Katrineholm

Kallelse

Viadidakt

2022-11-28

Sammanträdande organ

Viadidaktnämnden

Tid

2022-12-06 klockan 09:00

Plats

KTS-salen, Drottninggatan 18 Katrineholm

Nr	Ärende	Beteckning
1	Upprop	
2	Val av justerare	
3	Fastställande av dagordning	
4	Verksamhetsinformation	
5	Kontroll av dataskyddsefterlevnad för Viadidaktnämnden 2022	VIAN/2022:57
6	Förlängt sammanträde för Viadidaktnämnden	VIAN/2022:48
7	Anmälan av delegationsbeslut	
8	Meddelanden	

Gunilla Magnusson (S)

Ordförande

Katrineholm
VIADIDAKT

Stab och service

Datum
2022-11-23

Vår beteckning
VIAN/2022:57 - 1.5.2 - Mäta verksamhetskvalitet

Mottagare:

Vår handläggare
David Andersson

Handläggare telefon
0150-57840

Handläggare e-post
David.Andersson@viadidakt.se

Kontroll av dataskyddsefterlevnad för Viadidaktnämnden

Sammanfattning av ärendet

Dataskyddsförordningen (GDPR) gäller som lag i Sverige och innehåller regler om hur man får behandla personuppgifter. Den personuppgiftsansvarige (varje nämnd/styrelse) är ansvarig för att personuppgifter behandlas i enlighet med gällande lagstiftning.

Personuppgiftsansvarig får en återkoppling i form av denna rapport från kontroll av dataskyddsefterlevnad. Sydarkivera har i rollen som dataskyddsombud för Viadidaktnämnden rekommenderat vidare arbete i nedanstående punkter.

1. Sydarkivera rekommenderar nämnden att planera in regelbunden information om aktuella registerförteckningar.
2. Sydarkivera rekommenderar nämnden att göra en risk- och konsekvensbedömning med anledning av tredjelandsöverföringar. Utifrån denna bedömning tas en åtgärdsplan fram.
3. Sydarkivera rekommenderar nämnden att påbörja ett arbete med att informationssäkerhetsklassa informationen.

Ärendets handlingar

- Rapport från kontroll av dataskyddsefterlevnad för Viadidaktnämnden i Katrineholms kommun 2022

Förvaltningens bedömning

Förvaltningen har beaktat rekommendationerna och inlett en översyn utifrån dessa. I de två senare punkterna finns redan ett påbörjat arbete men det kan finnas ett behov av att förstärka detta ytterligare. I övrigt får kontrollarbetet anses som tillfredsställande.

David Andersson
Utredare

Rapport från kontroll av dataskyddsefterlevnad för viadidaktnämnden i Katrineholms kommun 2022

Ansluten part Katrineholms kommun
Personuppgiftsansvarig Viadidaktnämnden
Svarande på enkäten Johan Haarala, johan.haarala@viadidakt.se

Dataskyddsförordningen (GDPR) gäller som lag i Sverige och innehåller regler om hur man får behandla personuppgifter. Den personuppgiftsansvarige (varje nämnd/styrelse) är ansvarig för att personuppgifter behandlas i enlighet med gällande lagstiftning. Enligt art 37 GDPR måste personuppgiftsansvariga myndigheter ha utsett ett dataskyddsombud för sin verksamhet.

Sydarkiveras tjänst som dataskyddsombud utförs av ett team som består av jurist, informationssäkerhetsspecialist och arkivarie. Dataskyddsombudets viktigaste uppgifter är att ge råd och stöd i dataskyddsfrågor och kontrollera den personuppgiftsansvariges efterlevnad av GDPR och annan dataskyddslagstiftning. Tillsyn görs av den nationella myndigheten Integritetsskyddsmyndigheten (IMY).

Kontrollen av efterlevnaden hos de som är anslutna till tjänsten gemensamt dataskyddsombud görs i olika moment.

Ett årligt moment är att dataskyddsombudet tar fram en enkät för kontroll av dataskyddsefterlevnad som varje personuppgiftsansvarig ska besvara. Personuppgiftsansvarig får en återkoppling i form av denna rapport från kontroll av dataskyddsefterlevnad.

Denna rapport innehåller frågorna från självvärderingsenkäten samt ansluten personuppgiftsansvarigs svar på enkäten. Vidare finns kommentarer från dataskyddsteamet och en sammanvägd bedömning med förslag till åtgärder.

Rapporten lämnas till personuppgiftsansvarig för kännedom och vid behov för åtgärd.

Vill dataskyddssamordnaren eller någon annan från förvaltningen ha en muntlig uppföljning utifrån denna rapport kan man kontakta dataskyddsteamet för att boka en tid för möte, företrädesvis via webb. Vid behov eller önskemål från ansluten part kan också en extra kontroll av något område inom dataskydd genomföras.

Integritetsskyddsmyndigheten (IMY) kontrollerar att dataskyddsbestämmelserna följs. IMY kan göra utredningar utifrån t ex klagomål, anmälda personuppgiftsincidenter, förhandssamråd eller enligt sin egen tillsynsplan.

IMY har ett antal s k korrigerande befogenheter att ta till, t ex skriftlig varning, reprimand, föreläggande eller förbud.

