Stockholms stad

GDPR Årsrapport

2024

Utbildningsnämnden

GDPR årsrapport
December 2024

Dnr:
Utgivningsdatum:
Kontaktperson: Hanna Virtanen

1 Bakgrund

Dataskyddsförordningen (GDPR) reglerar hur myndigheter, bolag och andra organisationer får hantera personuppgifter. Syftet är att skydda enskildas fri- och rättigheter, främst rätten till privatliv och skyddet för enskildas personuppgifter, men även övriga rättigheter fastställda i EU:s rättighetsstadga.

Som personuppgift räknas all typ av information som kan kopplas till en fysisk person, vilket betyder att personuppgiftsbegreppet är brett. Utbildningsnämnden behandlar personuppgifter i stor omfattning, av känslig karaktär och om personer i beroendeställning (elever och anställda), vilket betyder att kraven på nämndens personuppgiftshantering är höga.

Enligt dataskyddsförordningen är varje nämnd och bolagsstyrelse ansvarig för att verksamheten följer dataskyddslagstiftningen vid hantering av personuppgifter. Det innebär att utbildningsnämnden behöver informera sig, styra och följa upp sin verksamhet avseende behandlingen av personuppgifter.

Varje nämnd och bolagsstyrelse i Stockholms stad har i enlighet med dataskyddsförordningen utnämnt ett Dataskyddsombud (DSO). DSO:n har till uppgift att övervaka verksamhetens dataskyddsregelefterlevnad samt att ge råd och rapportera direkt till högsta förvaltningsnivå.

Denna årsrapport är således ett medel för nämnden att ta emot de råd och rekommendationer som DSO:n är skyldig att ge till ansvarig enligt dataskyddsförordningen samt för att få insyn i vad DSO:ns granskande arbete av verksamhetens status avseende integritet och dataskydd visar. Årsrapporten syftar till att nämnden ska kunna fatta beslut om prioriteringar, resurser och initiativ framåt. Detta samspel resulterar i att det blir enklare för ansvarig nämnd att visa hur de som personuppgiftsansvarig efterlever dataskyddslagstiftningen.

Innehåll

2 Sammanfattning

Inom ramen för Dataskyddsombudets uppdrag lämnas följande årsrapport till utbildningsnämnden. Årsrapporten består av en rapportering av tio olika områden där nämndens efterlevnad enligt vissa kontrollpunkter redovisas.

Inom utbildningsnämnden finns en god medvetenhet kring vikten av att skydda de personuppgifter som nämnden har blivit anförtrodd att hantera. I förra årets rapport hade nämndens efterlevnad förbättrats inom flera områden i jämförelse med året innan. Denna årsrapport innehåller fler rapporteringsområden i jämförelse med 2023 och är därmed inte direkt jämförbar med tidigare år. Vid jämförelse inom de områden som är samma från föregående år (exempelvis personuppgiftsincidenter och delvis konsekvensbedömningar) har en viss förbättring skett. Dock krävs åtgärder för att komma till en hög mognadsnivå i dataskyddsarbetet och i ett läge där kraven i dataskyddsförordningen efterlevs i stort.

Områden som i dagsläget bedöms kräva omgående åtgärder är de *grundläggande principerna, konsekvensbedömningar och registrerades rättigheter*. De *grundläggande principerna* är kärnan i dataskyddet och det är därför viktigt att kunna tillämpa dem när personuppgifter behandlas. I dagsläget finns inte tillräcklig kunskap om principerna och de är inte integrerade i de processer där personuppgifter behandlas.

Konsekvensbedömningar är ett obligatoriskt moment om en personuppgiftsbehandling anses leda till hög risk för enskildas fri- och rättigheter, exempelvis när sårbara personer som barn eller anställda berörs, om personuppgifter behandlas i stor omfattning, vid övervakning och profilering. Då utbildningsnämnden behandlar uppgifter om barn i stor omfattning och även känsliga personuppgifter krävs konsekvensbedömningar i flera fall av nämndens personuppgiftsbehandlingar. Därför är det viktigt att dels ha gjort konsekvensbedömningar för personuppgiftsbehandlingar som redan pågår, dels säkerställa att konsekvensbedömningar görs i framtiden, där så krävs.

Enskilda personer vars personuppgifter nämnden hanterar, registrerade, har ett antal rättigheter (*registrerades rättigheter*). I dagsläget hanterar inte nämnden begäran från registrerade i tid och informationsplikten gentemot den registrerade uppfylls inte i tillräcklig grad. Förutom att rättigheterna är lagstadgade bidrar en

effektiv hantering till att öka förtroende och främja transparensen då den registrerade ges möjlighet till insyn och kontroll av sina personuppgifter.

3 Rapporteringsområden

Denna årsrapport spänner över tio rapporteringsområden, fler än föregående årsrapporter, med ett antal krav inom respektive område som den personuppgiftsansvarige (”PUA”), i detta fall utbildningsnämnden, är skyldig att uppfylla enligt dataskyddsförordningen. Rapporteringsområdena och kraven speglar samtliga krav i förordningen och en organisation som uppfyller dessa efterlever dataskyddsförordningen i stort.

Rapporteringsområdena, och kraven kopplade till dessa, beskrivs nedan. Därefter redogörs för hur kraven har följts upp under granskningen 2024, resultatet av granskningen enligt en färgkod (se tabellen nedan), jämförelse med granskningen 2023 tillsammans med en uppföljning av dataskyddsombudet rekommendationer från föregående år och en sammanfattning av nämndens efterlevnad inom området per december 2024. Sist anges dataskyddsombudets rekommendationer för nämndens framtida dataskyddsarbete inom området.

Nedanstående färger och skala används för att bedöma efterlevnaden av respektive kontrollpunkt/krav:

	Allvarliga brister identifierade som omgående kräver insatser av ledning och/eller övriga verksamheten
	Brister identifierade som bedöms vara omfattande och/eller kräva omgående åtgärder
	Brister identifierade som bör åtgärdas men ej bedöms vara brådskande, omfattande eller allvarliga
	Inga brister av nämnvärd betydelse identifierade

3.1 Registerförteckning

Varje personuppgiftsansvarig ska enligt artikel 30 i GDPR ha en förteckning över sina personuppgiftsbehandlingar (en registerförteckning) där bland annat syfte, typer av personuppgifter och lagringstid framgår. Registerförteckningen är en förutsättning för att överhuvudtaget kunna efterleva dataskyddsförordningens krav då flera övriga krav förutsätter att den personuppgiftsansvariga dokumenterat vilka personuppgifter som behandlas, hur och varför. Registerförteckningen är också ett sätt att uppfylla principen om ansvarsskyldighet (artikel 5.2) som anger att den personuppgiftsansvarige ska kunna visa att de grundläggande principerna för behandling av personuppgifter efterlevs (se även nästa område).

