IT SÄKERHETSBOLAGET

Utlåtande

2021-01-12

Rättsligt utlåtande om direktåtkomst för revisorer i kommunens diariesystem

Bakgrund

Kommunens revisorer är en självständig myndighet i den kommunala organisationen.[1] Revisorernas verksamhet regleras i 12 kap. Kommunallagen (”KL”). Där klargörs revisorernas självständiga ställning och vad de ska granska. Revisorerna ska självständigt välja vad som ska granskas och välja angreppssätt för granskningens genomförande.[2] För att kunna fullgöra sitt uppdrag enligt lagkraven har revisorerna rätt till information, 12 kap. 9 § KL.

Gävle kommuns revisorer har genom indragen direktåtkomst i systemet Platina fått inskränkta möjligheter till insyn i den verksamhet de ska granska. Kommunledningskontorets beslut har primärt motiverats med olika dataskyddsrättsliga principer, såsom proportionalitet och nödvändighet. Av de yttranden som gjorts har även paralleller dragits till offentlighetsprincipen med tillhörande praxis.

IT-säkerhetsbolaget kommer i detta rättsutlåtande att reda ut begreppen och belysa att:

- Kommunrevisionen inte har någon oinskränkt, lagstadgad rätt till direktåtkomst i Platina, men trots detta gäller att:
- Revisorerna mycket väl kan ha ett behov av behörighet i systemet, och att
- Kommunledningskontoret eller annan förvaltningsorganisation i kommunen på grund av revisorernas självständiga ställning och självständiga personuppgiftsansvar inte har någon rätt att besluta om vilken personuppgiftsbehandling som är eller kan vara nödvändig i revisorernas verksamhet.

Vi kommer också i utlåtandet att lyfta fram de dataskyddsbestämmelser som reglerar ansvarsförhållandet mellan de kommunala nämnderna och kommunens revisorer och ge några exempel på hur nämnderna (som beslutar om behörigheter i sina system) kan förfara för att minimera risken för sanktioner enligt dataskyddsförordningen (”DSF”) när de ger revisorerna den åtkomst som behövs för granskningen.

Förhoppningsvis kan utlåtandet stödja kommunrevisionen i att omformulera sin begäran och att rikta den till rätt instans, så att den behörighet som behövs för granskningsändamålen kan tilldelas.

---

[1] I vilken mån revisorerna samlat utgör en gemensam myndighet eller om respektive revisor är att betrakta som enskilda myndigheter var för sig kan variera beroende på hur det enskilda granskningsuppdraget rent faktiskt utförs och/eller beroende på hur fullmäktige har reglerat revisorernas förvaltning.
[2] SKR om Oberoende i praktiken (2021-01-07): https://skr.se/demokratiledningstyrning/revision/attvarafortroendevaldrevisor/revisorernasoberoende.26444.html

IT-Säkerhetsbolaget AB
Storgatan 73
852 30 SUNDSVALL

Telefon:
0709 - 249 250
070 - 330 11 89

E-mail:
info@itsakerhetsbolaget.se

Webb:
www.itsakerhetsbolaget.se

Orgnr:
556915-8990

IT SÄKERHETSBOLAGET

Utlåtande

2021-01-11

Informationsskyldighet

Det är de kommunala nämnderna, fullmäktigeberedningarna, de enskilda ledamöterna (och dess ersättare) och kommunens anställda som har skyldighet att lämna revisorerna de upplysningar som behövs för revisionsarbetet, 12 kap. 9 § KL. Av revisorernas självständiga ställning följer att det är revisorerna själva som avgör vilken information som behövs.[3]

Revisorernas rätt till information ska inte sammanblandas med rätten att ta del av allmänna handlingar enligt Tryckfrihetsförordningens andra kapitel. Trots att den allmängiltiga handlingsoffentligheten även gäller revisorerna,[4] och de övergripande och grundlagsfästa ändamålen med både handlingsoffentlighet och revisorernas granskning är desamma,[5] så har de två rättigheterna olika funktion och utövas från olika nivåer i samhället. Kommunallagens särreglering om informationsskyldighet skulle inte behövas om tryckfrihetsförordningens bestämmelser hade ansetts tillräckliga för att tillgodose revisorernas behov av information. De två rättigheterna (eller *skyldigheterna* för kommunens nämnder, ledamöter och personal) skiljer sig åt på så vis att revisorernas rätt till information är mer långtgående än allmänhetens rätt till allmänna handlingar.