Utöver eller i stället för övriga korrigerande åtgärder kan IMY besluta om att ta ut en sanktionsavgift. Nästan alla överträdelser av dataskyddsförordningen kan leda till administrativa sanktionsavgifter.

Organisation och struktur för dataskyddsarbetet

En personuppgiftsansvarig (PUA) är en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som ensam eller tillsammans med andra bestämmer ändamål och medel för behandlingen av personuppgifter.

Normalt sett är varje myndighet (nämnd, styrelse eller annan myndighet) PUA för sin verksamhet. Det ska framgå i reglementet vilket ansvar myndigheten har.

PUA ansvarar bl a för att utse dataskyddsombud, för att föra register över behandlingar, fastställa laglig grund för behandling, fastställa ändamål och syfte med behandling, anmäla personuppgiftsincidenter, vidta åtgärder så att behandlingen är säker, samt vidta åtgärder för att säkerställa att dataskyddsförordningen följs.

För att uppgifterna ska utföras behöver det finnas en organisation och struktur för dataskyddsarbetet.

1. Finns en beslutad lokal organisation för dataskyddsarbete inom er myndighet?

Ja

Kommentarer:
Det är viktigt att det finns en lokal organisation för dataskyddsarbetet och att den är beslutad och känd inom verksamheten. Dataskyddsarbetet ska vara en naturlig del av det administrativa arbetet. Det bör vara dataskyddssamordnaren som leder och samordnar det lokala dataskyddsarbetet.

Det är bra att det finns en beslutad lokal organisation inom er organisation då det är en förutsättning för att dataskyddsarbetet ska fungera.

2. Är arbetsuppgifterna inom dataskydd fördelade på utsedda tjänstepersoner inom er myndighet?

Ja

Kommentarer:

Roller för dataskyddsarbete behöver utses då det är en förutsättning för att organisationen ska arbeta systematiskt med dataskyddsfrågor. Dataskyddsteamet föreslår att man kallar rollerna dataskyddssamordnare och dataskyddsredogörare, men man kan naturligtvis välja andra benämningar. Rollen som övergripande kontaktperson till oss inom dataskyddsteamet vill vi gärna att ni kallar dataskyddssamordnare.

Det är bra att roller för dataskyddsarbetet har utsetts och förutsättningar finns för ett systematiskt dataskyddsarbete.

3. Får de som utsetts att arbeta med dataskyddsfrågorna inom er myndighet utbildning på dataskyddsområdet?

Ja

Kommentarer:
Att få regelbunden utbildning är en grundförutsättning för att medarbetare ska kunna göra ett bra jobb och utvecklas i sina kunskaper och färdigheter. Sydarkivera erbjuder grundutbildning inom dataskydd och informationssäkerhet som ingår i tjänsten. Dessa utbildningar genomförs digitalt vid fyra tillfällen per år. Vidare erbjuds nätverksträffar med fördjupande utbildningsmoment och erfarenhetsutbyten vid fyra tillfällen per år som också ingår i tjänsten.

Det är bra att de som utsetts att arbeta med dataskyddsfrågor får utbildning i dataskyddslagstiftningen och vi rekommenderar att ni fortsätter uppmuntra medarbetare till att delta i våra dataskyddsutbildningar.

4. Finns det en rutin för att informera personuppgiftsansvarig myndighet om sitt ansvar enligt dataskyddslagsstiftningen?

Ja

Kommentarer:
Personuppgiftsansvarig myndighet behöver få information om sitt ansvar enligt dataskyddslagstiftningen och det behöver finnas en rutin för detta. Normalt sett är det ju inte personuppgiftsansvarig själv som utför dataskyddsarbetet, men personuppgiftsansvarig behöver känna till sin roll och sitt ansvar. Det är lämpligt att t ex lägga in det som ett informationsärende i årsplaneringen eller göra det till en del av nyvaldutbildningen. Vi

rekommenderar att information till personuppgiftsansvarig om sin roll och ansvar bör lämnas minst en gång per mandatperiod. Är det flera förtroendevalda som byts under mandatperioden bör information lämnas till nya förtroendevalda. En fördel med att informationen lämnas vid ett sammanträde är att det dokumenteras i protokoll och kan följas upp.

Det är bra att personuppgiftsansvarig regelbundet får information om sin roll och sitt ansvar och att ni har en rutin för att fånga upp denna fråga.

5. Har personuppgiftsansvarig myndighet delegerat beslutanderätt för dataskyddsfrågor i sin delegationsordning?

Ja

Kommentarer:
Dataskyddsteamet har tagit fram en mall för delegation av dataskyddsfrågor som kan inkorporeras i den sammanhållna delegationsordningen för styrelsen eller nämnden. Att ha delegerat de ärenden som enligt dataskyddslagstiftningen kan komma att behöva fattas beslut om är ett effektivt sätt att jobba. Ärendetyperna blir synliga för både organisationen och för personuppgiftsansvarig och det finns en beredskap och planering när ärende uppstår.

Det är bra att ni har delegerat beslutanderätt för dataskyddsfrågor inom er verksamhet.

6. Vilka styrdokument gäller för er myndighet vad gäller dataskyddsfrågor?

Informationssäkerhetspolicy

Kommentarer:
Dataskyddsförordningen och annan dataskyddslagstiftning gäller, men organisationen behöver bestämma hur det ska genomföras lokalt genom egna styrdokument.