3.1.1 Krav och uppföljning under granskning 2024

Kontrollpunkt/krav	Metod för uppföljning	Resultat 2024	Resultat 2023
Nämndens registerförteckning är komplett	Granskning av informations-klassningsprotokoll och underlag från konsekvensbedömningar.		
Informationen i registerförteckningen är aktuell	Granskning av förvaltningens rutiner för uppdatering av registerförteckningen.		

3.1.2 Uppföljning av föregående års rekommendationer

I 2023 års rapport rekommenderade dataskyddsombudet att förvaltningen kompletterar registerförteckningen med de personuppgiftsbehandlingar som rör nämnden som personuppgiftsbiträde. Denna rekommendation är just nu inte relevant eftersom det pågår ett arbete på förvaltningen med att kartlägga och fastställa utbildningsnämndens roll i personuppgiftsbehandlingar där nämnden är involverad. Utbildningsnämndens roll behöver vara fastställd innan registerförteckningen kan kompletteras.

3.1.3 Nämndens efterlevnad av kraven

Utbildningsförvaltningen hade under 2023 och delar av 2024 ett projekt vars syfte var att skapa en komplett registerförteckning för utbildningsnämnden i enlighet med kraven i artikel 30 i GDPR. Förvaltningen har idag en roll kallad ”registeransvarig” vars

uppdrag är att ha översikt att samtliga personuppgiftsbehandlingar dokumenteras i registerförteckningen och att, tillsammans med andra funktioner, säkerställa att det finns rutiner för upprättande och hanteringen av registerförteckningen. Nämnden har därmed rutiner som säkerställer att förteckningen hålls uppdaterad. Registerförteckningen har setts över under hösten 2024 och ska genomgå en översyn två gånger per år enligt förvaltningens nuvarande rutiner.

Registerförteckningen bedöms även vara komplett i stora delar då framtagandet av registerförteckningen utgått för förvaltningens hanteringsanvisningar. Dock har det under informationsklassningar och konsekvensbedömningar framkommit att registerförteckningen inte innehåller alla förvaltningars personuppgiftsbehandlingar.

Även om hanteringsanvisningarna är en bra utgångspunkt vid upprättande av en registerförteckning är perspektivet ett annat vilket kan leda till att alla personuppgiftsbehandlingar inte framgår av registerförteckningen om den enbart strikt utgår från befintlig information i hanteringsanvisningarna. Förvaltningen bör därmed i sina rutiner säkerställa att registerförteckningen speglar förvaltningens samtliga personuppgiftsbehandlingar. Detta kan exempelvis ske genom att registeransvarig samarbetar med funktioner som är ansvariga med informationsklassningar och konsekvensbedömningar (där en del är att systematiskt beskriva de personuppgiftsbehandlingar som sker).

3.1.4 Råd och rekommendationer till PUA

Utbildningsnämnden har en, i stort, komplett registerförteckning och rutiner för att säkerställa att den hålls uppdaterad övertid. Under informationsklassningar och konsekvensbedömningar har det dock framkommit att registerförteckningen inte innehåller alla förvaltningens personuppgiftsbehandlingar. För att förvaltningen ska kunna dra nytta av registerförteckningen i sitt övriga arbete rekommenderas:

- Ta fram rutiner/arbetssätt som säkerställer att registerförteckningen speglar förvaltningens samtliga personuppgiftsbehandlingar. Rutinen/arbetssättet bör samordnas med informationsklassningsprocessen.

3.2 Grundläggande principer

Dataskyddsförordningen innehåller ett antal principer som styr hur personuppgifter får hanteras. Principerna är kärnan i dataskyddet och för att en personuppgiftsbehandling ska vara tillåten, ska de grundläggande principerna följas. Därför är det viktigt att en organisation förstår principerna och kan tillämpa dem. De grundläggande principerna handlar sammanfattningsvis om att, vid varje personuppgiftsbehandling:

- Ha ett tydligt syfte med att behandla personuppgifter och inte behandla personuppgifterna senare för andra oförenliga syften (*principen om ändamålsbegränsning*)
- Enbart behandla personuppgifter i den omfattning som behövs utifrån syftet och inte längre än nödvändigt för syftet (*principen om uppgiftsminimering* och *principen om lagringsminimering*)
- Ha ett lagligt stöd för sin personuppgiftsbehandling (en rättslig grund) samt behandla personuppgifter på ett öppet sätt gentemot den enskilde och inte på ett sätt den enskilde inte kan förvänta sig (*principen om laglighet, korrekthet och öppenhet*)
- Säkerställa att personuppgifter är riktiga och om nödvändigt uppdaterade (*principen om riktighet*)
- Skydda känsliga och integritetskänsliga uppgifter från att spridas till obehöriga och i övrigt för att minska risken för oönskade händelser som kan leda till negativa konsekvenser för de enskilda (*principen om integritet och konfidentialitet*)
- Visa att personuppgifterna behandlas enligt de grundläggande principerna (*principen om ansvarsskyldighet*)

De grundläggande principerna kan implementeras i organisationen på olika sätt, genom utbildning av medarbetare, styrdokument, kravställning på leverantörer och implementering av principerna i arbetsprocesser där personuppgifter behandlas.

3.2.1 Krav och uppföljning under granskning 2024

Kontrollpunkt/krav	Metod för uppföljning	Resultat 2024	Resultat 2023
Kännedom om de grundläggande principer finns och dessa beaktas i verksamhetens arbete som rör personuppgifter	Granskning av stadens och förvaltningens rutiner vid inköp av nya tjänster, upphandling och projekt där personuppgifter förekommer.		-
Medarbetare har fått grundläggande utbildning i GDPR	Statistik över stadens obligatoriska e-utbildningar.		-

3.2.2 Uppföljning av föregående års rekommendationer

Detta kravområde fanns inte inkluderat i dataskyddsombudets årsrapport 2023, därmed saknas rekommendationer att följa upp.

3.2.3 Nämndens efterlevnad av kraven

Utbildningen i dataskydd tar upp de grundläggande dataskyddsprinciperna, men i övrigt finns låg kunskap om principerna och varken stadens och förvaltningens styrdokument eller vägledningar tydliggör att det är de grundläggande principerna som ska genomsyra all personuppgiftsbehandling och som sätter ramarna för vad som är tillåtet.

I processer där nya och förändrade personuppgiftsbehandlingar ”uppstår”, främst vid inköp av nya IT-system, nyutveckling av system, upphandlingar och projekt, är det särskilt viktigt att ta hänsyn till de grundläggande principerna från början och säkerställa att systemets/tjänstens utformning/funktionalitet och det tänkta arbetssättet med personuppgifter sker i enlighet med principerna.