För det första kan rätten att ta del av allmänna handlingar begränsas enligt Offentlighets- och sekretesslagen (”OSL”). Revisorerna omfattas av tillämpliga bestämmelser om överföring av sekretess, vilket innebär att sekretessbelagda handlingar, som annars inte kunnat lämnas ut med stöd av handlingsoffentligheten, som huvudregel inte kan nekas revisorerna med hänvisning till OSL.

För det andra ska inte revisorerna, annat än undantagsvis, granska *ärenden*.[6] De flesta handlingar som registreras i ett diarium är hänförliga till ett visst ärende, men revisorerna kan även granska handlingar som inte diarieförts, exempelvis på grund av att ett ärende ännu inte avslutats eller att en handling inte diarieförts till följd av bristfälliga handläggningsrutiner.[7]

För det tredje framgår det direkt av 12 kap. 9 § st. 2 KL att nämnderna (och övriga upplysningsskyldiga) ska ge revisorerna tillfälle att när som helst *inventera de tillgångar* som nämnderna har hand om. I dagsläget utgör en organisations informationsmängd en av dess mest värdefulla tillgångar.[8]

Sammanfattningsvis sträcker sig revisorernas rätt till information längre än till att enbart omfatta det som kan lämnas ut med stöd av offentlighetsprincipen. Av detta följer att inte heller praxis ifråga om rätten att ta del av allmänna handlingar är relevant när det kommer till revisorernas rätt till insyn.[9]

---

[3] 12 kap. 7 § KL.
[4] Revisorerna har antingen samlat, som juridisk person, rätt till allmänna handlingar (RÅ2003 ref. 83) eller enskilt, i egenskap av ”envar” eller ”var och en”, 2 kap. 1 § TF.
[5] Rättssäkerhet och effektivitet i förvaltningen och folkstyret, se bl.a. prop. 1975/76:160 s. 70.
[6] 12:3 KL.
[7] Handlingar som inte upprättats kan blir allmänna först när ett ärende slutbehandlats, 2 kap. 10 § TF. Vidare får revisorerna göra en allmän granskning för att kontrollera handläggningsrutiner, standardfrågor etc, prop. 1990/91:117 s. 126.
[8] ”Informationstillgångar”.
[9] Exempelvis är jämförelser med regeringsrättens dom ifråga om rätt till upptagningar från databas/tillgången till arkiv inte tjänliga i sammanhanget (RÅ 1980 2:42).

Revisorer, personuppgiftsansvar och dataskyddsombud

Revisorerna bär personuppgiftsansvar för den personuppgiftsbehandling som görs i revisonens verksamhet. Det följer av att revisorerna är en egen myndighet. Att en myndighet är personuppgiftsansvarig kan utläsas bland annat i art. 37.1a DSF där det stadgas att en myndighet under alla omständigheter har skyldighet att utnämna dataskyddsombud.

Dataskyddsombudets roll är att granska efterlevnaden av dataskyddsförordningen inom den personuppgiftsansvariga organisationen, primärt med avseende på den personuppgiftsansvariges strategi för skydd för personuppgifter, inbegripet ansvarstilldelning och ”tillhörande granskning”.[10] Dataskyddsombudet ska alltså granska hur kommunen granskar sin egen verksamhet på dataskyddsområdet. Av detta kan utläsas att kommunen själv har ett ansvar för att granska hur väl den egna verksamheten lever upp till dataskyddsbestämmelserna, vilket kan göras genom internrevision, externrevision eller på annat vis.

