapp på gruppkatalogen U där endast berörda personer ges behörighet. En sådan beställs via Service desk av ansvarig chef. Filer som innehåller sekretessbelagda uppgifter bör lösenordskyddas. Uppgifter som omfattas av sekretess eller annars är integritetskänsliga ska aldrig förvaras i Microsoft 365 eller G Suite.

E-post

E-posten ska inte användas för överföring eller lagring av känsliga personuppgifter, sekretessbelagda uppgifter eller för integritetskänslig information. I de fall en handling inkommer som kan bli föremål för sekretesskydd tas den ut på papper och lämnas till registrator för bedömning. Därefter ska handlingen omgående tas bort ur e-postsystemet. Om det är möjligt att skicka ett svar utan att själv ange sekretesskyddade uppgifter ska det skickas utan att det ursprungliga mejlet skickas med. I annat fall får en kontakt tas på annat sätt.

Exempel: en lärare får ett mejl från en förälder med frågor om hur barnets stödåtgärder fungerar. Uppgifter om stödåtgärder i skolan är typiskt sett sekretesskyddade varför läraren inte kan svara på frågorna via mejl. Istället skickar hen ett mejl (där det ursprungliga mejlet inte finns med) med förslag på ett möte för att följa upp åtgärderna eller tar telefonkontakt med föräldern.

Personnummer (10 siffror) ska som regel inte mejlas.

Ostrukturerad behandling av personuppgifter

Med ostrukturerad behandling avses behandling som sker i löpande text till exempel i wordfiler eller e-post. För ostrukturerad behandling gäller samma krav som i övrigt i GDPR och dessa riktlinjer. Handlingar som upprättas inom skolan och som rör enskilda får inte innehålla ovidkommande värdeomdömen av allmänt nedsättande eller kränkande karaktär. Dokumentationen ska utformas med respekt för den enskildes integritet.

Personuppgiftsbiträde och personuppgiftsbiträdesavtal

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 i ett personuppgiftsbiträdesavtal mellan biträdet och den personuppgiftsansvarige. Om möjligt ska kommunens egna mall för biträdesavtal användas. Om biträdet vill använda ett eget avtal är det viktigt att granska avtalet så att det uppfyller alla punkter i kommunens checklista för biträdesavtal. Innan leverantörens eget avtal skrivs på måste det skickas till dataskyddsombudet för en slutlig kontroll.

Register över personuppgiftsbehandlingar

Varje behandling av personuppgifter som genomförs ska registreras i kommunens system för registerförteckningar (Draftit). En länk till Draftit fås av dataskyddskordinatorn. Registerförteckningen ska innehålla uppgifter om ändamålet med behandlingen, kategori av registrerade, vilka personuppgifter som behandlas, mottagare av personuppgifter i förekommande fall, eventuell överföring till tredje land med tillhörande säkerhetsåtgärder, uppskattad tidsfrist för gallring och beskrivning av tekniska och organisatoriska säkerhetsåtgärder för behandlingen.

Rättigheter för de registrerade

De registrerade ska alltid få information om att deras personuppgifter behandlas och på vilka grunder. GDPR ställer långtgående krav på vilken information de registrerade har rätt att få. För att säkerställa att de registrerade får all den information de har rätt till ska kommunens mall för information användas. Den nås via intranätet.

Alla har rätt att vända sig till kommunen och kostnadsfritt få ett registerutdrag dvs en förteckning över i vilka sammanhang den enskildes personuppgifter behandlas. Det är viktigt att man säkerställer att registerutdraget skickas till rätt person varför det ska skickas per post till folkbokföringsadressen. Om den sökande vill ha det skickat till en annan adress skickas det rekommenderat. Den sökande kan också komma till kommunhuset och hämta ut sitt utdrag efter att ha legitimerat sig.

Den registrerade har rätt att få felaktiga personuppgifter rättade och att komplettera med sådana personuppgifter som saknas och som är relevanta med hänsyn till ändamålet med personuppgiftsbehandlingen.

Kommunen är skyldig att om någon begär det radera dennas personuppgifter i de fall det inte finns annan lagstiftning som förhindrar detta. Inom kommunen finns det många situationer där det inte är möjligt då vi är skyldiga att bevara handlingarna exempelvis enligt arkivlagen som har företräde.

Anmälan av personuppgiftsincidenter

En personuppgiftsincident är någon typ av händelse som leder till att personuppgifter oavsiktligt förloras, ändras eller avslöjas. Exempel på incidenter: dokument/filer försvinner, systemkrascher, stöld av datorer, telefoner och andra enheter, skadlig programvara inklusive virus eller hackerattacker. Om en personuppgiftsincident inträffar ska den anställde som upptäcker det genast anmäla det i KIA.

Personuppgiftsincidenter som kan innebära en risk för registrerades rättigheter och integritet ska anmälas till Datainspektionen inom 72 timmar, det är därför av största vikt att en anmälan i KIA görs skyndsamt. Det är Dataskyddsombudet som efter att en anmälan inkommit i KIA i förekommande fall gör en anmälan till Datainspektionen. Det är dock verksamhetens ansvar att utreda och åtgärda incidenten.

Beroende på omständigheter och sannolikheten för att de inblandades integritet äventyras, ska personuppgiftsansvarige meddela berörda registrerade. Beslut om ifall de registrerade ska informeras tas i samråd med dataskyddsombudet.