Personuppgiftsansvarig

Utbildningsnämnden, Gävle kommun

Granskningsrapport 2024/2025

Dataskyddsombud

Boel Burman

Datum

2025-08-18

Innehåll

Sammanfattning

I aktuell granskning har dataskyddsombudet granskat styrande dokument. Det som har kontrolleras är hur den personuppgiftsansvarige uppfyller ansvarsskyldigheten i artikel 5.2. Granskningen visar att Utbildning Gävle har stora brister i sitt arbete med styrande dokument. Det saknas bland annat styrdokument för hantering av personuppgiftsbiträden, dataskyddsorganisation, behörighetsstyrning och fritextfält.

Dataskyddsombudet har också följt upp handlingsplaner och åtgärder som personuppgiftsansvarig vidtagit enligt tidigare rekommendationer som getts i samband med granskningarna 2022 och 2023. Enligt svar från den personuppgiftsansvarige har man 7 år efter att dataskyddsförordningen trädde i kraft inte en registerförteckning på plats. Det är allvarligt och ett skakrav enligt artikel 30 i dataskyddsförordningen.

1. Inledning

1.1 Allmänt om dataskyddsförordningen, GDPR

Dataskyddsförordningen, GDPR, trädde i kraft inom EU den 25 maj 2018 och är det generella regelverk som reglerar behandlingen av personuppgifter i såväl privat som offentlig sektor. Dataskyddsförordningen är bindande och direkt tillämplig i samtliga EU:s medlemsländer, men tillåter och förutsätter att medlemsstaterna kompletterar förordningen med nationell lagstiftning.

Dataskyddförordningen ska skydda enskildas grundläggande fri- och rättigheter, särskilt rätten till skydd av personuppgifter. Förordningens syfte är också att anpassa regelverket till det digitala samhället samt att skapa en enhetlig och likvärdig nivå för skyddet av personuppgifter inom EU så att det fria flödet av uppgifter inom unionen inte hindras.

Kraven i förordningen är ur ett internationellt perspektiv högt ställda och de organisationer som inte lever upp till dessa riskerar sanktioner från respektive lands tillsynsmyndighet. Den svenska tillsynsmyndigheten IMY, Integritetsskydds-myndigheten, har möjlighet att utdöma administrativa sanktionsavgifter för svenska myndigheter och företag.

1.2 Om årlig granskning

Enligt dataskyddsförordningen ska myndigheter samt företag som hanterar stora mängder personuppgifter ha ett utnämnt dataskyddsombud. Dataskyddsombudet, som har en fristående ställning i förhållande till myndigheten eller företaget, ska kontrollera att dataskyddsförordningen följs inom organisationen genom att bland annat genomföra kontroller och informationsinsatser.

Inom ramen för dataskyddsombudets kontrollerande arbete gör dataskyddsombudet en årlig granskning. Inriktningen på granskningen varierar år för år utifrån bland annat organisationens mognad och den risk som kan tänkas förekomma. I årets granskning har dataskyddsombudet under Q3-Q4 granskat styrande dokument. Det som har kontrolleras är hur den personuppgiftsansvarige uppfyller ansvarsskyldigheten i artikel 5.2.

Dataskyddsombudet har också följt upp handlingsplaner och åtgärder som personuppgiftsansvarig vidtagit enligt tidigare rekommendationer som getts i samband med granskningarna de senaste två åren:

- Registerförteckning (2023)
- Personuppgiftsbiträdesavtal och uppföljning av leverantörer (2022)
- Motivering av rättsliga grunder (2022)

1.3 Avgränsning

Ingen avgränsning är gjord.

1.4 Metod

Ett antal frågor har skickats ut till den personuppgiftsansvariges dataskyddssamordnare som besvarats skriftligt. Svaret/yttrandet från dåvarande dataskyddssamordnaren är knapphändigt och det har därför varit svårt att fullt ut genomföra en granskning.