En kommunrevision som utnämnt dataskyddsombud ska, liksom kommunens övriga nämnder, underkasta sig dataskyddsombudets granskning, men samtidigt iaktta att det inte finns något hinder emot att revisorerna själva granskar efterlevnaden av dataskyddsbestämmelserna.

För att granskning på dataskyddområdet ska kunna realiseras i praktiken finns vissa bestämmelser om dataskyddsombudets ställning. Bland annat har även dataskyddsombudet en rätt till upplysningar, som uttryckts genom rätt till ”tillgång till personuppgifter och behandlingsförfaranden”.[11] Ett dataskyddsombud som exempelvis anser sig behöva behörighet i ett system i syfte att granska någon dataskyddsjuridisk aspekt ifråga om en pågående behandling skulle med tanke på nämnda bestämmelse inte kunna nekas sådan.

Laglig grund och de övriga dataskyddsprinciperna

Det är med stöd av kommunallagens bestämmelser som revisorerna har en laglig grund för den personuppgiftsbehandling som görs i revisorernas verksamhet.[12] Den lagliga grunden är knuten till det ändamål som behandlingen syftar till, vilket närmare kommer att beskrivas i nästa avsnitt. Kraven på att ha en laglig grund och ett på förhand definierat ändamål för en behandling utgör centrala inslag i dataskyddsbestämmelserna. De grundläggande dataskyddsprinciperna utgörs av:[13]

- Laglighet, korrekthet och öppenhet
- Ändamålsbegränsning (och finalitet)
- Uppgiftsminimering
- Korrekthet
- Lagringsminimering
- Integritet och konfidentialitet
- Ansvarsskyldighet.

En behandling som genomförs utan att samtliga av de ovanstående principerna iakttas är per definition olaglig. Av den sista principen, ansvarsskyldigheten, följer att den personuppgiftsansvarige ska kunna (be-) visa att övriga principer efterlevs, av vilket det följer ett dokumentationsansvar.

[10] Art. 39 DSF.
[11] Art. 38.2 DSF.
[12] En laglig grund krävs för varje personuppgiftsbehandling som görs av en personuppgiftsansvarig, art. 6 DSF.
[13] Art. 5 DSF.

Ändamålens koppling till den lagliga grunden

Revisorernas ändamål med personuppgiftsbehandling kan på ett övergripande plan beskrivas som ”att granska den kommunala verksamheten”.[14] Detta ändamål skiljer sig från en nämnds ändamål med behandling av samma personuppgifter, vilket kan illustreras såhär:

Personuppgiftsbehandling	**Ändamål för en nämnd**	**Ändamål för revisorer**[15]
Namn, adress, personnummer på sökande av bygglov	Handlägga begäran om bygglov	Granska om bygglovsärenden hanterats i tid efter synpunkter från allmänheten
Namn, e-post och organisation i HR-system	Betala ut löner	Granska att rätt löner betalats ut under en viss period
Namn, adress, målsman, personnummer m.m. i skolsystem	Administrera ärenden enligt skollagen	Granska om GDPR efterlevs i skolan

Vilka ändamål en personuppgiftsansvarig organisation har med sin behandling ska förtecknas i ett register (en så kallad ”Registerförteckning”).[16] Som framgår av tabellen kan en behandling av samma uppgifter (i samma system), men som utförs av två olika myndigheter utgöra helt olika ”behandlingar”. De båda personuppgiftsansvariga organisationerna måste därför ta upp behandlingen i sin respektive förteckning.[17]

Precis som att ändamålen med en behandling kan skiljas åt så behöver inte heller den lagliga grund som respektive myndighet stödjer sin behandling på vara densamma:

