2019-03-06

Dataskyddsenheten

Styrning och stöd
Filip Henriksen

Kommunrevisionens direktåtkomst till diariet ur ett dataskyddsrättsligt perspektiv

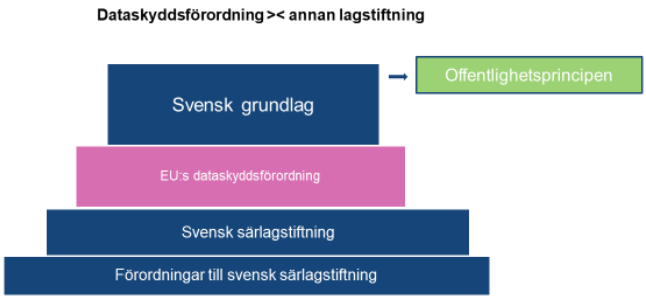
Bakgrund

En utredning pågår om de juridiska förutsättningarna för att ge kommunrevisionen en digital direktåtkomst till kommunkoncernens samtliga diarier, inkluderande samtliga ärenden och handlingar. Dataskyddsenheten har blivit ombedd att lämna ett yttrande i frågan ur ett dataskyddsrättsligt perspektiv.

Laghierarki

Dataskyddsförordningen[i] är en förordning, som gäller lika i alla EU-länder och som tillämpas på sådan behandling av personuppgifter som helt eller delvis företas på automatisk väg samt på annan behandling än automatisk av personuppgifter som ingår i eller kommer att ingå i ett register.[ii]

I hierarkin av lagar och förordningar placerar sig en EU-förordning på följande sätt:



Vid en eventuell lagkollition mellan exempelvis någon av grundlagarna och dataskyddsförordningen, får grundlagarna tolkningsföreträde framför förordningen.

Offentlighetsprincipen, utifrån perspektivet handlingsoffentlighet, bygger på de svenska grundlagarna (tryckfrihetsförordningen). Offentlighetsprincipen ska inte övertolkas som en skyldighet att publicera information ur allmänna handlingar. Dataskyddsförordningen tillämpas därför i sin helhet när en myndighet självmant vill sprida, tillhandahålla eller publicera information utan att någon begärt ut allmänna handlingar. Detsamma gäller om en

myndighet överlämnar uppgifter eller handlingar till en annan myndighet, enligt offentlighets- och sekretesslagen, utan att detta begärts av den annan myndigheten.

Dataskyddsförordningen tillämpas om Gävle kommuns nämnder (personuppgiftsansvariga) väljer att lämna direktåtkomst till sina diarium till kommunrevisionen, som betraktas som en egen, självständig nämnd/myndighet.

Personuppgifter

Alla uppgifter som direkt eller indirekt kan kopplas till en fysisk, levande person, är att betrakta som personuppgifter.[iii]

Ett diarium innehåller normalt ett stort antal personuppgifter.

Behandling av personuppgifter

Dataskyddsförordningen tillämpas på *behandling* av personuppgifter. Definitionen av begreppet ”behandling” är vid och omfattar samtliga delar av en normal livscykel för information, ex. insamling, bearbetning, lagring, läsning, utlämning genom överföring, spridning eller tillhandahållande och radering. [iv]

Om de personuppgiftsansvariga nämnderna väljer att ge direktåtkomst till sina diarium till kommunrevisiorerna som organisatoriskt finns utanför respektive nämnds gränser, betraktas denna behörighetstilldelning som behandling av personuppgifter genom det utlämnande som det innebär.

Grundläggande principer

Dataskyddsförordningen reglerar ett antal viktiga, grundläggande principer som gäller för all personuppgiftsbehandling. Av principerna framgår att en behandling av personuppgifter alltid ska ske *lagligt, korrekt och öppet*. Detta förutsätter bland annat att varje behandling bygger på en rättslig grund i dataskyddsfördordningen. Vidare regleras att personuppgifter inte får behandlas för andra ändamål än för de ändamål som de samlades in för; att man bara får behandla de personuppgifter som är nödvändiga för behandlingen, att uppgifterna ska vara korrekta och att uppgifterna inte får behandlas i identifierbar form längre än nödvändigt för ändamålet som uppgifterna samlades in för. Dessutom ska den som behandlar personuppgifter alltid vidta både organisatoriska och tekniska säkerhetsåtgärder för att skydda uppgifterna som behandlas. I denna grundläggande princip ingår bland annat att användare bara kommer åt de uppgifter som de behöver för att kunna utföra sina arbetsuppgifter, oberoende av om personuppgifterna är harmlösa eller känsliga.

