RAPPORT

Tillsyn av Barn och ungdomsnämnden och Gymnasie- och vuxenutbildningsnämnden Region Gotland Avseende personuppgiftsansvaret enligt den Europeiska Dataskyddsförordningen (GDPR) 2022

Fastställd av Barn och ungdomsnämnden och Gymnasie- och vuxenutbildningsnämnden
Framtagen av Regionens Dataskyddsombud
Datum 20230217
Gäller
Ärendenr RS 2023/359
Version 1

SLUTSATS

Barn och ungdomsnämnden och Gymnasie- och vuxenutbildningsnämnden uppfyller inte fullt ut kraven i den Europeiska dataskyddsförordningen (EU) 2016/679 (i fortsättningen benämnd GDPR). De brister som vi funnit består i bristande dokumentation, information och uppföljning. Det bedöms inte föreligga risk för att nämndens behandling av de registrerades personuppgifter äventyrar de registrerades personliga integritet.

För att förbättra regelefterlevnaden till GDPR bör informationen till de registrerade samt instruktionerna avseende samordnat personuppgiftsansvar och personuppgiftsbiträden ses över och utvecklas.

Innehåll

ADVOKATFIRMAN
SINGULARITY LAW AB

Fridhems Gränd 5, SE-184 91 ÅKERSBERGA, Sweden

BAKGRUND

I egenskap av Dataskyddsombud granskar vi hur de personuppgiftsansvariga nämnderna inom Region Gotland behandlar personuppgifter för att säkerställa att behandlingen följer gällande regler samt att de registrerades (medarbetarnas och medborgarnas) integritet skyddas.

Under 2022 har vi valt att granska följande områden

1 Uppföljning av PUB/samordnings-avtal när behandling av uppgifter sker av annan än den personuppgiftsansvarige

2 Information avseende personuppgiftsbehandling vid insamling av uppgifter

3 Inventering Kameraövervakning

4 Uppföljning av dokumentation över behandlingar

Regionstyrelsen har inkommit med svar på samtliga frågor.

Utöver ovanstående granskningsområden har vi även sett att det finns frågor kring ansvarsfördelningen mellan nämnderna som förtjänar uppmärksamhet.

Reglering av personuppgiftsansvaret inom regionen

Personuppgiftsansvariga är alltid genom ansvarsskyldigheten i GDPR's artikel 5 punkt 2 ansvariga för behandlingen av personuppgifter de är ansvariga för. Inom Region Gotland har respektive nämnd ansvar för sin behandling av personuppgifter, men det förekommer även behandlingar där mer än en nämnd behandlar uppgifter. I en del fall inom t.ex. IT-drift och centrala funktioner som HR och ekonomi uppstår något som liknar en biträdesrelation. Regionen och nämnderna behöver därför instruera egen personal och andra utförare som utför behandlingar så att de uppfyller samtliga krav på behandlingen och kan visa detta. En viktig del i att göra det är att kunna visa dokumentation på ansvarsfördelningen för behandlingar och att visa att den ansvarige genomfört lämplig verifikation av biträdet, underbiträden och behandlingarna.

I GDPR (artikel. 26) finns regler avseende de behandlingar som sker där ansvaret för behandlingarna är delat mellan två eller flera ansvariga. För att bedöma om det föreligger ett gemensamt ansvar är det frågan om vem som fastställer ändamål och medlen för behandlingen som behöver besvaras. Om två parter samarbetar och gemensamt genomför en behandling föreligger ett gemensamt personuppgiftsansvar. Ett sådant ansvar kan även föreligga om den ena parten fastställer ändamålet samtidigt som den andra parten fastställer medlen för behandlingen, ett fall som kan uppstå vid t.ex. outsourcing. Parterna är skyldiga att reglera arrangemanget och göra det tillgängligt för de registrerade, vilket i praktiken förutsätter någon form av dokumentation som liknar ett avtal, i GDPR benämns detta dock endast som "instrument".

I GDPR (artikel. 28) finns reglerna som föreskriver att den personuppgiftsansvarige ska upprätta avtal eller annan rättsakt enligt unionsrätten eller nationell lagstiftning om en annan part ska genomföra behandlingen av personuppgifter för den personuppgiftsansvariges räkning.