1.5 Efterlevnad

Uppfyller dataskyddsförordningens krav, mindre brister med låg risk kan förekomma

Uppfyller delvis dataskyddsförordningen krav, brister finns

Uppfyller till stora delar inte dataskyddsförordningens krav, stora brister finns

2. Granskning

2.1 Del 1: Styrande dokument

2.1.1 Utgångspunkt

Enligt dataskyddsförordningen ska den personuppgiftsansvarige ansvara för och kunna visa att förordningens sex principer efterlevs.[1] Detta kallas principen om *ansvarsskyldighet.*

Med beaktande av behandlingens art, omfattning, sammanhang och ändamål samt riskerna, av varierande sannolikhetsgrad och allvar, för fysiska personers rättigheter och friheter ska den personuppgiftsansvarige genomföra lämpliga tekniska och organisatoriska åtgärder för att säkerställa och kunna visa att behandlingen utförs i enlighet med dataskyddsförordningen. Dessa åtgärder ska ses över och uppdateras vid behov. Om det står i proportion till behandlingen, ska åtgärderna omfatta den personuppgiftsansvariges genomförande av lämpliga strategier för dataskydd[2].

En del av ansvarsskyldigheten innebär således att organisationen ska ha styrande dokument som beskriver hur dataskyddsarbetet ska bedrivas i verksamheten. Styrande dokument är ett viktigt verktyg för ledning och styrning och anger vad verksamheten ska göra, vem som ska göra det och i vissa fall hur det ska göras.

Denna granskningsdel har som syfte att kontrollera hur den personuppgiftsansvarige uppfyller ansvarsskyldigheten i artikel 5.2.

Granskningsunderlag:

Utbildningsnämndens yttrande över dataskyddsombudets granskning av styrande dokument 24UN105-5 (även UG:s del av intranätet har utgjort underlag)

2.1.2 Efterlevnad

Uppfyller till stora delar inte dataskyddsförordningens krav, stora brister finns

Dataskyddspolicy eller motsvarande
Skäl 78

För att den personuppgiftsansvarige ska kunna visa att och hur dataskyddsförordningen efterlevs bör den personuppgiftsansvarige anta interna

[1] artikel 5.2 Allmän dataskyddsförordning
[2] skäl 78 Allmän dataskyddsförordning

strategier och vidta åtgärder därav, exempelvis genom dataskyddspolicy, riktlinjer och andra rutiner. I sammanhanget ska nämnas att dataskydd ofta beskrivs som en juridisk mekanism som säkerställer integritet. I praktiken spelar det ingen större roll om dokumenten är namngivna med integritet eller dataskydd, det viktigaste är innehållet. Dataskyddsombudet har i fortsättningen av denna granskning valt att använda benämningen dataskyddspolicy, men det är innehållet som granskats, oaktat den personuppgiftsansvariges benämning av motsvarande dokument.

Den personuppgiftsansvarige har en informationstext på sin publika webbplats om hur de behandlar personuppgifter inom nämnden Så här behandlar Utbildningsnämnden dina personuppgifter – Gävle kommun Dataskyddsombudet anser att informationen är mer av karaktären ”information till de registrerade” än interna strategier för dataskydd.

Det finns en centralt framtagen policy för informationssäkerhet och där ingår i begränsad utsträckning dataskydd: ”Informationssäkerhetspolicy – Gävle 2020”[3]. Den har inte bifogats i svaret på granskningen, men det finns en generell hänvisning till centrala styrdokument för kommunen i svaret. Att den inte nämns i det ursprungliga svaret skulle kunna indikera att de personuppgiftsansvariga inte känt till dokumentet och att kunskapen om det är låg i organisationen. Av policyn framgår att ” Respektive sektorchef eller bolags VD ska analysera behovet av och ta fram, egna rutiner/instruktioner för underliggande verksamheter till stöd för denna policy”. Utbildningsnämnden har inte, som dataskyddsombudet förstår det fattat något beslut om att anta ovan nämnda policy som sin egen och som dataskyddsombudet förstått den muntliga kontakten med dåvarande dataskyddssamordnare avvaktar man en uppdatering och om det eventuellt tillkommer fler kommunövergripande styrdokument avseende dataskydd innan man tar beslut för nämndens räkning. Dataskyddsombudet rekommenderar att den personuppgiftsansvarige på något sätt gör det tydligt att policyn är en del av dennes ansvarsskyldighet enligt dataskyddförordningen och också tydliggör för verksamheten att så är fallet.