> I en dom i maj 2012 fastställde Förvaltningsrätten i Stockholm Datainspektionens beslut om att länsstyrelsen i Västra Götaland måste begränsa åtkomsten till dokument i det interna diariet (Platina). Datainspektionen hade uttalat att det inte varit förenligt med dåvarande lagstiftning (PuL) att alla handläggare kommer åt alla dokument som inte är sekretessbelagda utan behörigheterna måste styras så att respektive

> användare bara kommer åt de uppgifter de behöver för att kunna utföra sina arbetsuppgifter.[v]

De personuppgiftsansvariga är vidare skyldiga att kunna visa att de grundläggande principerna efterlevs i all behandling av personuppgifter (ansvarsskyldighet).[vi]

Om Gävle kommuns personuppgiftsansvariga nämnder väljer att ge direktåtkomst till sina diarier, inkluderande alla handlingar, till kommunrevisionen, behöver nämnderna tillgodose och kunna visa *att* och *hur* de grundläggande principerna efterlevs.

Rättslig grund

En laglig personuppgiftsbehandling behöver stödja sig på åtminstone en av följande rättsliga grunder:

- Samtycke av den registrerade
- Avtal som har ingåtts med den registrerade
- Rättslig förpliktelse (skyldighet)
- Skyddet av nödvändiga intressen
- Allmänt intresse eller myndighetsutövning
- Intresseavvägning (ej tillämplig hos myndigheter)[vii]

Uppräkningen i artikeln är uttömmande. Om ingen av de grunder som anges ovan är tillämplig är behandlingen inte laglig och får därmed inte utföras.

Av de rättsliga grunderna förefaller *allmänt intresse* som mest adekvat att utgå ifrån i den aktuella frågeställningen.

Personuppgifter får behandlas med stöd av grunden *allmänt intresse*, om behandlingen är nödvändig för att utföra en uppgift av allmänt intresse som följer av lag eller annan författning, av kollektivavtal eller av beslut som har meddelats med stöd av lag eller annan författning. [viii]

Nämndernas uppgiftsskyldighet gentemot revisionen regleras i 12 kap. 9 § kommunallagen (SFS 2017:725):

> **Revisorernas rätt till information**
> 9 § Nämnderna, fullmäktigeberedningarna, de enskilda ledamöterna och ersättarna i dessa, samt de anställda är skyldiga att lämna revisorerna de upplysningar som behövs för revisionsarbetet.
> De ska också ge revisorerna tillfälle att när som helst inventera de tillgångar som nämnderna eller fullmäktigeberedningarna har hand om och ta del av de räkenskaper och andra handlingar som berör deras verksamhet.

Genom bestämmelsen regleras nämndernas skyldighet att lämna behövlig information för revisorerna inom ramen för deras arbete. Bestämmelsen är även avsedd att användas som en sekretessbrytande regel.[ix]

Allmänt intresse kan agera som en rättslig grund i den aktuella frågeställningen, förutsatt att även kriteriet ”*nödvändig behandling*” uppfylls i sammanhanget.

Nödvändig behandling

När den tillämpliga rättsliga grunden har fastställts behöver man avgöra om den avsedda behandlingen är *nödvändig* i förhållande till den rättsliga grunden och om den uppfyller de grundläggande principerna i dataskyddsförordningen. Dessutom ankommer det på varje svensk myndighet att i all verksamhet iaktta proportionalitetskravet; dvs. en åtgärd får vidtas endast om det avsedda resultatet står i rimligt förhållande till de olägenheter som kan antas uppstå för den som åtgärden riktas mot – i denna fråga gentemot de registrerade.

Den metod som den personuppgiftsansvarige väljer för att exempelvis utföra sin uppgift av allmänt intresse måste – som all offentlig förvaltning – vara ändamålsenlig, effektiv och proportionerlig och får därmed inte medföra ett onödigt intrång i enskildas privatliv. Ju mer detaljerat en viss uppgift har reglerats, desto mindre utrymme finns det för den personuppgiftsansvarige att välja olika tillvägagångssätt. Detta medför i sin tur en större förutsebarhet i fråga om vilken personuppgiftsbehandling som kan aktualiseras.