Inför en upphandling, inköp av tjänst eller projekt som berör förvaltningens information görs vanligtvis en informationsklassning för att värdera den information som tjänsten har tänkt att innehålla. Sedan ställs informationssäkerhetskrav på leverantören utifrån informationsklassningen. En informationsklassning i sig säger dock inget om den personuppgiftsbehandling som kommer att ske är tillåten eller inte, utan det är de grundläggande principerna som avgör detta. En granskning av hur den tänkta personuppgiftsbehandlingen överensstämmer med de grundläggande principerna behöver alltså göras för att säkerställa att personuppgiftsbehandlingen är tillåten.

Denna granskning är idag inte en systematisk del av förvaltningens informationsklassningsprocess eller andra processer där nya personuppgiftsbehandlingar initieras (exempelvis inköp eller projekt) eller förändras (exempelvis förändringar/nyutveckling i system). I de fall en konsekvensbedömning gjorts (se avsnitt 3.4) har de grundläggande principerna tagits om hand i den processen och dataskyddsombudet har även tagit fram vägledning för hur förvaltningen kan utvärdera en IT-tjänst utifrån de grundläggande principerna som används i delar av verksamheten idag.

Vad gäller utbildning till medarbetare visar statistik från utbildningsplattformen att ca 72 procent av medarbetarna (inkluderar även vikarier och konsulter) inte genomgått den obligatoriska utbildningen i dataskydd. Statistiken visar dock enbart hur många som gått utbildningen sedan den blev obligatorisk i maj 2023 och vissa av personerna kan ha gått utbildningen i dataskydd tidigare. Siffran visar ändå att en stor andel av medarbetare på utbildningsförvaltningen antingen inte fått grundläggande utbildning i dataskydd eller inte uppdaterat sina kunskaper de senaste 1,5 åren.

3.2.4 Råd och rekommendationer till PUA

I dagsläget är de grundläggande principerna inte införlivade i de processer där personuppgifter behandlas, särskilt upphandling, inköp av tjänster och i projekt. Dataskyddsombudet rekommenderar därför att:

- Krav på inbyggt dataskydd ställs i upphandlingar och kravställningen i övrigt överensstämmer med de grundläggande principerna.
- De grundläggande principerna inkluderas i processer som berör inköp av nya tjänster, utveckling av nya funktioner och projekt/piloter/POC (och som innebär en personuppgiftsbehandling). Om hög risk föreligger (se avsnitt 3.4 nedan) ska även en konsekvensbedömning göras innan faktiska personuppgifter behandlas.

Statistik från utbildningsplattformen visar att en stor andel av medarbetare på utbildningsförvaltningen inte gått den obligatoriska utbildningen i dataskydd. Dataskyddsombudet rekommenderar därför att:

- Åtgärder vidtas för att höja andelen medarbetare som genomgått utbildningen, exempelvis genom informationsinsatser.

3.3 Personuppgiftsincidenter

Personuppgiftsincidenter är säkerhetsincidenter där personuppgifter, oavsiktligt eller avsiktligt, har förvanskats, raderats, är otillgängliga för verksamheten eller blivit tillgängliga för obehöriga. Hantering av personuppgiftsincidenter är en obligatorisk komponent bland dataskyddsförordningens olika verktyg för att åstadkomma en sund personuppgiftshantering.

Varje personuppgiftsansvarig ska ha processer för att upptäcka, utreda och åtgärda personuppgiftsincidenter samt anmäla vissa incidenter till tillsynsmyndigheten Integritetsskyddsmyndigheten (IMY). Det innebär att medarbetare ska kunna identifiera när en personuppgiftsincident har hänt, veta hur den ska rapporteras och att det finns processer för att ta hand om en bekräftad incident. Det är även av vikt att incidenten leder till uppdaterade rutiner och arbetssätt för att förhindra nya incidenter.

3.3.1 Krav och uppföljning under granskning 2024

Kontrollpunkt/krav	Metod för uppföljning	Resultat 2024	Resultat 2023
Medarbetare är informerade om definitionen och processen för informationssäkerhets-incidenter	Granskning av förvaltningens rutiner för kommunicering av anvisningen och antal incidenter per avdelning.		
Incidenterna har följts upp och föreslagna åtgärder har vidtagits.	Granskning av förvaltningens rutiner för uppföljning av incidenter.		

3.3.2 Uppföljning av föregående års rekommendationer

I 2023 års rapport rekommenderade dataskyddsombudet att anvisningar för informationssäkerhetsincidenter kommuniceras ut till medarbetare och att anvisningarna tydliggörs för att betona vikten av åtgärder för att förhindra framtida incidenter. Som redogörs nedan har anvisningen kommunicerats ut under 2024 men alla avdelningar har inte rapporterat in personuppgiftsincidenter och anvisningar har ännu inte uppdaterats utifrån dataskyddsombudets rekommendationer.

3.3.3 Nämndens efterlevnad av kraven

Utbildningsförvaltningen har en beslutad anvisning för hantering av informationssäkerhetsincidenter som följs vid en konstaterad informationssäkerhetsincident. Då alla personuppgiftsincidenter klassas som informationssäkerhetsincidenter gäller anvisningen även för personuppgiftsincidenter.

Anvisningen har kommunicerats ut i samordningsfunktionen för dataskydd och informationssäkerhet, förvaltningens forum för funktioner som arbetar med dataskydd och informationssäkerhet, och respektive av avdelnings personuppgiftskoordinator (PUK) har haft i uppgift att kommunicera vidare anvisningen på sin avdelning. Grundskolor har informerats på särskilda möten för skolornas personuppgiftskoordinatorer (Skol-PUK:ar). Det finns även särskilt framtagna mallar som kan användas av skolor eller enheter vid APT:er och liknande för att informera om informationssäkerhetsincidenter.

Under 2024 har 34 personuppgiftsincidenter rapporterats in, varav 7 anmälts vidare till IMY. Alla avdelningar har dock inte rapporterat in incidenter vilket kan bero på att anvisningen inte kommunicerats fullt ut till samtliga medarbetare.

Anvisningen och tillhörande mallar anger i dagsläget inte uttryckligen att åtgärder för att förhindra framtida incidenter alltid ska vidtas vid en incident. Vid allvarliga eller kritiska incidenter ska ett uppföljningsmöte ske för att dra lärdomar, men för övriga incidenter saknas tydliga anvisningar om att åtgärder bör ske vid varje incident.

3.3.4 Råd och rekommendationer till PUA

I stort har nämnden en förmåga att upptäcka och hantera personuppgiftsincidenter. Eftersom inte alla avdelningar rapporterat in incidenter under året rekommenderar dataskyddsombudet dock att:

- säkerställa att relevanta delar av anvisningen når ut till samtliga medarbetare så att alla känner till definitionen av en incident och vet hur den ska rapporteras.