Personuppgiftsbehandling	**Ändamål för en nämnd**	**Ändamål för revisorer**[18]
Namn, adress, personnummer på sökande av bygglov	Handlägga begäran om bygglov	Granska om bygglovsärenden hanterats i tid efter synpunkter från allmänheten
Laglig grund (exempel):	*Myndighetsutövning (6.1e DSF)*	*Allmänt intresse (6.1e DSF)*
Namn, e-post och organisation i HR-system	Betala ut löner	Granska att rätt löner betalats ut under en viss period
Laglig grund (exempel):	*Avtal (6.1b DSF)*	*Allmänt intresse (6.1e DSF)*
Namn, adress, målsman, personnummer m.m. i skolsystem	Administrera ärenden enligt skollagen	Granska om GDPR efterlevs i skolan
Laglig grund (exempel):	*Rättslig förpliktelse (6.1c DSF)*	*Allmänt intresse (6.1e DSF)*

Det har nu tydliggjorts att det inte är ovanligt att personuppgiftsbehandlingar, av samma personuppgifter, som utförs av olika nämnder i samma kommun rent faktiskt utgör olika ”behandlingar”.[19]

---

[14] Vid sidan av behandling för det övergripande ändamålet utför revisorerna personuppgiftbehandlingar exempelvis i mötesadministrationssyfte, för att kommunicera med tjänstemän och sakkunniga och för att tillmötesgå offentlighetsprincipen.

[15] Tabellen är hypotetisk.

[16] Art. 30 DSF.

[17] Vissa organisationer väljer att ha en koncerngemensam registerförteckning, vilket är fullt möjligt. Viktigt är då att det tydligt av dokumenterade beslut framgår vem som ansvarar för att löpande föra in och kontrollera de behandlingar som ska tas in i förteckningen för respektive organisations räkning.

[18] Tabellen är hypotetisk.

[19] Med *behandling* avses en åtgärd eller kombination av åtgärder beträffande personuppgifter eller uppsättningar av personuppgifter, oberoende av om de utförs automatiserat eller ej, såsom insamling, registrering, organisering,

Vidarebehandling (ytterligare behandling för nya ändamål)

När revisorerna, som utgör en egen myndighet med uppdrag att granska de andra kommunala nämnderna, får tillgång till personuppgifter ur nämndernas verksamhetssystem så utför de en behandling för andra ändamål än det ändamål för vilket personuppgifterna inledningsvis samlades in. Den upplysningsskyldiga nämnd, som ska ge revisorerna tillgång till informationen, ansvarar inför utlämnandet för att ta ställning till om den ytterligare behandling, som revisorernas granskning medför, är förenlig med de ursprungliga behandlingsändamålen. Detta görs i en så kallad förenlighetsbedömning.

Förenlighetsbedömning med exempel[20]
• **Vilka kopplingar finns mellan ändamålen med den ursprungliga personuppgiftsbehandlingen och revisorernas behandling?**
Exempel: Kopplingen består av att revisorerna enligt lag ska granska den verksamhet som har föranlett personuppgiftsbehandlingen.
• **I vilket sammanhang har uppgifterna samlats in och vilket förhållande har de registrerade till er som personuppgiftsansvarig? Vilken personuppgiftsbehandling kan de registrerade rimligen förvänta sig?**
Exempel: Nämnden informerar redan vid insamlingen av personuppgifterna, i enlighet med enligt art. 13 DSF, att denna typ av ytterligare behandling kommer att ske.
• **Vilken typ av personuppgifter ska behandlas? Är uppgifterna känsliga?**
*Exempel: Alla typer av personuppgifter som ingår i system X. Då känsliga personuppgifter behandlas görs det med stöd av att revisorernas verksamhet utgör ett viktigt allmänt intresse. (**Nödvändighetsbedömning** och **proportionalitetsbedömning** enligt art. 9.2g DSF har genomförts av regering och riksdag i och med införande av 12 kap. 9 § KL).*
• **Vilka konsekvenser kan personuppgiftsbehandlingen få för de registrerade?**
Exempel: Revisorerna är bundna av tystnadsplikt enligt OSL och bestämmelser om god revisionssed. Eftersom revisorerna är medborgarnas demokratiska instrument för granskning och kontroll av den verksamhet som samlat in och behandlar deras personuppgifter torde behandlingen gynna medborgarna ur demokratiskt hänseende.
• **Vilka skyddsåtgärder har ni vidtagit för att skydda uppgifterna, till exempel behörighetsstyrning, kryptering och pseudonymisering?**
Exempel: Revisorerna tilldelas behörighet årsvis i enlighet med granskningsplan och skriftlig begäran. När en revisor lämnar sitt uppdrag dras behörigheten omedelbart in. Behandlingen regleras i revisorernas personuppgiftspolicy. PUB-avtal och sekretessförbindelse med sakkunniga som deltar i behandlingen finns.