Rutiner för att hantera begäran om de registrerades rättigheter
Artikel 15-18, 20-22

Den registrerade, det vill säga den vars personuppgifter behandlas, har ett antal rättigheter enligt dataskyddsförordningen. Den personuppgiftsansvarige har ett ansvar att ha rutiner på plats för att hantera begäranden om att utöva dessa rättigheter när någon begär det. En sådan begäran ska hanteras så snabbt som möjligt, dock som huvudregel senast en månad efter att den inkom.

Av svaret framkommer det inte att den personuppgiftsansvarige har något styrdokument avseende registrerades rättigheter. Dataskyddsombudet kan inte heller hitta någon information om de registrerades rättigheter på Utbildning Gävles del av intranätet. Som dataskyddsombudet bedömer det saknas styrdokument för de registrerades rättigheter, den personuppgiftsansvarige rekommenderas därför att upprätta, besluta och implementera ett (eller flera) sådant styrdokument.

[3] Policy för informationssäkerhet Gävle kommun. Beslutad version 2020-09-28.pdf

Tekniska och organisatoriska säkerhetsåtgärder
Artikel 24 och 27

Personuppgiftsansvariga måste vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till den risk som behandlingen av personuppgifter utgör för fysiska personers rättigheter och friheter, särskilt när det gäller rätten till skydd av personuppgifter.

Tekniska åtgärder är sådana som ger data- eller systemsäkerhet, kommunikationssäkerhet eller fysisk säkerhet medan organisatoriska åtgärder omfattar sådant som styrdokument, processer, rutiner, metoder, analyser och utbildning. Utformningen av tekniska åtgärder förutsätter ofta organisatoriska åtgärder för att åtgärden ska ge det skydd som behövs. Många åtgärder innehåller därför både tekniska och organisatoriska delar. När det gäller till exempel säkerhetskopior behövs rutiner och ställningstaganden kring hur kopiorna ska sparas, hur ofta de ska tas och hur länge de ska sparas, med mera. Ett annat exempel, behörighetsstyrning, kräver både tekniska funktioner för att kunna begränsa åtkomst liksom analyser av vem som behöver åtkomst till vilka uppgifter och när samt rutiner för hantering av behörigheterna. Särskilt viktiga områden att belysa är hantering av skyddad identitet, behörighetsstyrning och hantering av verksamhetskritiska system.

Såsom dataskyddsombudet förstår svaret finns inget övergripande styrdokument för tekniska och organisatoriska skyddsåtgärder hos den personuppgiftsansvarige, det är inte ett krav enligt dataskyddsförordningen men kan underlätta för att få en helhetsbild. Det finns inom Utbildning Gävle en riktlinje för hur barn och elever med skyddade personuppgifter ska hanteras, den har inte bifogats svaret men finns publicerad på intranätet[4]. Riktlinjen bedömer dataskyddsombudet att den mycket väl uppfyller kraven i dataskyddsförordningen, dock har den inte reviderats sedan 2022. Enligt vad som står i riktlinjen ska den revideras årligen vilket gör ansvarsskyldigheten tydlig. Det finns enligt svaret på granskningen inte något övergripande styrdokument för verksamhetskritiska system. Det upprättas administrativa regler/rutiner tillsammans med systemförvaltaren när nya system tas i bruk. För äldre system som redan är i bruk tas rutiner fram i samband med konsekvensbedömningar. Värt att notera är att det av svaret framgår att dessa oftast inte är skriftliga varför dataskyddsombudet rekommenderar att skriftliga rutiner upprättas och beslutas på lämplig nivå. Den personuppgiftsansvarige saknar övergripande styrdokument för behörighetsstyrning, ansvaret följer som regel linjeorganisationen där ansvarig chef fattar beslut om tilldelning av behörigheter. Dataskyddsombudet rekommenderar att ett övergripande styrdokument för behörighetsstyrning tas fram samt att man överväger om vissa system/tjänster kräver egna rutiner.