Vi rekommenderar att ni ser över arbetet med styrdokument för dataskydd och att ni tar fram och beslutar om egna styrdokument för dataskydd anpassade för er verksamhet.

Dataskyddsombudet (DSO)

Den personuppgiftsansvarige ska utse dataskyddsombud om behandlingen utförs av myndighet eller annat offentligt organ – tidigare var det frivilligt med PuL-ombud för myndigheter.

Dataskyddsombudet (DSO) ska bland annat ge råd och ha en övervakande funktion gentemot personuppgiftsansvarig för att kontrollera att dataskyddsförordningen följs. Den som utsett dataskyddsombud ska offentliggöra dataskyddsombudets kontaktuppgifter och meddela dessa till Integritetsskyddsmyndigheten (IMY).

7. Har ni utsett dataskyddsombud och anmält ombudet till IMY enligt art 37?

Ja

Kommentarer:
Att utse dataskyddsombud och anmäla kontaktuppgifter till Integritetsskyddsmyndigheten är en grundläggande åtgärd. När man har avtal med Sydarkivera om gemensamt dataskyddsombud är det den som Sydarkivera anvisar som ska utse och anmälas. För närvarande är det förbundsjurist Therese Jigsved som ska utses som dataskyddsombud. Kontaktuppgift för e-post är dataskyddsteamets funktionsbrevlåda dataskydd@sydarkivera.se och telefonnummer 0472 – 39 10 16.

Det är bra att ni har utsett och anmält dataskyddsombud.

Registerförteckningar

Varje personuppgiftsansvarig (PUA) ska föra ett register över behandlingar som utförts under dess ansvar. Registret ska bland annat innehålla kontaktuppgifter till PUA och dataskyddsombud, ändamålen med behandlingen, typer av registrerade och kategorier av personuppgifter, gallringsfrister och säkerhetsåtgärder.

8. Har ni upprättat registerförteckningar enligt art 30 GDPR?

Ja

Kommentarer
Att upprätta registerförteckningar över behandling av personuppgifter är ett grundläggande krav på personuppgiftsansvarig. Det är normalt sett inte personuppgiftsansvarig själv som gör förteckningen, men det är personuppgiftsansvarig som ansvarar för att det blir gjort och för att det finns resurser som gör arbetet.

Det är bra att ni gått igenom era personuppgiftsbehandlingar och förtecknat dem i register.

9. Har ni rutiner för arbetet registerförteckningarna?

Ja

Kommentarer:
Det är viktigt att organisationen har bestämt hur arbetet med registerförteckningen ska gå till genom att anta egna rutiner. Det kan gälla t ex vilken mall eller systemstöd som ska användas för registerförteckning, men även för att hålla registerförteckningen aktuell.

Det är bra att ni har rutiner för ert arbete med registerförteckningarna.

10. Får er myndighet information om aktuella registerförteckningar över personuppgiftsbehandlingar?

Nej

Kommentarer:

Personuppgiftsansvarig ansvarar för att registerförteckningarna hålls aktuella och behöver därför få regelbunden information om statusen. Informationen bör lämnas vid sammanträde så att informationen dokumenteras i protokoll och kan följas upp. Det är lämpligt med information ungefär en gång per år.

Vi rekommenderar att ni planerar in regelbunden information om aktuella registerförteckningar till personuppgiftsansvarig i sammanträdeskalendern så att informationen dokumenteras i protokoll.

Tredjelandsöverföring

Det finns en allmän princip i art. 44 GDPR om att överföring av personuppgifter till tredje land (utanför EU/EES) eller en internationell organisation bara få ske om PUA /PUB uppfyller villkoren i GDPR. Annars är det förbjudet att föra personuppgifter utanför EU/EES.

Personuppgifter får överföras till tredjeland eller internationell organisation om EU-kommissionen har beslutat att mottagaren kan säkerställa en adekvat skyddsnivå (art. 45). Vidare finns det användande av EU-kommissionens standardavtalsklausuler enligt art. 46, bindande företagsbestämmelser enligt art. 47 eller undantag i särskilda situationer enligt art. 49. Vid genomgång av tredjelandsöverföringarna behöver man dokumentera i register-förteckningen vilket rättsligt stöd (överföringsmekanism) som används.

Dataskyddsombudet har tagit fram en vägledning med anledning av Schrems II-domen med förslag till åtgärder som man behöver göra.

11. Har ni med anledning av Schrems II-domen gått igenom och fastställt vilka behandlingar hos er som innebär tredjelandsöverföring?

Ja

Kommentarer:
Den 16 juli 2020 meddelade EU-domstolen en dom i det så kallade Schrems II-målet. EU-domstolen slår fast att Privacy Shield-avtalet mellan EU och USA inte ger ett tillräckligt skydd för personuppgifter när dessa förs över till USA och ogiltigförklaras därför.

