1. Dataskyddsorganisation

Beskriv verksamhetens organisatoriska förutsättningar för att kunna bedriva ett kontinuerligt dataskyddsarbete. Dataskyddsombuden önskar att verksamheten beskriver och resonerar kring verksamhetens dataskyddsorganisation, definierade ansvarsområden och rapporteringsvägar för involverade funktioner samt de resurser som tillhandahålls för arbetet. Dataskyddsombuden vill att verksamheten i sina svar resonerar om de anser att organisationen fungerar, om de har tillräckligt med resurser för att proaktivt arbeta med dataskydd, hur organisationen strategiskt arbetar med dataskydd, om det finns rätt kompetens, samt hur dataskyddsorganisationen bidrar till att dataskyddsarbetet är en naturlig del i verksamhetens processer. Bifoga: Om möjligt en organisationsskiss som visar dataskyddsorganisationens struktur, och om det finns styrdokument i kommunen som beskriver hur en dataskyddsorganisation ska se ut. Bifoga gärna också om dataskyddsorganisationen har en strategi eller årsplanering för sitt dataskyddsarbete.

Dataskyddsorganisation

Ansvaret för informationssäkerhet följer det ordinarie verksamhetsansvaret. Detta gäller från kommunledningen till den enskilde medarbetaren. Roller som arbetar med informationssäkerhet och IT-säkerhet fungerar som stöd till medarbetare, verksamheter och kommunens ledning att kunna ta ansvaret för informationssäkerheten.

Kommunfullmäktige fastställer övergripande mål och principer för informationssäkerhetsarbetet genom en kommunövergripande informationssäkerhetspolicy.

Kommunstyrelsen säkerställer att kommunens arbete med efterlevnad av dataskyddsförordningen sker på ett korrekt och samordnar sätt samt att kommunens informationssäkerhetspolicy efterföljs. För att underlätta för respektive personuppgiftsansvarig att fullgöra sina skyldigheter tar styrelsen fram och uppdaterar mer detaljerade rutiner, mallar och annat underlag. Detta innebär inte någon inskränkning eller begränsning av respektive personuppgiftsansvarigs ansvar.

Utifrån ”Handlingsplan Informationssäkerhet och Dataskydd i Alingsås kommun 2022” har en ny dataskyddsorganisation upprättats inom kommunledningskontoret. Organisationens syfte är att vara kommunens centrala dataskyddssamordnare inom områdena registerförteckning, personuppgiftsbiträdesavtal, tredjelandsöverföringar, personuppgiftsincidenter samt styrning och ledning. Organisationen ska lämna rådgivning till övriga förvaltningar inom dataskyddsområdet.

- **Säkerhetschef** – har det övergripande ansvaret att leda, utveckla och samordna Alingsås kommuns säkerhetsarbete.
- **Informationssäkerhetssamordnare** – har det övergripande ansvaret att leda, utveckla och samordna informationssäkerhetsarbetet. Informationssäkerhetssamordnare ska arbeta i samråd med säkerhetschefen och övriga ledamöter i kommunens informationssäkerhetsråd. Leder nätverket Informationssäkerhet och dataskydd.

- **IT-säkerhetssamordnare** – har det övergripande ansvaret att säkerställa säkerheten i Alingsås kommuns IT-miljö och är stödjande vid kravställning på externa aktörer. Ingår i kommunens informationssäkerhetsråd. Leder nätverket Informationssäkerhet och dataskydd.
- **Kommunjurist** – har det övergripande ansvaret att leda, utveckla och samordna arbetet med hantering av personuppgifter. Ingår i kommunens informationssäkerhetsråd. Leder nätverket Informationssäkerhet och dataskydd.

Ansvar inom respektive verksamhet

Kommunstyrelsen och varje nämnd i Alingsås kommun är personuppgiftsansvarige för den personuppgiftsbehandling som sker inom respektive verksamhet. Styrelsen och respektive nämnd är därmed ansvariga för att inom sitt verksamhetsområde se till att gällande dataskyddslagstiftning samt att ”Policy för behandling av personuppgifter” i Alingsås kommun följs.