Som nämns ovan anger anvisningen och rapporteringsmallarna inte tydligt nog att åtgärder för att förhindra framtida incidenter alltid ska vidtas även om förvaltningen i praktiken vidtar åtgärder för att förhindra framtida incidenter. För att betona vikten av att lära sig av

upptäckta incidenter, rekommenderar dataskyddsombudet därför också att:

- mallarna och anvisning revideras för att förtydliga att varje incident ska kräva minst en dokumenterad åtgärd för att förhindra framtida incidenter och att incidenter följs upp för att identifiera och införa förbättringar.

3.4 Konsekvensbedömningar (DPIA)

Om det finns en hög risk för enskildas fri- och rättigheter när personuppgifter behandlas, ska den personuppgiftsansvarige göra en konsekvensbedömning enligt GDPR (även kallad DPIA, Data Protection Impact Assessment) innan personuppgiftsbehandlingen påbörjas. Hög risk anses föreligga exempelvis vid övervakning eller kartläggning av personer, behandling av känsliga personuppgifter, behandling av personuppgifter i stor mängd om personer i beroendeställning (exempelvis anställda eller barn) eller användning av ny teknik (exempelvis AI).

Konsekvensbedömningar hjälper en organisation att identifiera och minimera integritetsriskerna för personuppgifter som behandlas. Baserat på bedömningen ska riskminimerande åtgärder vidtas. Om en hög risk kvarstår efter en konsekvensbedömning ska dessutom tillsynsmyndigheten (IMY) kontaktas för ett förhandssamråd innan personuppgiftsbehandlingen påbörjas. Eftersom en konsekvensbedömning ska göras innan personuppgiftsbehandlingen påbörjas är det viktigt att förvaltningen har processer för att fånga upp nya personuppgiftsbehandlingar, exempelvis i projekt eller nyutveckling av IT-tjänster, och kunna bedöma om en konsekvensbedömning krävs.

3.4.1 Krav och uppföljning under granskning 2024

Kontrollpunkt/krav	Metod för uppföljning	Resultat 2024	Resultat 2023
Dokumentation och bedömning om befintliga personuppgifts-behandlingar kräver en konsekvensbedömning (DPIA) är gjord.	Granskning av förvaltningens dokumentation av konsekvens-bedömningar.		
Rutiner för att säkerställa att konsekvens-bedömningar görs, där så krävs, för framtida personuppgifts-behandlingar finns.	Granskning av förvaltningens rutiner.		
Riskminimerande åtgärder från konsekvens-bedömningar har följts upp och genomförts	Stickprov av de konsekvensbedömningar som genomförts.		

3.4.2 Uppföljning av föregående års rekommendationer

I 2023 års rapport rekommenderade dataskyddsombudet att det säkerställs att konsekvensbedömningar görs för befintliga personuppgiftsbehandlingar och att en bedömning om en konsekvensbedömning krävs eller inte uttryckligen framgår av process- eller rutinbeskrivningar där nya personuppgiftsbehandlingar initieras, exempelvis processer relaterade till projekt eller inköp av IT-tjänster. Som beskrivs utförligare nedan har förvaltningen under 2024 genomfört ett antal konsekvensbedömningar i enlighet med dataskyddsförordningens krav och nämndens efterlevnad inom området har förbättrats, dock krävs fortsatt ett betydande arbete för att komma uppfylla kraven på konsekvensbedömningar.

3.4.3 Nämndens efterlevnad av kraven

Under 2024 har flera konsekvensbedömningar gjorts, bland annat inom ramen för upphandling av nya systemstöd inom skolplattformen. Dock har ingen systematisk genomgång av alla befintliga personuppgiftsbehandlingar gjorts och dokumenterats för att säkerställa att förvaltningen genomfört konsekvensbedömningar, där så krävs. Av Integritetsskyddsmyndighetens (IMY) vägledning går det att utläsa att de flesta av de personuppgiftsbehandlingar som

sker inom utbildningsnämndens verksamhetsområde bör konsekvensbedömmas enligt dataskyddsförordningen. Det finns därmed flera personuppgiftsbehandlingar som pågår idag men där förvaltningen inte gjort en konsekvensbedömning.

Det saknas även rutiner/processer för att säkerställa att framtida personuppgiftsbehandlingar genomgår en konsekvensbedömning, där så krävs, förutom vid kamerabevakning. I de lokala anvisningarna för informationssäkerhet och i stadens styrdokument för informationssäkerhet anges att vissa roller har ansvar för att en konsekvensbedömning görs, men förutom vid projekt är ansvaret inte tydligt nog och styrdokumenten är idag inte fullt ut implementerade i verksamheten.

Vad gäller uppföljning av risker från konsekvensbedömningarna är det idag inte tydligt vem som ska följa upp och säkerställa att åtgärder för att hantera riskerna vidtagits. Därför har riskerna och åtgärderna enbart delvis följts upp, där enskilda medarbetare tagit initiativ till detta.

3.4.4 Råd och rekommendationer till PUA

Konsekvensbedömningar genomförs inte systematiskt idag, varken där det krävs för befintliga eller på ett systematiskt sätt för framtida konsekvensbedömningar. På grund av den typ av verksamhet som utbildningsnämnden bedriver, där personuppgifter om barn, i stor omfattning och i många delar känsliga och integritetskänsliga uppgifter förekommer, är det troligt att kriterierna för när en konsekvensbedömning krävs uppfylls i flertalet av situationer där nämndens personuppgifter behandlas. Många befintliga personuppgiftsbehandlingar saknar därmed en konsekvensbedömning idag. Dataskyddsombudet rekommenderar därför att:

- Identifiera vilka pågående personuppgiftsbehandlingar som uppfyller kritikerna för när en konsekvensbedömning krävs.
- Genomföra konsekvensbedömningarna i enlighet med de formella kraven i dataskyddsförordningen, inkluderat även en plan för implementering och uppföljning av riskminimerande åtgärder.
- Säkerställa att konsekvensbedömningar görs för framtida personuppgiftsbehandlingar genom att se över befintliga rutiner/processer där nya personuppgiftsbehandlingar initieras (exempelvis vid köp av en ny IT-tjänst eller projekt).

3.5 Personuppgiftsbiträden (roller och ansvar)

Om fler än en aktör, exempelvis nämnder, leverantörer, myndigheter, är involverade i en personuppgiftsbehandling är det viktigt att utreda och fastställa respektive aktörs roll i personuppgiftsbehandlingen. Detta för att varje aktör ska känna till sitt ansvar. När fler än en aktör är involverad i en personuppgiftsbehandling kan följande kombinationer av ansvar uppstå:

- Varje part är självständig personuppgiftsansvarig.
- En eller flera parter är personuppgiftsbiträde åt en eller flera personuppgiftsansvariga. Personuppgiftsbiträdesavtal (PUB-avtal) behöver tecknas mellan personuppgiftsbiträdet och personuppgiftsansvarig.
- Parterna är gemensamt personuppgiftsansvariga. Ett ”inbördes arrangemang” där parternas ansvar framgår ska tas fram.