Dataskyddsteamet har tagit fram en vägledning med anledning av Schrems II-domen och för mer vägledning hänvisar vi till den och de vägledningar som den europeiska dataskyddsstyrelsen (EDPB) har tagit fram. Som ett första steg rekommenderar EDPB att personuppgiftsansvariga ska kartlägga alla tredjelandsöverföringar som görs. Detta görs genom att man går igenom avtal med leverantörer, även vad gäller underleverantörer. Resultatet av genomgången dokumenteras i registerförteckningen. Utifrån kartläggningen behöver man sedan gå vidare, analysera resultatet och ta fram en åtgärdsplan.

Att känna till vilka tredjelandsöverföringar som görs är nödvändigt för att veta vilka ytterligare åtgärder ni behöver vidta med anledning av Schrems II-domen. Det är bra att ni har gått igenom och kartlagt vilka tredjelandsöverföringar som görs inom er verksamhet. Det

är ett första steg i arbetet med att uppfylla lagkraven i GDPR med anledning av Schrems II-domen.

12. Har ni fastställt med vilket stöd som ni gör tredjelandsöverföringen?

Ja

Kommentarer:
Överföring av personuppgifter till tredjeland får bara ske om man uppfyller villkoren för det i GDPR. Gör man inte det är det förbjudet att föra personuppgifter utanför EU/EES.
Om man gör tredjelandsöverföring är det därför viktigt att veta med vilket rättsligt stöd i förordningen som man gör det.

Det är bra att ni har gått igenom och fastställt vilket rättsligt stöd som ni har för era tredjelandsöverföringar.

13. Har ni utifrån kartläggningen gjort en risk- och konsekvensbedömning med anledning av de tredjelandsöverföringar ni har?

Delvis

Kommentarer:
Använder man sig av standardavtalsklausuler som rättsligt stöd för att göra tredjelandsöverföringar behöver man göra risk- och konsekvensbedömningar för att veta vilka risker som finns, men också vilka skyddsåtgärder eller andra åtgärder som behöver göras. Skyddsåtgärder kan vara tekniska, organisatoriska eller beroende på avtalsvillkor.

Tänk också på att nya standardavtalsklausuler tagits fram under 2021 och att senast den 27 december 2022 behöver samtliga avtal som innefattar de gamla standardavtalsklausulerna vara ersatta med de nya standardavtalsklausulerna. Det är alltså hög tid att se över och uppdatera befintliga avtal med de nya standardavtalsklausulerna i den utsträckning som ni använder er av standardavtalsklausuler.

Det är bra att ni har påbörjat arbetet med risk- och konsekvensbedömning på detta område och vi rekommenderar att ni slutför arbetet och genomför de åtgärder ni har kommit fram till.

De registrerades rättigheter

Enligt art 12 GDPR ska den personuppgiftsansvarige vidta lämpliga åtgärder för att till de registrerade tillhandahålla all information som avses i art 13 och 14 samt all kommunikation enligt art 15-22 och 34.

Informationen ska bland annat vara begriplig, klar och tydlig, särskilt den informationen som är riktad mot barn.

De viktigaste rättigheterna är:
-Få information om sina rättigheter – art 12
-Få tillgång till sina personuppgifter – art 15
-Få felaktiga personuppgifter rättade – art 16
-Få sina personuppgifter raderade (sällan hos myndigheter) – art 17
-Invända mot att personuppgifter används för t ex direktmarknadsföring – art 18
-Få information om vidtagen rättelse eller radering – art 19
-Rätt att flytta personuppgifterna (dataportabilitet) – art 20

14. Har ni rutiner för att hantera de registrerades rättigheter?

Ja

Kommentarer
Den registrerade, det vill säga den vars personuppgifter behandlas, har ett antal rättigheter enligt dataskyddsförordningen (GDPR). Personuppgiftsansvariga (PUA) har ett ansvar för att ha rutiner på plats för att kunna lämna information och kunna handlägga dessa rättigheter när någon begär det.

Under våren 2022 har dataskyddsteamet tagit fram riktlinjer för hantering av registrerades rättigheter där det finns mallar för beslut och rutiner för samtliga rättigheter.

Det är bra att ni har rutiner för att handlägga de registrerades rättigheter enligt GDPR.

15. Var informerar ni någonstans om de registrerades rättigheter?

Webbplats, blanketter, E-tjänster och servicecenter.

Kommentarer
Det är bra att ha information om de registrerades rättigheter på många ställen så att informationen har bra förutsättningar för att nå fram.

Man kan välja att informera i olika skikt beroende på vilket sätt man informerar på. Ibland kan det vara lämpligt att informera mycket kort och hänvisa till exempelvis hemsida för mer information. När det gäller information behöver man också tänka på att annan lagstiftning också ställer krav på informationen, t ex service och tillgänglighet för alla.

Personuppgiftsbiträden

Ett personuppgiftsbiträde kan vara en fysisk eller juridisk person, offentlig myndighet eller annat organ som behandlar personuppgifter för den personuppgiftsansvariges räkning. Personuppgiftsbiträde förkortas ofta PUB.

Personuppgiftsansvarig ska endast anlita biträden som ger tillräckliga garantier om att behandlingen av personuppgifter sker på ett sådant sätt att de uppfyller kraven i GDPR. När uppgifter behandlas av ett personuppgiftsbiträde ska hanteringen regleras genom ett s k PUB-avtal.

16. Anlitar ni personuppgiftsbiträden och har ni ingått PUB- avtal med instruktioner enligt art 28 GDPR?

Ja, vi anlitar personuppgiftsbiträden och vi har avtal med samtliga biträden.