Inbyggt dataskydd och dataskydd som standard
Artikel 25

För att kunna visa att dataskyddsförordningen följs bör den personuppgiftsansvarige anta interna strategier och vidta åtgärder, särskilt för att uppfylla principerna om inbyggt dataskydd och dataskydd som standard.[5] Inbyggt dataskydd (privacy by design) innebär att den personuppgiftsansvariga tar hänsyn till integritetsskyddsreglerna redan när IT-system och rutiner utformas, exempelvis användning av pseudonymisering det

[4] Riktlinjer för hantering av barn och elever med skyddade personuppgifter
[5] skäl 78 Allmän dataskyddsförordning

vill säga att ersätta personligt identifierbart material med artificiell identifiering eller hantering av fritextfält. Dataskydd som standard innebär att inställningarna för en produkt, ett system eller en tjänst ska vara dataskyddsvänliga, exempelvis ska inte opt-ins användas.

Den personuppgiftsansvarige saknar, enligt svaret på granskningen, övergripande styrdokument för inbyggt dataskydd/dataskydd som standard. Det finns tex. inte ett övergripande styrdokument för fritextfält utan det hanteras i samband med konsekvensbedömning av respektive system. Dataskyddsombudet rekommenderar dels att den personuppgiftsansvarige upprättar som minst ett styrdokument med information om att principerna om inbyggt dataskydd och dataskydd som standard ska beaktas för tekniska system där personuppgifter behandlas dels att ett övergripande styrdokument för fritextfält tas fram och beslutas.

Personuppgiftsbiträden
Artikel 28

Det är vanligt att personuppgiftsansvariga anlitar personuppgiftsbiträden för att utföra en viss personuppgiftsbehandling. Även om den faktiska behandlingen överlåts kan aldrig själva personuppgiftsansvaret överlåtas. Den personuppgiftsansvarige måste således säkerställa att behandlingen sker i enlighet med dataskyddsförordningen, oavsett om denne utför behandlingen själv eller genom ett personuppgiftsbiträde. Ansvarsskyldighetsprincipen återspeglas bland annat i artikel 28 som fastställer den personuppgiftsansvariges skyldigheter när denne anlitar ett personuppgiftsbiträde.

Huvudregeln är att det är den personuppgiftsansvarige som är skadeståndsansvarig för skada som uppstår till följd av att personuppgifter har behandlats i strid med förordningen. Ett personuppgiftsbiträde kan dock bli ansvarigt för överträdelser av dataskyddsförordningen som är en följd av att biträdet inte har efterlevt den personuppgiftsansvariges instruktioner eller om biträdet har brutit mot de bestämmelser i förordningen som specifikt riktar sig till biträden. Eftersom den personuppgiftsansvarige måste säkerställa att personuppgiftsbehandlingarna som denne är ansvarig för sker i enlighet med dataskyddsförordningen, även om den faktiska behandlingen utförs av ett biträde, krävs det att denne har vetskap om hur biträdet behandlar och skyddar personuppgifterna. Ett första steg är att upprätta ett personuppgiftsbiträdesavtal eller annan rättsakt för att reglera förhållandet sinsemellan samt instruera personuppgiftsbiträdet. Nästa steg är att följa upp så att biträdet behandlar personuppgifterna i enlighet med de instruktioner som den personuppgiftsansvarige givit. Uppföljning av biträden bör göras löpande, men kan dock ske med olika intervall och olika omfattning beroende på hur riskfylld respektive behandling är. Rutiner för hantering av biträdessituationer bör finnas på plats hos verksamheten.