En organisation behöver därför ha kartlagt externa parter/leverantörer som är involverade i en personuppgiftsbehandling och sedan teckna PUB-avtal, om ett biträdesförhållande identifieras, eller ta fram ett ”inbördes arrangemang” om ett gemensamt personuppgiftsansvar fastställts.

3.5.1 Krav och uppföljning under granskning 2024

Kontrollpunkt/krav	Metod för uppföljning	Resultat 2024	Resultat 2023
Externa parter/leverantörer har kartlagts och en bedömning ifall parten/leverantören är personuppgiftsbiträde/gemensamt personuppgiftsansvarig är gjord	Granskning av förvaltningens rutiner vid upphandlingar, inköp av tjänster och samarbetsprojekt		-
Personuppgiftsbiträdesavtal (PUB-avtal) har tecknats med personuppgiftsbiträden	Granskning av information i registerförteckningen		-
PUB-avtal följs upp	Granskning av förvaltningens rutiner för uppföljning av incidenter		-

3.5.2 Uppföljning av föregående års rekommendationer

Detta kravområde fanns inte inkluderat i dataskyddsombudets årsrapport 2023, därmed saknas rekommendationer att följa upp. Dock tog dataskyddsombudet upp brister i uppföljning av PUB-avtal som en särskild risk som kräver åtgärd.

3.5.3 Nämndens efterlevnad

Förvaltningen har rutiner för att säkerställa att personuppgiftsbiträdesavtal (PUB-avtal) tecknas vid upphandlingar och inköp av tjänster. Nämndens delegationsordning anger att enbart IKT-enhetens chef är behörig att teckna PUB-avtal vilket betyder att förvaltningen har kontroll över vilka PUB-avtal som tecknas. Innan ett PUB-avtal tecknas granskas biträdet och tjänsten utifrån informationssäkerhetskrav och tredjelandsöverföring. Vid upphandling ställs krav på informationssäkerhet och tredjelandsöverföring. Förvaltningen har därmed processer för att säkerställa att PUB-avtal tecknas, där så krävs, när det kommer till upphandlingar och inköp av tjänster. Dock har ingen kartläggning av alla externa parter gjorts för att säkerställa att PUB-avtal tecknats, när det inte rör sig om inköp av tjänster eller upphandling, eller framtagande av ”inbördes arrangemang”, vid gemensamt personuppgiftsansvar. Idag har nämnden inga ”inbördes arrangemang” med en annan part.

PUB-avtal och biträdets hantering av personuppgifter ska också följas upp. I dagsläget följs inte PUB-avtal upp särskilt, dock sker annan avtalsuppföljning där dataskyddsfrågor kan behandlas.

3.5.4 Råd och rekommendationer till PUA

Nämnden har rutiner för att säkerställa att PUB-avtal tecknas med leverantörer av IT-tjänster, dock har ingen systematisk genomgång av samtliga roller gjorts och rutiner för att följa upp PUB-avtal saknas. Dataskyddsombudet rekommenderar därför att:

- Samtliga externa parter, även andra nämnder och myndigheter, kartläggs och en bedömning görs om parternas roller och ansvar, förslagsvis baserat på information från registerförteckningen.
- Processer för att följa upp PUB-avtal tas fram.

3.6 Tredjelandsöverföring

Tredjelandsöverföring innebär att personuppgifter överförs till ett land utanför EU/EES. Detta kan ske exempelvis genom en leverantör utanför EU/EES anlitas, personuppgifter skickas till ett land utanför EU/EES eller någon utanför EU/EES ges åtkomst till personuppgifter genom fjärråtkomst vid support.

Inom EU/EES finns ett likvärdigt skydd för personuppgifter och personlig integritet genom dataskyddsförordningen. Utanför EU/EES finns däremot inget motsvarande skydd. För att inte undergräva skyddet för enskilda personuppgifter och övriga fri- och rättigheter finns därför regler om när det är tillåtet att föra över personuppgifter till tredjeland.

3.6.1 Krav och uppföljning under granskning 2024

Kontrollpunkt/krav	Metod för uppföljning	Resultat 2024	Resultat 2023
Rutiner för att kontrollerat om personuppgifter överförs till tredje land (ett land utanför EU/ESS) finns.	Granskning av förvaltningens rutiner för tredjelandsöverföring		-
Om uppgifter överförs till tredjeland har lagligheten säkerställts.	Granskning av förvaltningens rutiner vid tredjelandsöverföring		-

3.6.2 Uppföljning av föregående års rekommendation

Detta kravområde fanns inte inkluderat i dataskyddsombudets årsrapport 2023, därmed saknas rekommendationer att följa upp.

3.6.3 Nämndens efterlevnad av kraven

Inom utbildningsnämnden sker tredjelandsöverföring huvudsakligen när ett personuppgiftsbiträde/leverantör anlitas utanför EU/EES eller om support sker från ett land utanför EU/EES. Staden har en restriktiv hållning gällande överföring till tredjeland, men utbildningsförvaltningen har i ett ställningstagande fattat beslut om att överföring till USA är möjlig under förutsättning att det amerikanska bolaget är anslutet till EU-US Data Privacy Framework. Vid upphandlingar och inköp av tjänster, vilket också

framgår av förvaltningens mall för PUB-avtal, är tredjelandsöverföring i regel inte tillåtet. Om ett anlitande av en leverantör ändå leder till tredjelandsöverföring sker en granskning av lagligheten innan PUB-avtal tecknas.

3.6.4 Råd och rekommendationer till PUA

Staden har i stort redan ett restriktivt hållningssätt till tredjelandsöverföring, därmed sker tredjelandsöverföring sällan och om tredjelandsöverföring sker kontrolleras lagligheten. När det kommer till stora molntjänster som M365 har rapporter och tillsynsärenden[1] visat att det kan vara krångligt att ta reda på vilka faktiska tredjelandsöverföringar som sker, därför rekommenderar dataskyddsombudet att:

- Förvaltningen kartlägger samtliga tredjelandsöverföring i tjänster där förvaltningens PUB-avtal inte gäller och där leverantören enligt villkoren kan överföra personuppgifter till tredjeland, exempelvis M365 och Adobe.

[1] https://www.edps.europa.eu/press-publications/press-news/press-releases/2024/european-commissions-use-microsoft-365-infringes-data-protection-law-eu-institutions-and-bodies_en

3.7 Arkivering och gallring (lagringsminimering)

Lagringsminimering är en av dataskyddsprinciperna och handlar om att personuppgifter endast får behandlas så länge de behövs för ändamålet. Personuppgifter förekommer ofta i allmänna handlingar och myndigheter är skyldiga att ha ordning och reda på sin information. Hanteringsanvisningar anger om informationen ska gallras, i så fall när, eller om den ska bevaras (arkiveras). Personuppgifter som inte ingår i allmänna handlingar ska rensas när de inte längre behövs. Om personuppgifter sparas längre än gallringsfristerna anger och inget annat syfte med att spara personuppgifterna föreligger, är personuppgiftsbehandlingen inte tillåten.