Kommentarer:
Sveriges Kommuner och Regioner (SKR) har tagit fram mallar för PUB-avtal och instruktioner. Vi rekommenderar att alla använder sig av dessa mallar och tar fram förslag till PUB-avtal och instruktioner utifrån dessa mallar. Äldre PUB-avtal kan behöva en genomgång, men de är inte ogiltiga pga att de hänvisar till PuL i stället för GDPR. Men vi rekommenderar att gärna gå igenom äldre PUB-avtal och ta fram förnyade avtal.

Det är mycket viktigt att ha PUB-avtal med relevanta, tydliga och korrekta instruktioner. Om ett biträde inte får tillräckligt tydliga instruktioner om hur behandling får ske eller inte alls tar fram instruktioner faller ansvaret för dessa fel tillbaka på personuppgiftsansvarig.

En del systemleverantörer använder sig i stället av standardvillkor som vid behov ensidigt kan ändras av leverantören. Det är svårt att praktiskt få till regelrätta PUB-avtal med instruktioner med sådana leverantörer. Det kan också vara svårt att få till PUB-avtal med leverantörer av appar och sociala medier. Ett sätt att hantera det är att i möjligast mån undvika sådana leverantörer. Anser ni att ni ändå måste anlita en sådan leverantör rekommenderar vi att ni ställer frågor om personuppgiftsbehandlingen, framför era synpunkter och krav och dokumenterar leverantörens svar. Men det är ni som personuppgiftsansvarig som står risken om man står utan PUB-avtal.

Det är mycket bra att ni har PUB-avtal med samtliga biträden, men gör gärna regelbunden kontroll av aktualiteten av PUB-avtal och dess instruktioner.

17. Har ni rutiner för framtagande av PUB-avtal med instruktioner?

Ja

Kommentarer:
Att ha bra PUB-avtal med instruktioner är viktigt för att kunna styra hur biträdet får behandla era personuppgifter. Det är viktigt att man inom organisationen har bestämt hur arbetet med PUB-avtal ska gå till i form av rutiner.

Det är bra att ni har rutiner för framtagande av PUB-avtal.

Risk- och konsekvensbedömningar

Om en typ av behandling sannolikt leder till en hög risk för fysiska personers rättigheter och friheter ska PUA före behandlingen göra en bedömning av den planerade behandlingens konsekvenser för skyddet av personuppgifter.

Nya system innebär ofta nya tekniska möjligheter och införskaffande av nya system i verksamheten är ofta ett tillfälle då risk- och konsekvensbedömning behöver göras. För att få fram olika perspektiv och ta vara på kunskap som finns i organisationen är det bra att det finns en utsedd grupp med olika kompetenser som utför risk- och konsekvensbedömningen.

18. Har ni rutiner för genomförande av risk- och konsekvensbedömningar?

Ja

Kommentarer:
Om man inte har en rutin för risk- och konsekvensbedömning kan det blir osäkert vem som ska göra vad innan man påbörjar en ny behandling. Eller man kanske helt missar att göra en risk -och konsekvensbedömning om man inte har en känd rutin. Med hjälp av denna rutin kan den personuppgiftsansvarige enklare bedöma vilka behandlingar som innebär en särskilt stor risk för personers fri- och rättigheter.

Det är bra att ni har en rutin för risk- och konsekvensarbete.

19. Gör ni risk- och konsekvensbedömningar om behandlingen sannolikt leder till hög risk för fysiska personers rättigheter innan en ny behandling påbörjas?

Ja

Kommentarer:
Det är viktigt att konsekvent göra risk- och konsekvensbedömningar när en ny behandling sannolikt leder till hög risk. Dels är på grund av att det är ett krav enligt art. 35 GDPR, men också för att det leder till högre kvalitet i verksamheten när man konstaterar risker, konsekvenser och åtgärder för att minimera riskerna.

IMY har tagit fram en förteckning över när en konsekvensbedömning ska göras och vi rekommenderar att man tar del av den och följer IMY:s rekommendationer.

Det är bra att ni gör risk- och konsekvensbedömningar när en ny behandling sannolikt leder till hög risk. Vi rekommenderar att ni fortsätter med detta arbete.

20. Vilka tjänstepersoner är utsedda att utföra era risk- och konsekvensbedömningar?

Andra personer, ange vilka: kvalitetsstrateg och IKT-samordnare.

Kommentarer:
När man jobbar med dataskyddsfrågor och riskarbete är det en fördel att ha med personer med olika kompetenser och erfarenheter för att få fram så många bra perspektiv och bedömningar som möjligt.

Personuppgiftsincidenter

En personuppgiftsincident är en säkerhetsincident som kan innebära risker för människors friheter och rättigheter. Riskerna kan innebära att någon förlorar kontrollen över sina uppgifter eller att rättigheterna inskränks. En personuppgiftsincident kan få allvarliga konsekvenser för enskilda.

En personuppgiftsincident som inte hanteras på rätt sätt kan också påverka tilltron till den organisation som behandlar personuppgifter. Allvarliga incidenter kan också leda till att Integritetsskyddsmyndigheten inleder granskning med sanktionsavgift som följd.