Den personuppgiftsansvarige saknar enligt svaret på granskningen styrdokument för biträdessituationer, såsom det förstås för såväl tecknande av PUB-avtal och uppföljning av dem. Dataskyddsombudet rekommenderar att Utbildning Gävle så snart som möjligt upprättar, beslutar och implementerar ett styrdokument för detta.

Registerförteckning
Artikel 30

Personuppgiftsansvariga och personuppgiftsbiträden är skyldiga att föra ett register över sina behandlingar av personuppgifter. Register över personuppgiftsbehandlingar ska upprättas skriftligen, vara tillgängliga i elektroniskt format och hållas uppdaterade. På begäran ska registret göras tillgängligt för IMY. Vad som ska finnas med i registret beskrivs i artikel 30. För att hålla behandlingarna uppdaterade och på så sätt säkerställa efterlevnad av dataskyddsförordningen bör den personuppgiftsansvariga ha rutiner för upprätthållandet av registerförteckning.

Eftersom den personuppgiftsansvarige fortfarande inte har någon registerförteckning (vilket i sig är allvarligt drygt sju år efter att dataskyddsförordningen trädde i kraft) så finns det inte heller någon rutin för att hålla registerförteckningen uppdaterad. Dataskyddsombudet rekommenderar i första hand att man tar fram en plan för att påbörja arbetet med att upprätta en registerförteckning och i andra hand ta fram en rutin för att hålla den uppdaterad (se även nedan under uppföljning föregående granskningar).

Incidenthantering
Artikel 33-34

Vid en personuppgiftsincident ska den personuppgiftsansvarige utan onödigt dröjsmål anmäla personuppgiftsincidenten till IMY inom 72 timmar såvida det inte är osannolikt att personuppgiftsincidenten medför en risk för fysiska personers rättigheter och friheter. Om personuppgiftsincidenten sannolikt leder till en hög risk för fysiska personers rättigheter och friheter ska den personuppgiftsansvarige utan onödigt dröjsmål informera den registrerade om personuppgiftsincidenten. Den personuppgiftsansvarige är skyldig att dokumentera alla personuppgiftsincidenter oavsett om de är av sådan grad att de ska anmälas till IMY eller inte. Dokumentationskravet inbegriper omständigheterna kring incidenten, dess effekter och de korrigerande åtgärder som vidtagits. Dokumentationsskyldigheten hänger ihop med principen om ansvarsskyldighet vad gäller att den personuppgiftsansvarige ska ansvara för och kunna visa att de grundläggande principerna i dataskyddsförordningen efterlevs. För att kunna uppfylla skyldigheterna enligt förordningen är det viktigt att ha tillräckliga rutiner på plats för att kunna upptäcka, rapportera och utreda personuppgiftsincidenter.

Det har inte bifogats någon rutin för hantering av personuppgiftsincidenter i svaret på granskningen. På Utbildning Gävles del av intranätet (Ankaret) finns, vad dataskyddsombudet bedömer vara en informationstext till de anställda hur de ska göra om det upptäcker en personuppgiftsincident, det har inte karaktären av styrdokument. Dataskyddsombudet rekommenderar att ett styrdokument för att hantera personuppgiftsincidenter tas fram och implementeras i verksamheten.

Högriskbehandlingar
Artikel 35-36

Om en typ av behandling, särskilt med användning av ny teknik och med beaktande av dess art, omfattning, sammanhang och ändamål, sannolikt leder till en hög risk för fysiska personers rättigheter och friheter ska den personuppgiftsansvarige före behandlingen utföra en bedömning av den planerade behandlingens konsekvenser för skyddet av personuppgifter. Den personuppgiftsansvarige ska vidare samråda med

IMY före behandling om en konsekvensbedömning visar att behandlingen skulle leda till en hög risk om inte den personuppgiftsansvarige vidtar åtgärder för att minska risken. För att säkerställa arbetsgången vid en sådan riskbedömning bör den personuppgiftsansvarige ha rutiner gällande konsekvensbedömning och eventuellt förhandssamråd.