Gallring och arkivering av förvaltningens information har andra fördelar utifrån ett dataskyddsperspektiv förutom att principen om lagringsminimering följs, exempelvis att skadan av ett intrång eller läckage blir mindre eftersom färre personuppgifter behandlas i ett system.

3.7.1 Krav och uppföljning under granskning 2024

Kontrollpunkt/krav	Metod för uppföljning	Resultat 2024	Resultat 2023
Hanteringsanvisningarna är upprättade och uppdaterade.	Granskning av förvaltningens rutiner för uppdatering och upprättande av hanteringsanvisningar.		-
Arkivering och gallring genomförs enligt hanteringsanvisningen.	Stickprov av arkiverings- och gallringsrutiner i förvaltningens centrala system.		-

3.7.2 Uppföljning av föregående års rekommendationer

Detta kravområde fanns inte inkluderat i dataskyddsombudets årsrapport 2023, därmed saknas rekommendationer att följa upp. Dock tog dataskyddsombudet upp arkivering och gallring som en särskild risk som kräver åtgärd.

3.7.3 Nämndens efterlevnad av kraven

Enheten för arkiv, registratur och förvaltningsservice (ARF-enheten) på avdelningen för personal och kompetensförsörjning är ansvarig för att upprätta och hålla nämndens hanteringsanvisningar uppdaterade. Uppdatering av hanteringsanvisningarna sker fyra gånger per år. Den verksamhet som hanterar informationen är dock ansvarig för att meddela ARF-enheten om förändringar i deras informationshantering och säkerställa att hanteringsanvisningarna täcker in de allmänna handlingar som verksamheten producerar.

Förvaltningens ansvar och organisation vad gäller arkivering och gallring anges i förvaltningens arkivinstruktion. Arbetet styrs, förutom av lagar och förordningen, av stadens arkivregler. Fokus för uppföljningen under 2024 har varit hanteringen i de centrala systemen då systemen hanterar en stor mängd information och tidigare årsrapport identifierat brister i gallring och arkivering i de centrala systemen.

Under 2023 och 2024 har projektet SALVE pågått vars syfte varit att omhänderta arkivering och gallring i de systemen som ingått i under det tidigare samlingsnamnet Skolplattformen, men som nu ersatts av nya appar och tjänster. Projektet kommer att avslutas innan årsskiftet. Arkivering och gallring inom ramen för projektet är planerat och har förberetts men inte skett innan årsskiftet. Vissa centrala system har ännu inte infört gallrings- och arkiveringsfunktioner, men dessa är planerade att införas under 2025.

3.7.4 Råd och rekommendationer till PUA

Förvaltningen har fungerande rutiner för att säkerställa hanteringsanvisningarna hålls uppdaterade, men arkivering och gallring av information i de centrala systemen sker inte tillfredsställande idag. Dataskyddsombudet rekommenderar därför att:

- Samtliga IT-tjänster har stöd för arkivering och gallring samt att arkivering och gallring verkställs enligt genomförda bevarande- och gallringsutredningar.
- Rutiner för informationens livscykelhantering finns med i objektsförvaltningens alla delar: upphandling/inköp, drift/ibruktagande och avveckling.
- Bevarande- och gallringsutredningar genomförs och tekniska funktioner för gallring/arkivering säkerställs inför driftsättande av nya system eller tjänster.

3.8 Registrerades rättigheter

Registrerade, personers personuppgifter nämnden behandlar, har enligt dataskyddsförordningen (artikel 12–22) ett antal rättigheter som på olika sätt ska garantera att den registrerade har en viss kontroll över och insyn i hur dennes personuppgifter hanteras. Följande rättigheter har den registrerade i förhållande till sina personuppgifter:

- Rätt att vända sig till en personuppgiftsansvarig för att få bekräftat om ens personuppgifter behandlas och i så fall få tillgång till dessa (Rätt till tillgång – även kallat ”registerutdrag”)
- Rätt att få information om hur personuppgifter hanteras (rätten till information)
- Under vissa förutsättningar få sina uppgifter raderade eller rättade (rätten till radering och rättelse)
- Rätt att invända, dvs. motsätta sig, mot en personuppgiftsbehandling och även begära begränsning av personuppgifternas användning (rätten att göra invändningar och begära begränsning)
- Rätt att inte bli föremål för automatiskt beslutsfattande
- Rätt att få ut sina personuppgifter på ett strukturerat sätt för att använda de hos någon annan (rätt till dataportabilitet – gäller enbart i få specifika fall inom offentlig förvaltning)

För att den registrerade ska kunna utöva sina rättigheter krävs att den personuppgiftsansvariga känner till rättigheterna och har rutiner för att ta hand om en begäran om att utöva något av rättigheterna. Den personuppgiftsansvarige har även krav på att underlätta utövande av rättigheter.

Rätten till information gäller dock utan att en enskild behöver begära detta särskilt. Detta betyder att en personuppgiftsansvarig måste ha säkerställt att information finns tillgänglig för den registrerade om respektive personuppgiftsbehandling som sker.

3.8.1 Krav och uppföljning under granskning 2024

Kontrollpunkt/krav	Metod för uppföljning	Resultat 2024	
Rutiner för utlämnade av registerutdrag (rätten till tillgång) finns, utdraget lämnas ut enligt kraven i GDPR och inom den lagstadgade tidsramen	Granskning av förvaltningens rutiner för registerutdrag och hanterade registerutdrag under året.		
Enskilda har informerats om hur deras personuppgifter hanteras (rätt till information)	Granskning av förvaltningens informationstexter till registrerade.		-
Rutiner för att hantera övriga rättigheter, dvs. begäran om radering, rättelse, invändning och begränsning (samt dataportabilitet, om tillämplig) finns och begäran hanteras inom den lagstadgade tidsramen	Granskning av förvaltningens rutiner och stickprov av hanterade begäran under året.		-

3.8.2 Uppföljning av föregående års rekommendationer

Kravområdet fanns enbart delvis med i föregående års rapport – enbart förvaltningens hantering av registerutdrag (rätten till tillgång) inkluderades dock togs brister i information till registrerade upp som en särskild risk som kräver åtgärd.

I 2023 års rapport rekommenderade dataskyddsombudet att rutinen för registerutdrag/rätten till tillgång ses över för att säkerställa att svar lämnas i tid och för att tydliggöra att tillgång till de faktiska personuppgifterna (en kopia) ska ges till den registrerade i första skedet. Rutinen har setts över under 2024 och förvaltningen ger nu tillgång till de faktiska personuppgifterna, dock lämnas registerutdrag i majoriteten av fallen fortfarande inte i tid.