För regionen kan det förhållandet som åsyftas i art. 28 3:e stycket vara aktuellt i och med att personuppgiftsansvaret är delegerat till nämnderna från regionstyrelsen, samtidigt som regionstyrelsen utför personuppgiftsbehandlingen i egenskap av central IT-organisation. Då förvaltningarna i sig inte är civilrättsliga subjekt i förhållande till varandra är det inte lämpligt med avtalsreglering. För att reglera personuppgiftsansvaret utan att behöva upprätta detaljerade instruktioner för varje behandling kan regionen i ett reglemente ange vilka nämnder som ska vara personuppgiftsansvariga för olika behandlingar i kommunens system[1] samt ange principer för ansvarsfördelningen om en annan nämnd än den personuppgiftsansvariga utför behandlingar.

För att tydliggöra ansvaret mot de registrerade kan det annars finnas anledning att reglera ansvarsfördelningen i delegationsordningen eller genom ett beslut i regionstyrelsen. Vi har vid tillsynen inte funnit ett sådant i nuvarande delegationsordning, men med beaktande av att det är regionstyrelsen som i slutänden har ansvaret för behandlingarna får det en styrande effekt för eventuellt

[1] Behövs biträdesavtal internt inom den kommunala förvaltningen? Sveriges Kommuner och Regioner 20180821

ansvarsutkrävande.

I ett stort antal fall är det dock externa utförare som utför behandlingarna för de personuppgiftsansvariga. Hur det ska göras har regionen styrt genom riktlinjen *EU:s dataskyddsförordning - Roller och ansvar RS 2018/1333* och en instruktion på intranätet https://intra.gotland.se/sidor/stod-och-interna-tjanster/informations--och-arendehanteringsstod/gdpr-region-gotland/pub-avtal.html?query=delegationsordning.

Därutöver behöver reglerna i artiklarna 79 (effektiva rättsmedel mot personuppgiftsansvariga och biträden), 82 (ansvar och rätt till ersättning), 83 (allmänna villkor för påförande av sanktionsavgifter) beaktas vid regleringen av ansvar och vidtagande av åtgärder för att lindra skador.

Frågeställning 1 Uppföljning av PUB/samordnings-avtal när behandling av uppgifter sker av annan än den personuppgiftsansvarige

Regionen har fattat beslut om hur personuppgiftsansvariga ska hantera frågor om ansvar för behandlingar och personuppgiftsavtal vilket det informeras om på intranätet under ”GDPR information”, vilket i sin tur är baserat på en riktlinje och en delegationsordning (RS 2022/327) som reglerar det övergripande ansvaret för GDPR men inte specifikt hur och när förvaltningarna ska ingå personuppgiftsavtal, där det hänvisas till respektive nämnds delegationsordning för information om vem som har rätt att teckna PUB-avtal.

Det finns en risk att biträden med tiden tappar respekten för avtal och regelverk om de inte följs upp och kontrolleras eftersom de är medvetna om det betydande arbete som avhåller en beställare från ett leverantörsbyte. I en del fall kan såväl tekniska lösningar som administrativa rutiner ha ändrats vilket gör att det inte längre är tydligt att de ger lämplig säkerhet, t.ex. genom byte av underbiträden. För att undvika att leverantörer bedriver sin verksamhet så att den ger problem för beställaren är det angeläget att kunna visa att det finns en vilja och förmåga att genomföra revisioner och agera vid överträdelser av avtalen, vilket kan vara svårt om det inte finns förberedda rutiner.

Syftet med tillsynsfrågan är att synliggöra vikten av dokumenterad reglering av ansvar som överensstämmer med hur personuppgiftsansvarig vill bedriva behandlingen av personuppgifter. Avsikten är även att personuppgiftsansvariga ska kontrollera att utförare lever upp till sina åtaganden, i syfte att förbättra regelefterlevnaden och bidra till att uppgifterna om behandlingen är korrekta och att regionens hantering av personuppgifter är trovärdig.

Bifogat finns en lista över de PUB-avtal som finns dokumenterade i LiSA. I flera fall är det sannolikt så att avsaknaden av PUB- eller samordningsavtal beror på att behandlingen sker internt, men med den fördelning av personuppgiftsansvar som regionen valt.