21. Har ni rutiner för hantering av personuppgiftsincidenter med fastställd ansvarsfördelning?

Ja

Kommentarer:
När en personuppgiftsincident inträffar blir det ofta en allmän oro på en arbetsplats. Finns inte rutiner med fastställd ansvarsfördelning kan det bli svårt att agera på ett snabbt och effektivt sätt. Risken ökar för att personers fri- och rättigheter påverkas. Uppgift om vem som har befogenhet att anmäla personuppgiftsincident och vem som har uppdrag att dokumentera personuppgiftsincidenter bör finnas med i rutinerna. Dataskyddsteamet har tagit fram mallar för hantering av personuppgiftsincidenter som man kan utgå ifrån.

Det är bra att ni har rutin för hantering av personuppgiftsincidenter med fastställd ansvarsfördelning för att få en snabb och effektiv hantering av personuppgiftsincidenter.

22. Hur informeras personal om rutiner för personuppgiftsincidenthantering?

Intranät och arbetsplatsträff.

Kommentarer:
När en personuppgiftsincident inträffar blir det ofta en allmän oro och osäkerhet på arbetsplatsen. Det är bra och nödvändigt att se till att alla anställda känner till vad som ska göras om en personuppgiftsincident inträffar. Därför är det viktigt att alla i personalen känner till att det finns rutiner som ska användas. Det är bra att ni informerar all personal om rutiner för hantering av personuppgiftsincidenter på arbetsplatsträffar, intranät och liknande.

23. Får personuppgiftsansvarig information om anmälda personuppgiftsincidenter?

Ja

Kommentarer:
Det är viktigt att den som är personuppgiftsansvarig får information om anmälda personuppgiftsincidenter som har förekommit inom dennes ansvarsområde. Detta för att bedöma åtgärder som behöver göras. Det är den som är personuppgiftsansvarig som har hela ansvaret för de personuppgiftsbehandlingar som görs inom verksamheten.

Det är en nödvändighet för den som är personuppgiftsansvarig att känna till de anmälda personuppgiftsincidenter som inträffar så det är bra att ni informerar om det.

Informationssäkerhet

Enligt art 5 och art 32 GDPR ska personuppgifter behandlas på ett säkert sätt. PUA ska vidta säkerhetsåtgärder som säkerställer lämplig säkerhet för personuppgifterna, inbegripet skydd mot obehörig eller otillåten behandling och mot förlust, förstöring eller skada genom olyckshändelse. Detta ska göras med användning av lämpliga tekniska eller organisatoriska åtgärder (integritet och konfidentialitet).

24. Informationssäkerhetsklassar ni den informationen som er myndighet hanterar?

Delvis

Kommentarer:
Att informationssäkerhetsklassa sin information är en viktig del av informationssäkerhetsarbetet. Klassning görs för att organisationen ska få en bild av vilken information myndigheterna hanterar, hur känslig den är och hur den bör hanteras och förvaltas. Varje myndighet bör klassificera all sin information.

Det är bra att ni delvis informationssäkerhetsklassar er information. Vi rekommenderar att ni fortsätter arbetet och ha som mål att klassa alla informationstyper.

25. Finns fastställda roller runt systemförvaltning (dvs systemägare, systemförvaltare, driftansvar) hos er?

Ja, övergripande systemförvaltning inom vår kommun

Kommentarer:
Att ha fastställda roller för systemförvaltning är en viktig del i att ha ordning och reda i sin förvaltning.

Det är bra att ni har fastställda roller.

Frågor om GDPR i samband med upphandling

I samband med att organisationen ska skaffa nya system är det bra att tänka igenom så att det ställs krav i upphandlingsunderlaget även på frågor som rör dataskydd. Vid upphandling är det viktigt att adekvata krav på val av säkerhetslösningar, behörighetskontroller, överföringsteknik, lagringstjänster mm ställs. Många myndigheter anlitar upphandlingscentraler som sköter upphandlingarna åt myndigheterna och även där behöver myndigheterna säkerställa att dessa krav finns med.

26. Har ni en checklista för dataskyddsfrågor som behöver beaktas i samband med upphandling av nya system?

Ja

Kommentarer:
I samband med upphandling av nya system är det många saker att ta ställning till och dataskyddsfrågorna behöver beaktas redan på detta stadium.

Det är också viktigt att man har olika roller klara för sig. Den upphandlande organisationen är ofta personuppgiftsansvarig och leverantören är ofta biträde. Vid upphandling måste ansvar, roller och villkor för personuppgiftsbehandlingen framgå redan av upphandlingsdokumenten, bland annat genom krav på anbudsgivarna, krav på tjänsten och genom särskilda kontraktsvillkor.

Ofta krävs samverkan mellan olika funktioner hos den upphandlande myndigheten. Funktioner som bör involveras är IT-säkerhetsansvariga, jurister och dataskyddssamordnare. Dataskyddsombudet kan också tillfrågas för vägledning.

Det är bra att ha någon form av checklista för dataskyddsfrågor i samband med upphandling av nya system. På Upphandlingsmyndighetens hemsida finns bra information om vad man kan tänka på vid GDPR och upphandling.

Det är bra att ni har tagit fram en checklista för dataskyddsfrågor vid upphandling av nya system.