3.8.3 Nämndens efterlevnad av kraven

Förvaltningen har rutiner för att ta hand om registerutdrag (rätten till tillgång), radering och rättelse. Skriftliga rutiner för övriga

rättigheter saknas i dagsläget. Under 2024 har rutinen för registerutdrag (rätten till tillgång) setts över för att säkerställa att den registrerade även ges en kopia på sina personuppgifter och att begäran hanteras i tid. Förvaltningen har under 2024 hanterat 14 begäran om registerutdrag. Statistik för radering, rättelse och övriga rättigheter saknas då en registrerad ofta vänder sig direkt till den verksamhet som behandlar personuppgifterna och om rättigheten kan tillgodoses, registreras inget ärende. Av de begäran som dataskyddsombudet granskat har endast ca en fjärdedel hanterats inom den lagstadgade tidsramen. Under granskningen har det också framkommit att kopian på personuppgifterna i vissa fall inte kan tas ut i ett begripligt format, vilket leder till att den registrerade inte kan kontrollera personuppgifterna laglighet och riktighet (vilket är syftet med registerutdraget).

Rätten till information eller informationsplikten handlar om att ge den registrerade en komplett bild över varför och hur personuppgifterna behandlas. Dataskyddsförordningen reglerar dels vilken typ av information som ska ges och när (beroende på om personuppgifterna samlas in direkt från den enskilde eller från en annan källa) och att informationen ska ges på ett begripligt och tillgängligt sätt. Skolorna informerar vårdnadshavare och elever vid läsårsstart. Informationen innehåller till viss del den information som krävs, men beskrivningen utgår främst från IT-tjänster som används och inte de faktiska personuppgiftsbehandlingarna. Övriga personer vars personuppgifter behandlas, exempelvis anställda, informeras inte särskilt i dagsläget.

3.8.4 Råd och rekommendationer till PUA

I dagsläget hanteras registrerades rättigheter inte inom de lagstadgade tidsramen i majoriteten av fallen. Registrerade informeras inte om hur deras personuppgifter hanteras i tillräcklig omfattning i enlighet med dataskyddsförordningens krav. Dataskyddsombudet rekommenderar därför att:

- Åtgärder vidtas för att säkerställa att begäran från registrerade om att utöva sina rättigheter hanteras inom den lagstadgade tidsramen.
- Åtgärder vidtas för att säkerställa att underlaget i ett registerutdrag (rätten till tillgång) är begriplig för den registrerade.
- Förvaltningen säkerställer att respektive verksamhet (enhet, avdelning eller skola) informerar sina registrerade enligt kraven i dataskyddsförordningen. För att detta ska bli effektivt krävs samordning av informationstexterna mellan

verksamheter som behandlar uppgifter om samma typ av registrerad (exempelvis elev i grundskola).

3.9 Känsliga och integritetskänsliga personuppgifter

Det finns ett generellt förbud mot att hantera känsliga personuppgifter i dataskyddsförordningen. Det är enbart tillåtet om ett av undantagen är tillämpliga, därför är det viktigt att veta om känsliga personuppgifter behandlas och om den är tillåten. Förutom känsliga personuppgifter, finns det en grupp personuppgifter kallat integritetskänsliga personuppgifter som inte kräver ett undantag för att det ska vara tillåtet att hantera dem men är samtidigt av en karaktär som kräver att de skyddas med högre säkerhet. Dessa typer av uppgifter och känsliga personuppgifter får enbart hanteras enligt säkerskilda rutiner och i system/lagringsytor med högre krav på konfidentialitet.

3.9.1 Krav och uppföljning under granskning 2024

Kontrollpunkt/krav	Metod för uppföljning	Resultat 2024	Resultat 2023
Om känsliga personuppgifter hanteras, har ett undantag enligt artikel 9 GDPR säkerställts.	Stickprov av personuppgiftsbehandlingar från registerförteckningen.		-
Rutiner för hur och var känsliga och integritetskänsliga personuppgifter får hanteras finns och har kommunicerats till medarbetare	Granskning av förvaltningens rutiner och kommunicering av dessa.		-

3.9.2 Uppföljning av föregående års rekommendationer

Detta kravområde fanns inte inkluderat i dataskyddsombudets årsrapport 2023, därmed saknas rekommendationer att följa upp.

3.9.3 Nämndens efterlevnad av kraven

Myndigheter får enligt dataskyddslagen 3 kap. 3 § behandla personuppgifter med stöd av artikel 9.1g i GDPR

- om uppgifterna har lämnats till myndigheten och behandlingen krävs enligt lag,
- om behandlingen är nödvändig för handläggningen av ett ärende, eller i annat fall,

- om behandlingen är nödvändig med hänsyn till ett viktigt allmänt intresse och inte innebär ett otillbörligt intrång i den registrerades personliga integritet.

Personuppgifter som behandlas inom hälso- och sjukvården inom elevhälsan behandlas med stöd av patientdatalagen. En granskning av slumpmässigt utvalda personuppgiftsbehandlingar från registerförteckningen visar att nämnden har en rättslig grund för att behandla känsliga personuppgifter där denna typ av uppgifter förekommer.

Vad gäller rutiner för att hantera känsliga och integritetskänsliga personuppgifter har nämnden en beslutad anvisning för personuppgifter i kommunikationsverktyg och digitala dokument/datafiler på utbildningsförvaltningen. För vissa IT-tjänster finns instruktioner för vilka typer av uppgifter som kan hanteras i tjänsten. Rutiner och anvisningar för känsliga och integritetskänsliga personuppgifter generellt kommuniceras i samordningsfunktionen för dataskydd och informationssäkerhet och har även tagits upp med grundskolornas personuppgiftskoordinatorer. Dock inkommer ofta frågor från medarbetare om hur de får hantera en viss typ av personuppgift och förvaltningens rutiner är inte tydliga nog kring vilken typ av personuppgift som får hanteras eller kommuniceras i vilken tjänst/system.

3.9.4 Råd och rekommendationer till PUA

Granskningen visar att det råder otydlighet kring vilka typer av personuppgifter som får hanteras i vilka tjänster/system. Dataskyddsombudet rekommenderar därför att:

- Uppdaterad vägledning för hur och var känsliga och integritetskänsliga personuppgifter får hanteras tas fram, inkluderat särskilt kommunicering (e-post) och lagring.

3.10 Informationssäkerhet

En av de grundläggande principerna är integritet och konfidentialitet som handlar om att kunna säkerställa personuppgifternas konfidentialitet (att inga uppgifter röjs för obehöriga), tillgänglighet (att uppgifterna är tillgängliga när de behövs) och riktighet (att uppgifterna är korrekta). I artikel 32 ställs dessutom särskilt krav på säkerhet vid behandling av personuppgifter. Det innebär att ett aktivt och systematiskt med informationssäkerhet krävs för att uppfylla kraven.