Det kan dock finnas anledning att överväga en avtalsreglering även i de fallen, i alla fall då den personuppgiftsansvarige inte själv bestämmer medlen för behandlingen (teknisk lösning). I de fall behandling utförs av en extern leverantör och det inte finns notering om avtal där, behöver det kontrolleras om det finns ett sådant och i sådana fall dokumenteras i LiSA.

Personuppgiftsansvarig uppmanas att genomföra ett stickprov för att följa upp att avtalet återspeglar hur behandlingen av uppgifter hos biträdet faktiskt sker, samt om det skett förändringar avseende underbiträden. Den här punkten kommer sannolikt att bli allt viktigare ju mer vikt som läggs vid privacy by design (PBD) i artikel 25 (skäl 78) där genomförande av uppföljning och dokumentation av detta är krav. Avsikten med att ta upp frågan nu är att förbereda och börja etablera rutiner för hur detta ska kunna genomföras utan att bli allt för betungande för verksamheten, särskilt med beaktande att villkor om detta bör tas in redan vid upphandlingen av externa leverantörer.

Förvaltningens egen bedömning

Förvaltningen har identifierat 7 system som saknar PUB-avtal, varav ett är avvecklat, ett avtal ligger på regionstyrelsen, ett inte är ett system och ett lagras på en server som förvaltningen själv kontrollerar, för 3 av systemen behöver utredas vidare.

Dataskyddsombudets bedömning

Situationen för de system där det är oklart huruvida det behövs PUB-avtal eller inte behöver klaras ut. Det bör även genomföras stickprov för att kontrollera de PUB-avtal som finns, framförallt avseende om instruktionerna beskriver den faktiska behandlingen och efterföljs av leverantören. Då det kan förekomma särskilt skyddsvärda uppgifter är det viktigt att säkerställa att behandlingarna uppfyller de legala kraven och har en lämplig teknisk och administrativ säkerhet. Förvaltningen bör genomföra stickprov för att kunna utvärdera biträdenas avtalsefterlevnad.

Frågeställning 2 Information avseende personuppgiftsbehandling

För personuppgiftsansvariga som likt Region Gotland behandlar uppgifter som är nödvändigt för ett allmänt intresse eller som ett led i myndighetsutövning med uttryckligt lagstöd (art. 6.1 e) GDPR) är transparens och information avseende behandlingar en förutsättning för att det ska finnas en acceptans från de registrerade.

Det är inte ovanligt att registrerade ifrågasätter varför deras personuppgifter publiceras eller lämnas ut med hänvisning till offentlighetsprincipen, vilket förvisso kan anses en självklarhet då offentlighetsprincipen är grundlagsfäst och väl etablerat. Det är dock ett exempel på information som bör lämnas till de registrerade i samband med att information samlas in.

Genom att se över informationen som lämnas om behandlingarna och vid behov genomföra förändringar förbättras regelefterlevnaden och de registrerades insyn i behandlingen vilket bidrar till att uppgifterna är korrekta och att regionens hantering av personuppgifter i egenskap av personuppgiftsansvarig är trovärdig.

Reglernas omfattning

I GDPR (artikel. 5.1) finns den grundläggande principen om att den personuppgiftsansvarige ska vara transparent avseende behandlingen av personuppgifter.
Reglerna om de registrerades rättigheter finns i kapitel 3 till GDPR där reglerna om information till de registrerade finns i artiklarna 12 till 15. En förutsättning för att de registrerade ska kunna utöva sina rättigheter är att personuppgiftsansvariga vidtar lämpliga åtgärder för att underlätta de registrerades tillgång till korrekt och rättvisande information om behandlingen. Kraven på information till de registrerade har skärpts jämfört med PUL bl.a. med följd att det nu krävs explicit lagstöd för att kunna åberopa undantag från informationsplikten vid erhållande eller utlämnande av uppgifter. De gällande reglerna för information till de registrerade är som huvudregel att information ska lämnas när informationen samlas in, behandlingen startar t.ex. genom ett utlämnande. Med startar anses även förändringar som sker av behandlingen, t.ex. om uppgifterna tas in från eller lämnas till ny tredje part, eller i förändringar av den information som behandlas.