Varje nämnd utser en kontaktperson/GDPR-samordnare som är ansvarig för samordningen av arbetet med personuppgiftshantering på respektive förvaltning. Dessa personer ingår i nätverket Informationssäkerhet och dataskydd som arrangeras av kommunstyrelsen med syfte att samordna arbetet med informationssäkerhet och dataskydd inom kommunen.

- **Kontaktperson/GDPR-samordnare för Barn- och ungdomsförvaltningen** – ansvarar för att samordna arbetet med informationssäkerhet och dataskydd på Barn- och ungdomsförvaltningen, t.ex. personuppgiftsincidenter, registrerades rättigheter (exempelvis begäran om registerutdrag samt rättelse och radering), registerförteckning, information till registrerade, säkerhetsbedömning av digitala tjänster/appar, personuppgiftsbiträdesavtal. Ingår som förvaltningens representant i nätverket Informationssäkerhet och dataskydd.
- **System-/Objektägares ansvar** – ansvarar för att objekt efterlever kommunens informationssäkerhetspolicy och riktlinjer för informationssäkerhet.
- **Förvaltningschef** – ytterst ansvarig för system/objekt inom sin verksamhet. Förvaltningschef kan delegera system-/objektägarskap till annan roll inom sin verksamhet.
- **Medarbetare** – alla medarbetare inom verksamheten har ett ansvar att följa verksamhetens informationssäkerhetsarbete. Varje anställd ska i eget arbete följa riktlinjer för informationssäkerhet samt eventuella verksamhetsspecifika regler.

Dataskyddsombud

Dataskyddsombud via samverkansavtal med Göteborgsregionen (GR). Dataskyddsombudet har bland annat till uppgift att informera och ge råd till den personuppgiftsansvarige kring vilka skyldigheter som gäller enligt dataskyddslagstiftning, samt att övervaka efterlevnaden av dataskyddslagstiftningen.

Dataskyddsarbetes organisation i verksamheten

En välfungerande organisation finns. I takt med att organisation och omvärld förändras finns också konstant behov av att roller och ansvarsområden förtydligas och förmedlas i organisationen. Ett kvalitativt arbete med dataskydd är mycket resurskrävande och verksamheterna har en stor andel personuppgiftsbehandlingar. Förvaltningen har allokerat om resurser för att möta ökade krav samtidigt som en del frågor kräver juridisk specialistkompetens som idag saknas i organisationen. De resurser som finns för arbetet med dataskydd används för att arbeta strategiskt utifrån ”Informationssäkerhetspolicy i Alingsås kommun” och tillhörande ”Handlingsplan för informationssäkerhet och dataskyddsarbete”. Det strategiska arbetet sker i huvudsak på förvaltningscentral nivå och innehållet i handlingsplanen verkställs tillsammans med verksamheterna och innefattar bland annat verksamhetsanalys, riskanalys och kontinuitetsplanering. Det genomförs informationsinsatser och det förs en dialog om informationssäkerhet och dataskydd för att verka för att det ska vara en naturlig del av verksamhetens processer sker dels i samtal med rektorer och andra enhetschefer, elevhälsa och administrativ personal men också i samtal med IKT-ansvarig personal vid varje enhet.

Dataskyddsorganisationen finns beskriven i ”Informationssäkerhetspolicy i Alingsås kommun” som innehåller kommunens långsiktiga målsättning med informationssäkerhetsarbetet och dataskydd. Det årliga arbetet beskrivs inom ramen för ”Handlingsplan för Informationssäkerhet och Dataskydd i Alingsås kommun” som innehåller kommunens beslutade aktiviteter för kommande år med syfte att uppnå fullmäktiges långsiktiga mål. Ny handlingsplan fastställs inför varje år.

2. Behandlingsregister och informationsskyldigheten

Under denna punkt önskar dataskyddsombuden att verksamheten redovisar hur nämndens behandlingsregister ser ut både i egenskap av personuppgiftsansvarig men också i egenskap som personuppgiftsbiträde. Dessutom önskar dataskyddsombuden att verksamheten beskriver sitt bedömda nuläge och hur många av verksamhetens behandlingar som i dagsläget bedöms finns dokumenterade. Dataskyddsombuden önskar också en beskrivning hur verksamheten arbetar i val av rättslig grund samt en motivering kring när den rättsliga grunden samtycke används för personuppgiftsbehandling och de överväganden som gjorts kring användandet av den rättsliga grunden i verksamheten.