27. Ställs det krav på lämplig säkerhet för personuppgiftsbehandlingar vid upphandling av nya system som ni berörs av?

Ja

Kommentarer:
Enligt dataskyddsförordningen ska personuppgiftsansvarig säkerställa lämplig säkerhet för de personuppgifter som hanteras, inbegripet skydd mot obehörig eller otillåten behandling och mot förlust, förstöring eller skada genom olyckshändelse. Det kan vara svårt att i efterhand ändra kravställningar på säkerhetsåtgärder. Oftast blir det åtgärder som blir kostnadsdrivande och svåra att införa.

Det är bra att ni har med kravställning på lämplig säkerhet vid upphandlingar.

28. Tar ni fram förslag till PUB-avtal med instruktioner som en del av upphandlingsunderlaget i samband med upphandling av nya system som ni berörs av?

Ja

Kommentar:
Det är bra att ha förslag till personuppgiftsbiträdesavtal med instruktioner som en del av upphandlingsunderlaget för då vet leverantören vad det är som ni förväntar er. Om man inte har med förslag till PUB-avtal och instruktioner kan det lätt bli så att man hamnar i underläge gentemot leverantören och har svårt att med framgång hävda sina krav.

Det är bra att ni har med förslag till PUB-avtal med instruktioner som en del av upphandlingsunderlaget. Vi rekommenderar att ni fortsätter med denna rutin i samverkan med ert upphandlingsteam.

29. Har ni något mer ni vill tillägga?

30. Vad tycker du om enkäten?

Ett bra uppföljningsverktyg.

Sammanfattning

Ett dataskyddsombuds viktigaste uppgifter är att ge råd och stöd samt att ha en kontrollerande funktion så att dataskyddslagstiftningen efterlevs. Det operativa arbetet i den personuppgiftsansvariges förvaltning behöver utföras av personer som är anställda hos personuppgiftsansvarig.

Organisation och struktur för dataskyddsarbetet
Vid genomgång av era svar kan vi se att det finns en organisation med utsedda roller för nämnden dataskyddsarbete. Personerna får utbildning inom dataskyddsområdet. Detta är grundförutsättningar för att dataskyddsarbetet ska kunna fungera.

Det finns rutiner för att informera personuppgiftsansvarig myndighet om sitt ansvar.

Nämnden har beslutat om delegationsordning för dataskyddsfrågor. Det är inget krav enligt GDPR, men det finns fördelar med att göra det.

Dataskyddsförordningen och annan dataskyddslagstiftning gäller, men organisationen behöver bestämma hur det ska genomföras lokalt genom egna styrdokument. Ni har antagit en informationssäkerhetspolicy.

Kontaktuppgift till dataskyddsombud
Att utse dataskyddsombud och anmäla kontaktuppgifter till Integritetsskyddsmyndigheten (IMY) är en grundläggande åtgärd och detta är genomfört.

Registerförteckningar
Att ha kontroll över sina registerförteckningar är också grundläggande för dataskyddsarbetet och det är bra att ni har upprättade förteckningar, rutiner för arbetet och att personuppgiftsansvarig får regelbunden information om aktuella registerförteckningar.

Tredjelandsöverföring
Efter Schrems II-domen är det särskilt viktigt att ha kartlagt vilka tredjelandsöverföringar som ni har. Kartläggningen av era tredjelandsöverföringar är genomförd och det är en nödvändig förutsättning för att veta vilka ytterligare åtgärder som kan behöva göras.

Genomgången ni har gjort innebär också att ni har fastställt med vilket rättsligt stöd som ni gör tredjelandsöverföringen. Ni har också påbörjat arbetet med risk- och konsekvensbedömning med anledning av de tredjelandsöverföringar ni gör.

De registrerades rättigheter
Av era svar framgår att ni har rutiner för att hantera de registrerades rättigheter och ni informerar även om rättigheterna på ett bra sätt.

Personuppgiftsbiträden
Ert arbete med personuppgiftsbiträdesavtal (PUB-avtal) verkar fungera tillfredsställande och det är mycket bra att det finns biträdesavtal med instruktioner med nästan samtliga personuppgiftsbiträden och ni har även rutiner för arbetet.

Risk- och konsekvensbedömningar
Ni gör risk- och konsekvensbedömningar och har rutiner samt utsedda personer för detta arbete. Vi vill här påminna om att dataskyddsombudet ska rådfrågas i samband med risk- och konsekvensbedömningar. Det är bra att ni har utsedda personer som deltar i arbetet med risk- och konsekvensbedömningar.

Personuppgiftsincidenter
När det gäller hantering av personuppgiftsincidenter har ni rutiner för hantering av personuppgiftsincidenter och er personal informeras om rutinerna. Nämnden får regelbunden information om anmälda incidenter.

Informationssäkerhet
Vad gäller informationssäkerhetsarbetet så är det oklart om ni gör något arbete med informationssäkerhetsklassning, men ni har fastställda roller runt systemförvaltning.

Frågor om GDPR i samband med upphandling
När det gäller frågor om GDPR i samband med upphandling har ni en form av checklista för dataskyddsfrågor i samband med upphandling av nya system.

Det ställs krav på lämplig säkerhet vid upphandling av nya system som ni berörs av.