Frågan

Information avseende personuppgiftsbehandling

Granskning av den information om behandling av personuppgifter som lämnas till registrerade och allmänheten. Det är alltså inte information som lämnas ut med stöd av offentlighetsprincipen eller artikel 15 som efterfrågas utan den information som avses i artiklarna 12-14. Aktiviteten genomförs genom genomgång av texter på web och i dokument som distribueras till allmänheten avseende personuppgiftsbehandling. Den hjälp jag önskar från personuppgiftsansvariga och dataskyddsnätverket är:

1 Att ni översiktligt undersöker hur informationsgivningen sker

A) När en behandling inleds

B) När uppgifter hämtas in från den registrerade själv

C) När uppgifter hämtas in från annan än den registrerade själv

2 Att ni lämnar in representativa exempel på den information som ges till de registrerade enligt ovan.

Förvaltningens egen bedömning

Utbildnings- och arbetslivsförvaltningen (UAF) (i egenskap av svarande)

Inom båda BUN och GVN har vi information om GDPR på alla blanketter och E-tjänster. Det som vi inte informerar är att vi samlar information i våra system såsom t ex Edlevo, SchoolSoft, (förskolan, grundskolan), lt´s learning (gymnasiet, vuxenutbildningen) Office 365. Dessa system får information från kir.
Sen har vi även PMO (elevhälsan) där alla elever finns mer eller mindre. De läggs in där för att skolsköterskan ska kunna göra uppföljning från BVC och sen lägger specialpedagoger och rektorer in särskilda elevers information. (annan teckentyp och storlek, du bör ha samma)

Ingen av ovanstående fall informeras den registrerade om att detta göras såvida de inte begär ut ett registerutdrag.

Dataskyddsombudets bedömning

Förvaltningen (i egenskap av personuppgiftsansvarig) bör i framtida utskick till de registrerade informera om de behandlingar som sker med information som samlas in från annan än de registrerade. Förvaltningen bör även se över om den information som lämnas i blanketter och e-tjänster på ett korrekt sätt återspeglar de behandlingar som görs. Se över och informera om uppgifterna överförs till tredje part.

Frågeställning 3 Inventering Kameraövervakning

Kameraövervakning förekommer i flera av de tillsynsärenden som IMY granskat och har varit föremål för sanktionsavgifter. Genom teknikutveckling har kameratekniken blivit billigare, lättare att använda och ger mer avancerade analysmöjligheter än tidigare, vilket gör att den på samma sätt som molntjänster lätt kan börja användas utan att det skett en djupare analys av konsekvenserna för t.ex. personlig integritet.

Kameraövervakning innebär en behandling av personuppgifter om den sker så att det är möjligt att identifiera de som registreras, framförallt när inspelning sker.

Kameraövervakning anses vara generellt integritetskänslig oavsett om den sker på allmän plats eller på privat område. Det är dock endast på allmän plats som tillstånd måste sökas när kameraanvändningen innebär varaktig eller regelbundet upprepad personbevakning.
I samtliga fall och även i miljöer där inte allmänheten har tillträde är det viktigt att GDPR's regler för personuppgiftsbehandling följs. Av artikel 5.1 a följer att all personuppgiftsbehandling måste vara laglig, korrekt och präglas av öppenhet. Att behandlingen ska vara korrekt innebär att den ska vara rättvis, skälig, rimlig och proportionerlig i förhållande till de registrerades rätt till skydd för sin integritet.

I och med att den tidigare Kameraövervakningslag (2013:460) ersattes med GDPR och i vissa fall Kamerabevakningslag (2018:1200) har regleringen avseende användning av kameror för personbevakning förändrats på så sätt att tillstånd behöver sökas för verksamheter som är myndigheter eller förlitar sig på berättigat ändamål som grund för personuppgiftsbehandling/kamerabevakning. En stor del av offentlig verksamhet behöver därför fortsatt tillstånd.

Enligt beslut från Regionfullmäktige 2020-09-28 har det samlade ansvaret för verksamheten inom regionstyrelsens avdelning försörjning flyttat till tekniska nämnden. Inom avdelning försörjnings ansvarsområde nämns *Hjälpmedelsförsörjning med inköp, förrådshållning, distribution, teknik och service av hjälpmedel (t ex nyckelgömmor och kameraövervakning i hemmen) samt hjälpmedelspolicyn.* Om avsikten är att även ansvaret för kamerabevakning i övrigt ska hanteras av tekniska nämnden bör det klargöras, för att undvika situationer där det är oklart vem som ansvarar för personuppgiftsbehandling av uppgifter från kamerorna.