Såvitt dataskyddsombudet känner till finns det inga styrande dokument som reglerar hantering av högriskbehandlingar. Av svaret framgår att konsekvensbedömningar görs men när och i vilken omfattning framgår inte. Dataskyddsombudet rekommenderar därför den personuppgiftsansvarige att upprätta rutin som reglerar hantering av högriskbehandlingar. Dataskyddsombudet anser att det åtminstone bör finnas en generell skrivning kring när en konsekvensbedömning ska göras och att dataskyddsombudet ska involveras och rådfrågas vid behandlingar som kan medföra allvarliga risker för de registrerades rättigheter.

Dataskyddsorganisation
Artikel 37-39

Den personuppgiftsansvarige ska under alla omständigheter utnämna ett dataskyddsombud bland annat om behandlingen genomförs av en myndighet eller ett offentligt organ. Den personuppgiftsansvarige har en skyldighet att tillhandahålla de resurser som krävs för att dataskyddsombudet ska kunna fullgöra sina arbetsuppgifter enligt förordningen. Det innebär att den personuppgiftsansvarige måste ha en dataskyddsorganisation inom sin verksamhet för att organisatoriskt skapa ett effektivt dataskyddsarbete enligt förordningens krav. Den personuppgiftsansvarige bör således ha en rutin eller annan beskrivning för att tydliggöra dataskyddsorganisationens roller och ansvar.

Enligt svaret på granskningen finns ett utkast till dataskyddsorganisation framtaget men man har medvetet valt att avvakta med att fatta beslut om dataskyddsorganisation till dess det finns övergripande riktlinjer från kommunstyrelsen. Detta för att undvika att behöva göra om arbetet. Med tanke på att den DSS som tagit fram svaret och som varit den som jobbat länge med dataskyddsfrågor slutat, bedömer dataskyddsombudet det som angeläget att det beslutas om en dataskyddsorganisation. Det kan finnas en risk dels för att det blir ett vacuum dels att man på sikt bygger upp ett nytt personberoende av en person.

Övriga relevanta styrande dokument

För att den personuppgiftsansvarige ska kunna visa att och hur dataskyddsförordningen efterlevs kan andra styrande dokument än ovanstående vara nödvändiga. Ett sådant exempel kan vara i de fall det förekommer kamerabevakning.

Den personuppgiftsansvarige bedriver enligt svaret på föregående granskning inte någon egen kamerabevakning (det är Gavlefastigheter i egenskap av fastighetsägare som har kameror uppsatta på skolor och förskolor).

Av svaret framgår att Utbildning Gävle har egna rutiner för hantering av sociala medier (utöver de som finns framtagna centralt). Rutinen har inte bifogats svaret och dataskyddsombudet kan inte heller hitta den på intranätet varför innehållet inte kan granskas. Dataskyddsombudet är positiv till att en sådan rutin finns inte minst med tanke på att det främst är barn, som räknas som en utsatt grupp enligt

dataskyddsförordningen, som är de som utgör de registrerade hos den personuppgiftsansvarige.

Beslut, översyn och kommunikation

För att effektivt arbeta med styrande dokument som ett verktyg för ledning och styrning rekommenderas att löpande göra översyn av dokumenten. Genom att kontinuerligt revidera och fastställa säkerställs regelefterlevnaden och dataskyddet inkluderas systematiskt. Det rekommenderas också att ha utpekad ägare som ansvarar för att dokumenten uppdateras. Det behöver inte vara samma roll som faktiskt uppdaterar dokumentet men en roll med ansvar att revidering görs med återkommande intervall. En tydlig kommunikationsplan för styrande dokument är också viktigt för att upprätthålla informationen hos berörda medarbetare.

Av svaret på granskningen framkommer dels att det finns brister när det gäller att ta fram skriftliga rutiner dels att regelbundet uppdatera de styrdokument som finns skriftligt när det gäller dataskyddet. Dataskyddsombudet rekommenderar därför att skriftliga styrdokument tas fram och regelbundet uppdateras.