Ni tar fram förslag till PUB-avtal med instruktioner som en del av upphandlingsunderlaget i samband med upphandling av nya system som ni berörs av.

Sammanvägd bedömning

Vår bedömning är att det viktigaste som viadidaktnämnden i Katrineholms kommun behöver arbeta vidare med är:

1. Planera in regelbunden information om aktuella registerförteckningar med nämnden.

2. Vi rekommenderar att ni gör en risk- och konsekvensbedömning med anledning av de tredjelandsöverföringar som ni har. Utifrån denna bedömning tar ni fram en åtgärdsplan

3. Vi rekommenderar att ni påbörjar ett arbete med att informationssäkerhetsklassa er information.

Dataskyddsteamet

Therese Jigsved Dataskyddsombud/ Förbundsjurist	Anders Danielsson Informationssäkerhets- specialist	Ria Larsson Arkivarie	Hugo Persson Jurist, dataskydd och IT-rätt

Datum
2022-11-24

Vår beteckning
VIAN/2022:48 - 2.1.1 - Mötesplanering

Mottagare:

Vår handläggare
Emma Fälth

Handläggare telefon
0150-570 15

Handläggare e-post
emma.falth@katrineholm.se

Förlängt sammanträde för Viadidaktnämnden

Förvaltningens förslag till beslut

Viadidaktnämnden beslutar att förlänga sammanträdet den 14 februari 2023 så att sammanträdet börjar kl 09:00.

Sammanfattning av ärendet

Med anledning av ny mandatperiod finns behov av utbildningsinsatser och information om de olika verksamheterna inom Viadidakt för den nya Viadidaktnämnden. Men anledning av detta föreslås det första nämndsammanträdet, som är den 14 februari 2023, börja kl 09:00 istället för klocka 13:30.

Emma Fälth
Utredare

Beslutet skickas till:

Berörda

Akten

Datum
2022-11-24

Vår beteckning

Mottagare:

Vår handläggare
Emma Fälth

Handläggare telefon
0150-570 15

Handläggare e-post
emma.falth@katrineholm.se

Anmälan av delegationsbeslut

Förvaltningens förslag till beslut

Viadidaktnämnden lägger anmälan av delegationsbesluten till handlingarna.

Sammanfattning av ärendet

Redovisning av beslut fattade på Viadidaktnämndens vägnar under perioden

2022-09-17 – 2022-11-29 enligt nedan:

Kommunal vuxenutbildning

Ärendegrupp/Ärende	Antal
Mottagande och antagning av elever	
Beslut om att ta emot elev till utbildning på grundläggande nivå eller till särskild utbildning på grundläggande nivå, även från annan kommun	126
Beslut om mottagande och antagning av elev till utbildning på gymnasial nivå eller till särskild utbildning på gymnasial nivå, även från annan kommun	1412
Beslut om mottagande av elev till svenska för invandrare, även från annan kommun	272
Sökande till annan huvudman	
Yttrande till annan huvudman om den sökande uppfyller villkoren att delta i utbildning på grundläggande nivå eller särskild utbildning på grundläggande nivå, i de fall ansökan avser utbildning som anordnas av annan huvudman	0
Yttrande till annan huvudman om kommunen åtar sig att svara för kostnaderna för den sökandes utbildning, i de fall en ansökan avser utbildning på gymnasial nivå eller särskild utbildning på gymnasial nivå som anordnas av annan huvudman	21

Ärendegrupp/Ärende	Antal
Yttrande till annan huvudman om kommunen åtar sig att svara för kostnaderna för den sökandes utbildning, i de fall en ansökan avser svenska för invandrare som anordnas av annan huvudman	0
Förklara eleven behörig att delta i utbildning i folkhögskola som motsvarar kommunal vuxenutbildning i svenska för invandrare i samband med beslut om mottagande enligt SL 20 kap. 33 §	0
Beslut om ersättning till folkhögskola som tagit emot elev till utbildning i svenska för invandrare	0
Studiestartsstöd	
Beslut om sökande tillhör målgruppen för studiestartsstöd	3
Upphörande och återupptagande av studier	
Besluta om att utbildningen ska upphöra om elev saknar förutsättningar att tillgodogöra sig utbildningen eller annars inte gör tillfredsställande framsteg.	3
Beslut om att låta elev återuppta studier på grund av att särskilda skäl föreligger. Gäller de fall där beslut tidigare fattats att utbildningen ska upphöra för elev som saknar förutsättningar att tillgodogöra sig utbildningen eller annars inte gör tillfredsställande framsteg.	0
Undervisningens omfattning inom sfi	
Beslut om att sfi för en elev får omfatta mindre än 15 timmars undervisning i veckan, om eleven begär det och det är förenligt med utbildningens syfte.	0

Datum
2022-11-24

Vår beteckning

Mottagare:

Vår handläggare
Emma Fälth

Handläggare telefon
0150-570 15

Handläggare e-post
emma.falth@katrineholm.se

Meddelanden

Förvaltningens förslag till beslut

Viadidaktnämnden lägger anmälan av meddelanden till handlingarna.

Sammanfattning av ärendet

Utdrag ur Viadidaktnämndens diarium över handlingar för perioden

2022-09-17 – 2022-11-29 finns att tillgå på Viadidakt, Bievägen 1B, Katrineholm.