Barn och ungdomsnämnden bedriver ingen kamerabevakning

Gymnasie- och vuxenutbildningsnämnden bedriver verksamhet i Wisbygymnasiet, där Teknikförvaltningen har tillståndet och ansvaret för behandlingen. Men är därför inte ansvarig för den uppgiftsbehandlingen.

Dataskyddsombudets bedömning

Som i princip alla frågor som rör informationssäkerhet och GDPR är utbildning av medarbetarna den mest effektiva åtgärden för att höja säkerheten och minska risken för regelöverträdelser. Överväg att tydliggöra ansvaret för kameraanvändning och införa en övergripande policy för regionens kameraövervakning avseende hantering av personuppgifter. All användning av fast monterade kameror som direkt eller indirekt kan samla in uppgifter om identifierbara personer (t.ex. registreringsskyltar på fordon) ska föregås av ett beslut av ansvarig chef.

I de fall där det är tydligt att det inte kommer att samlas in personuppgifter kommer det inte att vara ett problem, men i praktiken kommer troligen i många fall personuppgifter att samlas in även om det inte varit den direkta avsikten. Om det finns anledning att anta att personuppgifter behandlas aktualiseras GDPR vilket ställer krav på rättslig grund för behandlingen, och upplysning om att behandlingen sker. Med

beaktande av rättsutveckling kan det finnas anledning att vara noga med hur de insamlade uppgifterna används och hur sådan användning motiveras.

Kameraanvändning kommer därför att kräva ställningstaganden när det gäller personuppgifter. Det är därför viktigt att medarbetarna får tydlig information om hur användning av monterade kameror får ske samt vilka villkor som måste uppfyllas.

Frågor kring information, förvaring, åtkomst, utlämnande, gallring och övriga rättigheter för registrerade avseende inspelat material kan med fördel ges en central ledning. Om det finns en central vägledning underlättas hanteringen av att det finns övergripande ställningstaganden kring hur ett sådant utlämnande eller andra åtgärder kan ske. På samma sätt underlättas de ansvarigas hantering om de har en policy att förhålla sig till, och vid behov motivera avsteg ifrån.
I och med att inspelat material med personuppgifter både faller under GDPR och offentlighetsprincipen kan en begäran om utlämnande som allmän handling kräva en granskning.

Inför ett krav på att all kameranvändning ska registreras i LiSA. IT har tagit fram en kompletterande möjlighet i LiSA för att ange att information lagras i ett kameraövervakningssystem. Det bör dock av uppföljningsskäl övervägas om även övriga kamerasystem ska registreras.

Frågeställning 4 Uppföljning av dokumentation över behandlingar

Bakgrund

Regionen har fattat beslut om hur personuppgiftsansvariga ska hantera frågor om ansvar för behandlingar vilket bl.a. innefattar dokumentation och skyldigheter mot de registrerade. I och med att de registrerade inte kan förväntas veta vilken nämnd som är ansvarig finns ett stort värde i att de personuppgiftsansvariga agerar på ett samordnat och likartat sätt för att underlätta för de registrerade att utöva sina rättigheter.

Vid dataskyddsombudets tillsyn 2020 kunde det konstateras att dokumentationen av behandlingarna inte uppfyllde kraven i GDPR Artikel 30, då redovisningen som finns i stödsystemet LiSA utgick från informationsmängder/system. Sedan dess har förvaltningarna arbetat med att försöka åtgärda avvikelsen dels genom att kartlägga sina processer där behandlingar av personuppgifter sker, dels genom att undersöka alternativa sätt att dokumentera behandlingen än i LiSA. Syftet med granskningen är att följa upp vilka åtgärder som vidtagits sedan 2020 samt granska om det med nuvarande dokumentation föreligger risker för de registrerades personliga integritet. I och med att tillsynen identifierat bristen behöver den följas upp till dess den kan konstateras vara åtgärdad.