Förenlighetsbedömningen kan ta sikte på en generell och vidsträckt behörighet i alla relevanta system, och återspegla revisorernas hela behov under en viss period. Ett sådant tillvägagångssätt bygger på förtroende för att revisorerna, liksom förordningen kräver, har förmåga att leva upp till dataskyddsbestämmelserna på egen hand. Ett annat angreppssätt att besluta om behörighet för revisorerna från fall till fall genom att genomföra en riktad kontroll av lagligheten i den potentiella ytterligare personuppgiftsbehandling som kan aktualiseras. I sådana fall förnyas förenlighetsbedömningen kontinuerligt. Resultatet av förenlighetsbedömningen ska alltid dokumenteras enligt ansvarsprincipen.[21]

Efter förenlighetsbedömningen gör nämnden ett *utlämnande* av personuppgifter genom att öppna systemet för revisorerna. Därefter tar revisorernas personuppgiftsansvar vid. Huruvida behandlingen är nödvändig

strukturering, lagring, bearbetning eller ändring, framtagning, läsning, användning, utlämning genom överföring, art. 4.2 DSF.

[20] Art. 6.4 a-e DSF.

[21] Art. 5.2 DSF.

är det alltså revisorerna själva som måste ta ställning till, initialt när de definierar den rättsliga grund som behandlingen ska utföras med stöd av.

Rollfördelning vid personuppgiftsansvar

Då flera myndigheter gemensamt behandlar personuppgifter inom ramen för samma process eller system kan de i ansvarsfrågan ha någon av följande relationer:

- Självständiga personuppgiftsansvariga (med ett utlämnande),
- Gemensamt personuppgiftsansvariga, eller
- Personuppgiftsansvarig och personuppgiftsbiträde (biträdesrelation)

När en nämnd behandlar personuppgifter för ett visst ändamål och revisorerna å sin sida behandlar (samma) personuppgifter för andra ändamål så föreligger som huvudregel ett självständigt personuppgiftsansvar för de två organisationerna. När nämnden som ansvarar för det system som personuppgifterna behandlas i på förfrågan ger revisorerna tillgång till systemet så är det alltså fråga om ett utlämnande av personuppgifter.[22]

Vilken relation som finns mellan revisorerna och den nämnd som har skyldighet att lämna revisorerna de upplysningar som behövs för revisionsarbetet ska dokumenteras. Detta följer av personuppgiftsansvarets kärna och att den ansvarige ska kunna visa att förordningen efterlevs.[23] Beroende på vilken relation som organisationerna har till varann så följer olika praktiska krav. Om organisationerna istället kommer fram till att det föreligger ett gemensamt personuppgiftsansvar så krävs fastställande av inbördes arrangemang mellan parterna. Är det fråga om en biträdesrelation krävs ett personuppgiftsbiträdesavtal.[24]

Oaktat vilken relation som organisationerna kommer fram till att de har till varann så finns reella möjligheter (och genom 12 kap.9 § vissa lagkrav på) att tillhandahålla revisorerna de personuppgifter som behandlas i nämnderna för andra ändamål. För att effektivisera arbetet i en koncern där flera organisationer delar på olika system är det rimligt att det högsta beslutande organet (fullmäktige) beslutar om gemensamma principer för personuppgiftsansvarets fördelning inom koncernen.[25]

Beslut om ändamål och medel

Om det ändå råder osäkerhet i ansvarsfrågan och det inte är särskilt reglerat i lag (eller förtydligat i fullmäktigebeslut) vem som ansvarar för en viss behandling så ska följande två frågor besvaras:

- Vem beslutar om *ändamålen* med behandlingen?
- Vem beslutar om *medlen* (dvs. tillvägagångssättet) för behandlingen?