Bifoga kopia på registerförteckning som upprättats av nämnden som personuppgiftsansvarig och även det register som ska föras om nämnden som personuppgiftsbiträde. Under denna punkt önskar dataskyddsombuden också få en beskrivning om hur verksamheten har arbetat med informationsskyldigheten i allmänhet. Av beskrivningen bör framgå om det huvudsakligen handlar om information när den enskilde själv har lämnat informationen (art. 13 GDPR) och i vilken omfattning som information sker utifrån att förvaltningen fått informationen från någon annan än den enskilde själv (art. 14 GDPR) Bifoga: En eller flera informationstexter om behandling av personuppgifter som gått ut till de registrerade rörande någon/några av de behandlingar verksamheten har upprättade i sitt behandlingsregister.

Barn- och ungdomsnämnden registerförteckning bifogas. Barn- och ungdomsnämnden har inga behandlingar i dagsläget där nämnden är biträde. Samtliga personuppgiftsbehandlingar som idag sker i digitala system/tjänster finns redovisade i behandlingsregistret.

Utgångspunkten är att personuppgiftsbehandlingar inte ska förekomma om rättsligt stöd saknas. Personuppgiftsbehandlingar inom verksamheten bedöms vara nödvändiga i syfte att genomföra uppdraget att tillhandahålla och bedriva utbildning och annan pedagogisk verksamhet av hög kvalitet i enlighet med skollag och övriga författningar. Exempel på sådana behandlingar är mottagande av barn och elever och erbjudande av plats i förskola och skola, administrativa ändamål för att kunna planera, genomföra och följa upp elevernas utbildning, registrering av närvaro och frånvaro, dokumentation inför utvecklingssamtal och vid upprättande av individuella studieplaner, dokumentation av olika typer av utredningar, t.ex. om särskilt stöd och i undervisningen genom användandet av t.ex. en digital lärplattform, fortlöpande informera vårdnadshavare om elevens utveckling. Dessa personuppgiftsbehandlingar sker med stöd av den rättsliga grunden uppgift av allmänt intresse. När det gäller åtgärder som vidtas med stöd av skollagen, t.ex. beslut om betyg och beslut om särskilt stöd görs personuppgiftsbehandlingar med stöd av den rättsliga grunden myndighetsutövning. Samtycke används som rättslig grund för personuppgiftsbehandlingar som omfattar foto- film- och ljudupptagning som sker utanför skolans och förskolans ordinarie uppdrag, där lagstöd allmänintresse saknas för personuppgiftsbehandlingen. I dessa fall är syftet annat än pedagogiskt arbete. Det kan exempelvis vara att informera eller att marknadsföra verksamheten.

Särskilda överväganden görs vid behandling av känsliga uppgifter inom ramen för elevhälsoarbetet utifrån Skollagen 2 kap , 25-28 §§ , OSL 23 kap § 1-5, kap 4 § 3. Allmänt intresse utgör rättslig grund för behandlingen samt 26 a kap. skollagen, att känsliga person-

uppgifter om hälsa ska få behandlas med stöd av artikel 9.2 g GDPR om det är nödvändigt för ändamålet med behandlingen och behandlingen inte innebär ett otillbörligt intrång i den registrerades personliga integritet. Undantagna är personuppgiftsbehandlingar som sker i elevhälsan och som utförs inom hälso- och sjukvården. Sådan personuppgiftsbehandling omfattas i stället av bl.a. patientdatalagens (2008:355) bestämmelser. Det innebär att hälso- och sjukvårdspersonal inom elevhälsan som är skyldig att föra patientjournal och behandla personuppgifter enligt patientdatalagens bestämmelser även fortsättningsvis tillämpar den lagen med tillhörande föreskrifter.