Stadens riktlinjer för informationssäkerhet anger att alla stadens informationstillgångar ska vara klassade med stöd av SKR:s verktyg KLASSA. Utan informationsklassningen har verksamheten inte förutsättningar att välja rätt åtgärder för att skydda sin information. Det är därför av stor betydelse för dataskyddsarbetet att informationsklassning är genomförd för personuppgifter som verksamheten hanterar. Informationsklassning är dock endast första steget i att kunna genomföra tekniska och organisatoriska åtgärder. När informationens skyddsvärde är känd, ska tekniska och organisatoriska åtgärder vidtas för att skydda informationen. En viktig teknisk och organisatorisk åtgärd är behörighetshantering. Då utbildningsnämnden behandlar personuppgifter i stor omfattning och i många situationer även känsliga och integritetskänsliga är det av vikt att behörighetshanteringen fungerar, både den tekniska styrningen över vad en användare kommer åt och rutiner för att säkerställa att behörigheterna hålls uppdaterade över tid.

3.10.1 Krav och uppföljning under granskning 2024

Kontrollpunkt/krav	Metod för uppföljning	Resultat 2024	Resultat 2023
Informationstillgångar har informationsklassats	Granskning av genomförda informationsklassningar och information från registerförteckningen		
Informationsklassningen inkluderar även tekniska och organisatoriska säkerhetsåtgärder för att skydda personuppgifter	Stickprov av genomförda informationsklassningar		-
Tillgång till personuppgifter har behörighetsstyrts enligt principen lägsta behörighet och behörigheterna följs upp regelbundet	Stickprov av behörighetsstruktur och rutiner för behörighetsadministration i förvaltningens centrala system.		-

3.10.2 Uppföljning av föregående års rekommendationer

Kravområdet fanns enbart delvis med i föregående års rapport – enbart genomförda informationsklassningar följdes upp. I 2023 års rapport rekommenderade dataskyddsombudet att fokusera på att klassificera information i stället för att klassificera informationen i respektive IT-system, vilket även var dataskyddsombudets rekommendation året innan. Informationsklassning genomförs fortfarande efter IT-system. Dock är förvaltningens långsiktiga plan att informationsklassning genomförs efter informationsmängd. Som redogörs för närmare nedan har förvaltningen under 2024 inte uppdaterat samtliga informationsklassningsprotokoll vilket betyder att flera IT-system saknar uppdaterade informationsklassningar.

3.10.3 Nämndens efterlevnad av kraven

Nämndens verksamheter genomför idag informationsklassningar efter system eller tjänst och inte informationsmängder. Det betyder att skyddet för personuppgifter inte nödvändigtvis upprätthålls genom hela processen/behandlingen, då personuppgifter kan behandlas i olika system, lagringsplatser och liknande i en process/personuppgiftsbehandling.

En genomgång av information i registerförteckningen visar att ca 60 procent av alla personuppgiftsbehandlingar sker i system som

samtliga är klassade. Övriga personuppgiftsbehandlingar sker delvis eller helt i system som saknar informationsklassning. Informationen i registerförteckningen anger dock inte om informationsklassningen är aktuell och uppdaterad. En genomgång av genomförda informationsklassningar visar att endast 22 (av 72) IT-system har uppdaterade informationsklassningsprotokoll. Det finns därmed ett behov av en översyn av informationsklassningarna. En granskning av ett urval av informationsklassningsprotokoll visar att det i flera fall saknas dokumenterade säkerhetsåtgärder som en följd av klassningen. I vissa fall har riskanalyser gjorts som lett till dokumenterade säkerhetsåtgärder.

Vad gäller behörighetsstyrning har systemen som omfattats av granskningen en dokumenterad behörighetsstruktur och beskrivning över rollerna. I ett av de centrala systemen är det inte möjligt att begränsa behörigheterna till det användaren behöver och dataskyddsombudet vill understryka vikten av att även teknisk begränsa åtkomst till uppgifter, särskilt när det gäller uppgifter om barn och skyddade personuppgifter. En uppföljning av behörigheter visar att användare i flera fall har en behörighet de inte har behov av längre. Chef över respektive verksamhet är ansvarig för att hålla behörigheterna uppdaterade och detta tyder på att en uppdatering av behörigheterna inte görs regelbundet i alla verksamheter.

3.10.4 Råd och rekommendationer till PUA

Flera av förvaltningens system och tjänster saknar uppdaterade informationsklassningar och de informationsklassningar som gjort inkluderar inte alltid implementation av faktiska tekniska och organisatoriska åtgärder. Uppföljning av behörigheterna visar att det i flera fall finns användare med behörighet till personuppgifter som förmodligen inte har behov av det. Dataskyddsombudet rekommenderar därför att:

- Uppdatering sker av samtliga IT-systems informationsklassningsprotokoll, vilka också inkluderar en handlingsplan och riskanalys med säkerhetsåtgärder. Säkerhetsåtgärderna ska implementeras och följas upp.
- Förvaltningsövergripande rutin/process tas fram för granskning av användares behörigheter. Respektive verksamhet bör minst årligen granska sina behörigheter.

4 Sammanfattning av dataskyddsombudets rekommendationer

Dataskyddsombudet har ovan redovisat nämndens efterlevnad av dataskyddsförordningen utifrån ett antal områden och krav. Nämnden bör kontinuerligt höja sin mognadsnivå inom dataskyddsområdet genom att aktivt arbeta med dataskyddskraven. Ett moget dataskyddsarbete är en förutsättning för en hållbar digitalisering och särskilt viktigt om nämnden exempelvis avser dra nytta av utvecklingen inom artificiell intelligens. Utifrån bedömningen av hur allvarliga avvikelserna som observerats i årets granskning är rekommenderar dataskyddsombudet att följande områden prioriteras i det fortsatta dataskyddsarbetet:

- Implementering av de grundläggande principerna i organisationens processer/arbetssätt rörande personuppgifter (se avsnitt 3.2)
- Genomförande av konsekvensbedömningar, vilket även inkluderar ett riskhanteringsarbete för att säkerställa att åtgärder genomförs och följs upp (se avsnitt 3.4)
- Uppföljning av personuppgiftsbiträdesavtalen (se avsnitt 3.5)
- Säkerställa funktioner för och verkställande av arkivering och gallring i förvaltningens IT-system (se avsnitt 3.7)
- Översyn av processen för registerutdrag och framtagande av informationstexter (se avsnitt 3.8)
- Höja aktivitetsnivån i informationsklassningsprocessen, inklusive arbetet med att införa tekniska och organisatoriska åtgärder (se avsnitt 3.10)

Dataskyddsombudet rekommenderar att en åtgärdsplan tas fram för att ta hand om råden inom de prioriterade områdena ovan.