Det är nämligen den som beslutat om ändamål och medel med en behandling som ansvarar för den.[26]

Ändamålen med revisorernas behandling framgår implicit av kommunallagen. Så länge inte kommunfullmäktige beslutat annat är det revisorerna själva som ansvarar för den behandling som utförs

[22] Resonemanget bygger på att revisorerna och nämnden gemensamt kommit fram till att det föreligger ett enskilt personuppgiftsansvar organisationerna emellan.
[23] Art. 24 och 6.2 DSF.
[24] Artiklarna 26 och 28 DSF.
[25] Ett sådant beslut skulle även kunna uppfylla kravet på inbördes arrangemang enligt bestämmelserna om gemensamt personuppgiftsansvar, art. 26 DSF.
[26] Art. 4.7 och 26 DSF.

inom ramen för det lagreglerade uppdraget.

Det ligger nära tillhands att också utgå ifrån att revisorerna självständigt beslutar om *medlen* för den behandling som krävs i deras verksamhet. Så är dock inte alltid fallet, vilket illustreras i följande exempel:[27]

> När behandling av personuppgifter utförs inom en kommun är det vanligtvis kommunstyrelsen eller en kommunal nämnd som bär personuppgiftsansvaret. Förutsättningen för att en nämnd ska bära ett personuppgiftsansvar är att den är tillräckligt självständig i förhållande till kommunstyrelsen. Det medför till exempel att en utbildningsnämnd är personuppgiftsansvarig för personuppgiftsbehandling som sker inom en kommunal skola. Socialnämndens personuppgiftsansvar är särskilt reglerat i förordningen (2001:637) om behandling av personuppgifter inom socialtjänsten.
>
> Om kommunstyrelsen eller en annan nämnd tillhandahåller ett gemensamt IT-system som används av flera nämnder inom en kommun kan den tillhandahållande nämnden anses vara personuppgiftsbiträde åt de nämnderna som använder IT-systemet i sin verksamhet. Normalt bör nämnderna på grund av sekretess vara skyldiga att separera den information som de behandlar inom sin verksamhet. Nämnderna kan i sådana fall vara personuppgiftsansvariga var och en för sin behandling i IT-systemet. Bedömningen kan bli en annan om det är ett IT-system som till exempel används för informationsutbyte mellan nämnderna. I dessa fall kan nämnderna anses vara gemensamt personuppgiftsansvariga.

Liksom det redan under föregående avsnitt konstaterats kan det även av exemplet utläsas att revisorerna på grund av sitt självständiga förhållande till styrelsen och övriga nämnder själva bär personuppgiftsansvaret för sin behandling. Om behandlingen som revisorerna gör skulle utföras för samma ändamål som inom den granskade nämnden hade det istället varit fråga om ett gemensamt personuppgiftsansvar.[28] Så är dock inte fallet, vilket även det belysts i tidigare avsnitt. Detta innebär sammanfattningsvis att kommunens nämnder inte ansvarar för revisorernas personuppgiftsbehandling, för den nödvändighetsbedömning som krävs eller för att revisorernas behandling uppfyller proportionalitetsprincipen.[29]

Beslut om tekniska och organisatoriska säkerhetsåtgärder

Först när revisorernas och respektive nämnds relation är fastställd kan det avgöras vilken myndighet som ska besluta om de tekniska och organisatoriska säkerhetsåtgärder som krävs för att skydda de personuppgifter som behandlas,[30] eftersom det är den personuppgiftsansvariga som har att ta ställning till det.