Arbete med informationsskyldighet

Information till de registrerade sker på olika sätt beroende på kontaktväg. Standardhänvisningar finns på Alingsås kommuns hemsida[1] vilka också finns hänvisning till i Barn- och ungdomsförvaltningens portal (Arena för lärande) för kommunikation och tillgång till digitala tjänster.

I förvaltningens e-tjänster finns information till registrerade anpassade efter respektive behandling. Bifogat finns exempel på information till registrerade i samband med ansökan till grundsärskola samt vid ändring om vistelsetid i förskola.

[1] https://www.alingsas.se/kommun-och-politik/diarium-och-arkiv/sa-hanterar-vi-dina-personuppgifter/

3. Personuppgiftsincidenter

Beskriv verksamhetens förutsättningar för att identifiera och hantera personuppgift-incidenter. För att uppfylla ansvarsskyldigheten bör verksamhetens rutin för hanteringen vara dokumenterad. I de fall verksamheten är både personuppgiftsansvarig och person-uppgiftsbiträde bör rutinen omfatta båda scenarier. Beskriv också verksamhetens rutin för att bedöma incidenter, hantering av eventuell anmälan till tillsynsmyndigheten samt hur rutinerna tillgängliggörs och kommuniceras inom verksamheten. Beskriv också hur verksamheten lever upp till dokumentationsskyldigheten, att alla inträffade personuppgifts-incidenter dokumenteras. Dataskyddsombuden önskar också en redogörelse kring hur verksamheten arbetar för att uppmärksamma sina anställda om deras viktiga roll att larma vid misstänkt personuppgiftsincident och om de känner till hur de ska agera vid misstanke.

Hantering av personuppgiftincidenter

Alingsås kommuns rutin för hantering av personuppgiftsincidenter [2] finns bifogad och rutinen är framtagen av Kommunledningskontoret och gäller för samtliga nämnder/styrelser och vänder sig till alla medarbetare och chefer i kommunen. Rutinen ska ses över årligen och vid behov revideras av kommunledningskontoret.

Rutinen finns publicerad på kommunens intranät Kommunportalen tillsammans med länk till den e-tjänst som används inom kommunen för att anmäla en personuppgiftsincident.

Barn- och ungdomsförvaltningen har en kontaktperson/GDPR-samordnare som tar emot anmälan av personuppgiftsincidenter och samordnar arbetet utifrån den rutin som kommun-ledningskontoret tagit fram samt ger råd och stöd till verksamheten. Personuppgiftsansvarig delegerar till GDPR-samordnare att bedöma om en personuppgiftsincident ska anmälas till Integritetsskyddsmyndigheten.

Dataskyddsombud finns tillgänglig för konsultation avseende denna rutins alla delar men beslut fattas alltid av personuppgiftsansvarig själv

Anmälan och rapportering vid en personuppgiftsincident (utdrag ur rutinen)

1. Den anställde som själv upptäcker en potentiell incident eller får kännedom om en incident från ett personuppgiftsbiträde kontaktar omedelbart sin närmaste chef.
2. Ansvarig chef och den anställde genomför en första kartläggning av incidenten. Därefter fylls kommunens e-tjänst för anmälan av personuppgiftsincidenter i. Detta sker vanligtvis i samråd med GDPR-samordnare. Anmälan skickas per automatik till Barn- och ungdomsförvaltningens e-postlåda för hantering och utredning samt diarieföring. En kopia skickas till kommunledningskontoret i statistik- och samman-ställningssyfte.

   Anmälan innehåller en beskrivning av:

[2] https://alfresco.alingsas.se/share/proxy/alfresco/api/node/workspace/SpacesStore/283b6a5d-7c8a-4105-ac6a-59cc9b662333/content/thumbnails/pdf?c=force&lastModified=pdf%3A1662122222972&a=true

a. när incidenten upptäcktes
b. händelseförlopp, plats, inblandade program, system och tjänster etc.
c. vad som gjorts för att åtgärda eller mildra effekterna av incidenten
d. vilken typ av incident som har inträffat (t.ex. obehörigt röjande, förlust, ändring).
e. vilka personuppgifter som berörs av incidenten samt vilka kategorier av registrerade som berörs och hur många
f. vilka konsekvenser incidenten kan få
g. bedömning om incidenten ska anmälas till IMY
h. bedömning om de registrerade behöver informeras