Dokumentationen ska utgå från de registrerades perspektiv d.v.s. följa den process t.ex. en ansökan om en förmån där personuppgifterna behandlas. Regionen har beslutat om **Klassificeringsstruktur Region Gotland (STY-15127)** som innehåller definition av verksamheternas processer som utgör en bra grund för presentation av de behandlingar av personuppgifter som förekommer inom regionen. Av det följer att behandlingar som inte innefattar personuppgifter inte behöver dokumenteras.

I LiSA finns i princip all den dokumentation om behandlingarna som behövs för att leva upp till regleringen, med undantag av information om uppgifter överförs till tredje part. Informationen är dock knuten till informationsmängden som finns i ett system och inte behandlingen från början till slut. Det finns i dagsläget ingen möjlighet att se om behandlingen börjar eller fortsätter i ett annat system eller på ett enkelt sätt se om det finns andra beroenden till andra system.

Frågeställning

> **Uppföljning av dokumentation över behandlingar**
>
> Granskningsrapporterna från 2020 påtalade att det fanns brister i hur regionens behandling av personuppgiftsbehandling dokumenterades. En då genomgående invändning var att det inte gick att följa i vilka system behandlades utifrån de registrerades perspektiv. Det fick till följd att det inte gick att utifrån de registrerades perspektiv följa hur och i vilka system uppgifterna behandlades vid när ett ärende hanterades. I många fall är det bara ett, två system eller tre system (där det ena är diariet, det andra är arkivet) som används för handläggning vilket gör det till en ren förklaringsfråga, men det förekommer även ärenden som behandlas i flera verksamhetssystem och då skulle behöva redovisas utifrån syfte och skäl för behandlingen.

En del av inventeringsrapporten är ”Uppföljning av dokumentation över behandlingar” för regionen att besvara. Svaret är ett gemenast svar från Region Gotlands samtliga nämnder. Då det administrativa systemet LISa är gemensam bas för alla nämnder gällande informationsklassningar. Övriga eventuella svar inkommer från respektive objektägare.

Historik och sammanhang

Region Gotland genomförde ett projekt mellan 2014 och 2017 för att införa ett ledningssystem för informationssäkerhet (LIS) med syfte att på ett strukturerat sätt skydda regionens verksamhetsinformation. LIS administreras i verktyget LISa sedan årsskiftet 2017/2018. Det pågår löpande ett arbete att få området dataskydd till att bli en integrerad del av informationssäkerhetsarbetet utifrån regionens LIS.
Sedan dataskyddsförordningen (GDPR) infördes i maj 2018 har delar av arbetet med att skydda personuppgifter införts i LIS. Detta sker bland annat att verksamheter som klassar sin information uppger huruvida personuppgifter är en del av

informationsmängderna, vilket i sin tur påverkar vilket skydd som informationen bör ha och på vilket sätt som den ska och får hanteras. Verktyget LISa genererar också det registerförteckning. Den registerförteckning som genereras stämmer dock inte överens med GDPR eftersom förteckning sorter i första hand efter system och inleder inte företeckning med behandling.
I mars 2019 fattade regionfullmäktige ett beslut om att införa en processorienterad struktur för förvaltningen av regionens information utifrån ett arkivperspektiv För att åskådliggöra processerna har en klassificeringsstruktur skapats och som beskriver samtliga verksamhetsområden, huvudprocesser och processer inom Region Gotland.

Nämnden har inte inkommit med något eget svar utöver det ovan angivna.

Dataskyddsombudets bedömning

Förvaltningen bör göra en genomgång av verksamhetens processer och utifrån den undersöka vilka system som används och vilken information som behandlas. Miljön förefaller komplex vilket riskerar medföra att de registrerade inte får rättvisande information om behandlingarna. I flera fall är det sannolikt att mer än ett system används i verksamhetsprocesser, vilket gör att de registrerade inte får en helt korrekt bild av behandlingen med nuvarande dokumentation.
Det förefaller vara relativt stora mängder personuppgifter (personnummer) vilket ställer krav på säkerhet i behandlingen, vilket förutsätter att dokumentationen är korrekt och att systemlösningarna är lämpliga. Det ser även ut att förekomma behandling av särskilt skyddsvärda uppgifter vilket ställer än högra krav på att behandlingarna och överföringar av information redovisas korrekt.