Är det fråga om ett system som en annan nämnd ansvarar för så torde en rimlig princip vara att revisorerna omfattas av samma säkerhetsåtgärder som övriga medarbetare med tillgång till uppgifterna.

---

[27] Exemplet är hämtat ur Svenskt Näringslivs Rapport om rollfördelning av korrekt personuppgiftsansvar av den 8 april 2019.
[28] Se förtydligande bilder på sida 31 i Svenskt Näringslivs Rapport om rollfördelning av korrekt personuppgiftsansvar, i vilken det också finns en checklista för fastställande av ansvar.
[29] Ifråga om den behandling som görs då revisorerna diarieför egna handlingar i Platina skulle dock kommunen kunna anses utgöra ett personuppgiftsbiträde till revisorerna, vilket i så fall ska regleras genom PUB-avtal.
[30] Art. 24-25 DSF.

Liksom Datainspektionen (nu Integritetsskyddsmyndigheten) understryker, utgör en konsekvensbedömning avseende dataskydd en mycket god metod för att komma fram till vilka skyddsåtgärder som måste vidtas, exempelvis i samband med ett utlämnande.[31]

Slutsatser

Revisorerna är själva *personuppgiftsansvariga* för merparten av den behandling som görs i revisorernas verksamhet. Det innebär att exempelvis *nödvändighetsbedömningen* måste utföras av revisorerna själva inför en eventuell personuppgiftsbehandling. Det är också revisorerna som självständigt definierar vilken *rättslig grund* och vilka *ändamål* som möjliggör den personuppgiftsbehandling som aktualiseras i deras verksamhet.

Den behandling som revisorerna utför utgör ofta en *vidarebehandling* av personuppgifter som nämnderna samlat in och ansvarar för. Inför ett utlämnande av sådana uppgifter ska den ansvariga nämnden göra en *förenlighetsbedömning*, men utan att med det ta ställning till vilken behandling som är *nödvändig* för revisorernas granskning. Det bedömer revisorerna själva.

Oavsett om styrelse och nämnder ger *direktåtkomst* eller ej så följer det av revisorernas *självständiga ställning* att de också vet bäst vilken information som behövs utifrån granskningsändamålen. Därvid har den granskade nämnden en skyldighet att tillhandahålla den *information* som krävs i sammanhanget. Om tillhandahållen information innehåller personuppgifter är det sedan upp till revisorerna att utifrån givna tekniska och organisatoriska förutsättningar avgöra om en faktisk behandling av dessa personuppgifter krävs för att uppfylla granskningsändamålen.

Om revisorerna exempelvis skulle besluta att granska hur de olika nämnderna efterlever kravet på registrering av allmänna handlingar skulle en vidsträckt behörighet *behövas* i såväl epostsystem som diarium. Samma princip gäller vid granskning av vilka säkerhetsåtgärder som vidtagits i samband med upphandling av ett nytt system. Huruvida det går att göra inställningar i kommunens system för att inför en granskning begränsa åtkomsten till särskilda *personuppgifter* är sannolikt inget som revisorerna på förhand kan påverka. Det är den som ansvarar för den *primära behandling* som görs i systemet, eller på delegation köper in ett system på uppdrag av andra organisationer eller nämnder, som ska tillämpa principerna om *inbyggt dataskydd och dataskydd som standard*.[32] Att revisorerna behöver göra en *vidarebehandling* för att kunna utföra sitt uppdrag är otvivelaktigt.

Sammanfattningsvis ser inte IT-säkerhetsbolaget att det föreligger något principiellt hinder ur dataskyddsrättslig karaktär för att ge revisorerna direktåtkomst till Platina. Att de i vissa potentiella granskningsuppdrag tvärtemot har ett reellt behov av behörighet i olika system är ett faktum.[33]

Liv Zettergren
Dataskyddsjurist, IT-säkerhetsbolaget

[31] Art. 35 DSF.
[32] Art. 25 DSF.
[33] Se exempel i föregående stycke och i tabellen med laglig grund och olika ändamål.