3. GDPR-samordnare bedömer om det är fråga om en personuppgiftsincident och om den ska anmälas till Integritetsskyddsmyndigheten. Samordnaren genomför eventuell anmälan inom 72 timmar från att incidenten blivit känd. Diarienumret från ärendet i diariesystemet (Platina) anges som referensnummer vid anmälan. Diarieföring av själva anmälningen ska också ske hos den personuppgiftsansvarige. Delegationsbeslut ska upprättas för information till ansvarig nämnd. Dataskyddsombud finns att konsultera om ett sådant behov finns.
4. GDPR-samordnare gör bedömningen ifall de registrerade behöver informeras. Om de registrerade behöver informeras så tar ansvarig chef fram en informationsplan och ser till att den verkställs.
5. GDPR-samordnare initierar att ansvarig chef, vid behov i samråd med andra som kan bidra med bedömningen, gör en utredning om incidenten samt inkluderar en plan för att förhindra/minska risken för att liknande händelser sker igen. Utredningen med tillhörande plan för att förhindra/minska risken att liknande händelser sker igen diarieförs tillsammans med övrig dokumentation om incidenten i Platina. i ärendet. Bifogat finns den kommungemensamma utredningsmallen[3] som används för utredning och analys av incidenter.

Om flera personuppgiftsansvariga är en del av samma personuppgiftsincident så ska en anmälan per personuppgiftsansvarig upprättas.

Informationsinsatser har genomförts för rektorer och IKT-ansvariga på förskolor/skolor rörande GDPR, dataskyddsfrågor och personuppgiftsincidenter. Som en del av ”Handlingsplan informationssäkerhet och Dataskydd” planeras utbildningsinsatser inom området informationssäkerhet och dataskydd för samtliga anställda.

Rutin för att bedöma incidenter

Om en inträffad händelse bedöms att den ska anmälas till Integritetsskyddsmyndigheten, (IMY), så ska detta ske inom 72 timmar från den tidpunkt som den inträffade. Därför är det viktigt att den interna hanteringen och rapporteringen sker skyndsamt och i nära anslutning till att händelsen upptäcks.

[3] https://alfresco.alingsas.se/share/proxy/alfresco/api/node/content/workspace/SpacesStore/2d1a0970-3c5e-4efd-a624-c8eea188f5a/Utredning%20och%20analys%20efter%20intr%C3%A4ffad%20personuppgiftsincident%2C%20mall.docx?a=true

Avväganden rörande anmälan till tillsynsmyndigheten (IMY) görs utifrån IMYs riktlinjer ”Riktlinje om anmälan av personuppgiftsincidenter”, och vid behov i samråd med dataskyddsombudet.

Utifrån aktuellt nuläge i verksamheten rörande kompetens för dataskydd är bedömningen att det finns förutsättningar för att identifiera och utreda personuppgiftsincidenter. Samtliga systemansvariga för de digitala system som används för behandling av uppgifter samt Nyckelpersoner och chefer har god kunskap om personuppgiftshantering och tillvägagångssätt vid eventuell incident. Förvaltningen har identifierat behov av ytterligare kompetenshöjande insatser som riktar sig till samtliga i organisationen för att höja den generella kompetensen. Behov finns även inom den kommunala organisationen vad gäller förtydligande av roller och ansvar för kommungemensamma system.

Under 2022 har sex personuppgiftsincidenter identifierats. Inga av dessa har bedömts vara föremål för anmälan till IMY.

4. Registrerades rättigheter

Beskriv verksamhetens förutsättningar för att hantera de registrerades rättigheter, till exempel registerutdrag eller radering. Beskriv gärna hur verksamheten hanterar en begäran om ett registerutdrag eller radering av personuppgifter. En förutsättning för att verksamheten ska kunna hantera de registrerades rättigheter är att man har en process och rutiner för arbetet, så att den registrerades personuppgifter enkelt kan lokaliseras vid efterfrågan. Bifoga: Rutin kopplat till hanteringen av de registrerades rättigheter. Bifoga också om det finns en rutin för att hantera ett tillbakadragande av samtycke. Bifoga också antal ärenden som hanterats under 2022 rörande registrerades rättigheter.