Rekommendationer

Rekommendationen ersätter inte skyldigheten att leva upp till lagstiftningens krav utan är utformad för att förbättra regelefterlevnaden genom att hitta en rimlig balans mellan arbetsinsats och de formella krav som finns på behandlingen utifrån de risker för de registrerade integritet som föreligger.

I och med att nämndens verksamhet i bedriver myndighetsutövning och behandlar stora mängder särskilt skyddsvärda personuppgifter ställs mycket höga krav administrativ och teknisk säkerhet vilket innefattar att kunna visa upp fullständig dokumentation och information till de registrerade. Det är av stor vikt att underlätta för de registrerade att utöva sina rättigheter utan att röja uppgifter med sekretess eller som rör någon annan än de registrerade.

Då möjligen en del uppgifter som behandlas faller under sekretess med omvänt

skaderekvisit enligt OSL 26 kap 1§ kan det i vissa fall ställas högre krav på säkerhet än i GDPR. Det gäller t.ex. vid utkontraktering av behandlingar där det inte med säkerhet går att avgöra om leverantörer kan leva upp till lämplig administrativ och teknisk säkerhet (t.ex. där behandling sker utanför Sverige). I sådana fall kan den enda verksamma åtgärden vara att återta tjänsteleveransen i egen regi eller att aktivt följa upp leveransen. De högre kraven på nämndens verksamhet tillsammans med Hälso- och sjukvården skiljer sig därför från regionens övriga verksamheter. Det gör att det finns ett särskilt värde i att kartlägga och dokumentera behandlingarna samt utbyta erfarenheter.

Ett område som bör adresseras är ansvarsfördelningen mellan de olika personuppgiftsansvariga förvaltningarna och den centrala förvaltningen. I och med att personuppgiftsansvaret är fördelat på nämnderna behöver det vara tydligt vem som ansvarar för behandlingar och information när mer än en nämnd berörs, på samma sätt behöver det informeras om insamlad information lämnas vidare till eller hämtas in från en annan förvaltning.

Rekommendationerna ska därför ser som en hjälp att komma igång med arbetet, men det är självklart inget som hindrar att ambitionsnivån sätts högre eller fokuserar mer på områden där konkreta problem uppstår.

Lämpliga åtgärder kan vara följande:

Gemensamt med övriga nämnder och förvaltningar

1. Genomför en inventering av behandlingar där det förekommer ett gemensamt personuppgiftsansvar för förvaltningarna
2. Se över och inför en reglering av ansvar och villkor för behandlingar som sker mellan olika förvaltningar, detta kan behövas både då en förvaltning agerar som biträde för en annan förvaltning och då mer än en förvaltning är ansvarig för behandlingen antingen i en process eller ett system.
3. Ta fram riktlinje/checklista för hur behandlingsinstruktioner ska vara utformade (enligt uppgift förekommer ett arbete kring detta inom GDPR-nätverket)
4. Ta fram checklista för upphandlingskrav som kompletterar befintliga instruktioner och PUB-avtal avseende förmågan att kravställa och följa upp lämplig administrativ och teknisk säkerhet för behandlingarna.
5. Ta fram riktlinje för när och hur stickprover/verifiering och revision av personuppgiftsbiträden och underbiträden ska göras
6. Ta fram instruktion för hur ett biträdes brott mot eller bristande uppfyllelse av avtal ska hanteras
7. Inför i riktlinje att personuppgiftsansvariga ska införa dokumentation om det inte redan finns av PUB-avtal i LiSA eller annat sammanhållande register
    a. samt ange orsaken till att det inte finns, t.ex. att behandlingen inte rör personuppgifter
    b. Länk till kameraövervakningstillstånd
    c. Information om personuppgifter överförs till 3e part samt metod för överföring

   d. Historik över förändringar/revisionshistoria för informationen t.ex. genom länk till W3D3
8. Ta i samverkan med övriga nämnder fram en rapportstruktur som gör att det går att redovisa behandlingarna utifrån verksamhetsprocesserna.

Utbildnings- och arbetslivsnämnden

9. Undersöka och identifiera behandlingar av särskilt skyddsvärda personuppgifter.
10. Gå igenom den information om behandlingarna som lämnas till de registrerade för att säkerställa att det sker vid inhämtande eller behandling såvida det inte finns uttryckligt lagstöd för behandlingen