Om ett uppdrag i stället har reglerats på en mer övergripande och resultatinriktad nivå kan det sannolikt utföras på många olika sätt, vilka i förhållande till varandra kan vara mer eller mindre nödvändiga i dataskyddsförordningens mening. Kravet på att ändamålet ska vara nödvändigt för att utföra en uppgift av allmänt intresse innebär alltså i sig en spärr mot helt onödig behandling av personuppgifter eller sådan behandling som utgör ett oproportionerligt intrång i privatlivet som inte kunnat förutses.[x]

I sammanhanget är det viktigt att repetera en av de grundläggande principerna: *att man bara får behandla de personuppgifter som är nödvändiga för behandlingen*. Direktåtkomst som frågeställningen avser, innebär en mycket omfattande behörighet och tillgång till både känsliga och integritetskänsliga uppgifter om ett stort antal personer. Utifrån det intrång i privatlivet som detta skulle innebära krävs att åtgärdens proportionalitet är välövervägd och välmotiverad av de personuppgiftsuppgiftsansvariga nämnderna.

Slutsatser

Utgångspunkten för detta yttrande har varit den teoretiska och tekniskt lagda frågan, huruvida det kan bedömas uppfylla dataskyddslagstiftningens krav att tilldela kommunrevisionen behörighet till samtliga nämnders diarium, inkluderande alla ärenden och handlingar. Denna personuppgiftsbehandling skulle innebära att kommunrevisionen har den allra högsta och bredaste behörigheten till ärendehanteringssystemets olika diarium i kommunen.

Ovan framgår att kommunrevisionens rätt till information från nämnder och anställda är begränsat till deras uppdrag inom revisionsarbetet. Vidare framgår ovan att nödvändighetsbedömningen delvis bör göras utifrån personuppgiftsansvarigas motiverade intresse av en effektiv och smidig

förvaltning, samtidigt som begreppet syftar till att agera som en spärr mot helt onödig behandling av personuppgifter eller sådan behandling som utgör ett oproportionerligt intrång i privatlivet som inte kunnat förutses.

Revisionernas möjlighet till upplysningar och information kommer i uttryck genom en generellt utformad bestämmelse i kommunallagen och begränsas till den information som behövs för revisionsarbetet. I stället för en direktåtkomst till alla personuppgifter i systemet, vilket den avsedda behandlingen skulle innebära, torde det finnas flera andra mindre integritetsingripande och mer proportionerliga metoder att använda sig av för att tillgodose revisorerna sin rätt till information.

Dataskyddsombuden bedömer att det är tveksamt om direktåtkomst till samtliga diarier kan anses vara nödvändig behandling för att uppfylla den uppgiftsskyldighet som föreskrivs nämnderna i 12 kap. 9 § kommunallagen. Därmed torde nämnderna sakna rättsligt stöd för att ge revisionen direktåtkomst till samtliga diarier. Att genomföra en personuppgiftsbehandling utan rättsligt stöd strider mot dataskyddsförordningen. Direktåtkomst i den form som är aktuell i föreliggande situation skulle även medföra risk för att personuppgiftsansvariga nämnder skulle bryta mot de grundläggande principerna som bland annat kräver att endast nödvändiga personuppgifter behandlas. Att inte följa de grundläggande principerna anses vara ett allvarligt brott mot dataskyddsförordningen.

I tjänsten,

Anu Sundin och Parisa Maleki Nordin

Dataskyddsombud
Gävle kommuns dataskyddsenhet

---

[i] *Europarlamentets och rådets förordning 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv* 95/46/EG (allmän dataskyddsförordning)
[ii] Artikel 2, dataskyddsförordning 2016/679
[iii] Artikel 4, dataskyddsförordning 2016/679
[iv] Artikel 4, dataskyddsförordning 2016/679

[v] https://www.datainspektionen.se/nyheter/2012/lansstyrelse-maste-begransa-tillgangen-till-personuppgifter/
[vi] Artikel 5, dataskyddsförordningen 2016/679
[vii] Artikel 6, dataskyddsförordningen 2016/679
[viii] 2 kap. 2 §, lagen om kompletterande bestämmelser till EU:s dataskyddsförordning (SFS 2018:218)
[ix] Prop. 2016/17:171, s. 435
[x] Prop. 2017/18:105, s. 60