Alingsås kommuns rutiner för att hantera begäran om registerutdrag[4] och begäran om rättelse/radering [5] finns bifogade och de är framtagna av Kommunledningskontoret.

Registrerade begär registerutdrag samt rättelse/radering via kommungemensamma e-tjänster som finns tillgängliga på kommunens hemsida. Vad gäller frågan om de registrerades rättigheter, utöver informationsskyldigheten, finns tillgängliga e-tjänster för begäran om registerutdrag och/eller begära rättelse/radering av personuppgifter.

Begäran om registerutdrag alternativt rättelse/ändring skickas per automatik till Barn- och ungdomsförvaltningens e-postlåda för hantering samt diarieföring. GDPR-samordnare på Barn- och ungdomsförvaltningen hanterar och samordnar begäran om registerutdrag och rättelse/radering. När en begäran om registerutdrag inkommer fastställs först vilken roll den registrerade har i verksamheten, såsom vårdnadshavare, elev, personal eftersom all personuppgiftshantering är rollstyrd. Utifrån identifierad roll sammanställs vilka uppgifter som behandlas i vilka system, för vilka syften, hur länge informationen lagras osv. Dessa uppgifter meddelas sedan den registrerade på det sätt som den valt. I vissa verksamhetssystem finns möjlighet för den registrerade att själv ta ut ett registerutdrag (t.ex. närvarosystemet Skola 24). Förekommer inte personen i Barn- och ungdomsförvaltningens system/register, meddelas detta den registrerade skriftligen.

För tillbakadragande av samtycke uppmanas den registrerade att skicka in en anmälan på nytt via Barn- och ungdomsförvaltningens e-tjänst för samtycke (alternativt fylla i blanketten för samtycke) och lämna till aktuell förskola/skola för hantering. Information om hur den registrerade ska gå tillväga vid tillbakadragande av samtycke finns i den e-tjänst och blankett som används för samtycke.

Under 2022 har en begäran om rättelse/radering av personuppgifter inkommit till Barn- och ungdomsförvaltningen.

---

[4] https://alfresco.alingsas.se/share/proxy/alfresco/api/node/workspace/SpacesStore/7af7df35-87df-4b9a-baae-d03a8d62eb0b/content/thumbnails/pdf?c=force&lastModified=pdf%3A1567606356321&a=true

[5] https://alfresco.alingsas.se/share/page/site/dokument---styrande-dokument/document-details?nodeRef=workspace://SpacesStore/ab5541eb-95f0-4152-b699-c033e5226f10

5. Konsekvensbedömningar

Beskriv verksamhetens förutsättningar för att kunna identifiera när en konsekvensbedömning ska göras samt arbetsprocessen vid genomförandet av en konsekvensbedömning. Även verksamhetens rutiner för arbetet med konsekvensbedömningar samt hur dataskyddsombudet involveras i arbetet. Beskriv också verksamhetens rutin för att hantera de risker som identifieras i konsekvensbedömningen, samt hur genomförda konsekvensbedömningar följs upp och hålls aktuella. Bifoga: Om sådan finns, en genomförd konsekvensbedömning och eventuell mall som ska användas i detta arbete.

Alingsås kommun har en kommungemensam e-tjänst för konsekvensbedömning av dataskydd. E-tjänsten används i syfte att identifiera huruvida nya eller förändrade personuppgiftshanteringar kräver konsekvensbedömning samt för att genomföra en konsekvensbedömning innehållande en riskanalys, framtagning av rutiner/åtgärder för att bemöta risker och dokumentera hur kraven i Dataskyddsförordningen uppfylls.

Barn- och ungdomsförvaltningen har inte genomfört några konsekvensbedömningar avseende dataskydd enligt Dataskyddsförordningen i dagsläget. Konsekvensbedömning planeras att genomföras för nuvarande behandling av Google Workspace for Education samt inför nya personuppgiftsbehandling som bedöms innebära hög risk för de registrerades fri- och rättigheter.