Rekommendation
Dataskyddsombudet rekommenderar den personuppgiftsansvarige att:

1. anta kommunövergripande policy för informationssäkerhet alternativt på annat sätt tydligt visa att policyn tillämpas inom nämnden

2. upprätta, besluta (på rätt nivå) och implementera styrdokument avseende registrerades rättigheter

3. ta fram ett övergripande styrdokument för behörighetsstyrning och utreda om det behövs specifika för vissa system/tjänster

4. den personuppgiftsansvarige upprättar dels en rutin med information om att principerna om inbyggt dataskydd och dataskydd som standard ska beaktas för tekniska system där personuppgifter behandlas dels att ett övergripande styrdokument för fritextfält tas fram och beslutas

5. upprätta styrdokument för hantering av personuppgiftsbiträden såväl avtalstecknande som uppföljning.

6. påbörja arbetet med att ta fram en registerförteckning, det är av mycket stor vikt att det arbetet påbörjas omgående. Därefter ta fram en rutin för regelbunden översyn av förteckningen.

7. upprätta rutin som reglerar hantering av högriskbehandlingar där det som minst finns en generell skrivning kring när en konsekvensbedömning ska göras och att dataskyddsombudet ska involveras och rådfrågas vid behandlingar som kan medföra allvarliga risker för de registrerades rättigheter

8. upprätta styrande dokument som beskriver dataskyddsorganisationens roller och ansvar.

9. genomföra en kartläggning och sammanställning över de styrande dokument som i dagsläget finns och berör dataskydd samt ta fram en åtgärdsplan för de som inte finns men som bör finnas enligt dataskyddsförordningen.

2.2 Del 2: Uppföljning av föregående års granskningar

Dataskyddsombudet har vid tidigare års granskningar funnit brister inom vissa områden i dataskyddsarbetet hos personuppgiftsansvarig. Dataskyddsombudet har i denna granskningsdel följt upp handlingsplaner och åtgärder som personuppgiftsansvarig vidtagit enligt tidigare rekommendationer. Enligt svaret på granskning pågår alltjämt arbetet med den processkartläggning som ska ligga till grund för registerförteckningen, samma svar som givits i många år. Dataskyddsombudet är positiv till ansatsen att göra en processkartläggning men ser mycket allvarligt på att det i dag 7 år efter att dataskyddsförordningen trädde i kraft fortfarande inte finns någon registerförteckning. Det är en handling som på begäran ska kunna lämnas ut till IMY och den är också en allmän handling. Dataskyddsombudet rekommenderar att arbetet med registerförteckningen för hög prioritet. När det gäller information till de registrerade har en kartläggning gjorts av vilka e-tjänster och blanketter som behöver uppdateras, arbetet med att ändra informationen är inte avslutat. Som nämnts ovan saknas styrdokument för tecknande och uppföljning av PUB-avtal.

3. Slutsats

Dataskyddsombudet har i sin granskning av styrande dokument funnit stora brister i delar av den personuppgiftsansvariges dataskyddsarbete. Arbetet med dataskydd, är precis som övrigt kvalitetsarbete en löpande process som ständigt pågår och som aldrig är något som blir färdig. Samhällsutvecklingen går allt snabbare och de förändringar som sker i omvärlden ställer nya krav när det kommer till dataskyddsarbetet i stort. Styrande dokument är ett viktigt verktyg för ledning och styrning och anger vad verksamheten ska göra, vem som ska göra det och i vissa fall hur det ska göras. Rutinbeskrivningar är också betydelsefulla för att säkerställa att dataskyddsförordningens regler följs, inte minst för att reducera personberoenden.

Dataskyddsombudet rekommenderar därför den personuppgiftsansvarige att prioritera och aktivt arbeta med frågor kopplade till dataskydd för att hantera de brister som konstaterats och för att fortsätta arbeta med att skapa en god dataskyddskultur.