Granskningsrapport

Dataskyddsombud granskning 2020
”Samtycke som rättslig grund”

Mottagare: Kommunstyrelsen
Diarienummer: KS 2021/0227
Datum: 2021-03-30
Dataskyddsombud: Constance Bell Dahlbäck

Innehåll

Sammanfattning

Rapporten gäller användningen av samtycke som rättslig grund för behandling av personuppgifter enligt dataskyddslagstiftningen. Granskningen har skett på ytlig nivå, en så kallad ”screening”.

Dataskyddsombudet (DSO) konstaterar att kommunstyrelsens verksamhet visar en strävan att efterleva dataskyddslagstiftningen. När det gäller att använda samtycke som rättslig grund bedömer DSO att kommunstyrelsen har en bristande efterlevnad av dataskyddslagstiftningen inom det granskade området eftersom verksamheterna uppgett att det inte kan garanteras att de registrerade fått all nödvändig information för att samtycket ska bli korrekt.

Samtliga verksamheter har rapporterat att de ämnar rätta sig efter DSO:s rekommendationer.

Dataskyddsombudets funktion och uppdrag

Dataskyddsombudets funktion och uppdrag kan återfinnas i artiklarna 38 och 39 i dataskyddsförordningen. Relevant för granskningsarbetet är artikel 38.2[1] och 39.2[2] som stipulerar följande om dataskyddsombudets ställning och uppgifter.

Den personuppgiftsansvarige ska tillhandahålla de resurser som krävs för att dataskyddsombudet ska kunna fullgöra sitt uppdrag. I det ingår även att ge dataskyddsombudet tillgång till de personuppgifter som behandlas och förfarandena för att göra behandlingarna.

[1]Art. 38.2. – dataskyddsombudets ställning: ”Den personuppgiftsansvarige och personuppgiftsbiträdet ska stödja dataskyddsombudet i utförandet av de uppgifter som avses i artikel 39 genom att tillhandahålla de resurser som krävs för att fullgöra dessa uppgifter samt tillgång till personuppgifter och behandlingsförfaranden, samt i upprätthållandet av dennes sakkunskap.”

[2] Art. 39.2 – dataskyddsombudets uppgifter:” Att övervaka efterlevnaden av denna förordning, av andra av unionens eller medlemsstaternas dataskyddsbestämmelser och av den personuppgiftsansvariges eller personuppgiftsbiträdets strategi för skydd av personuppgifter, inbegripet ansvarstilldelning, information till och utbildning av personal som deltar i behandling och tillhörande granskning.”

Dataskyddsombudet ska övervaka efterlevnaden av både dataskyddslagstiftningen och den personuppgiftsansvarigas strategi för att skydda personuppgifter, inklusive hur ansvar fördelas, vilken information och utbildning som de som ska behandla personuppgifter får. Informationen och utbildningen ska avse både behandlingen och vilka uppgifter som ska utföras när dataskyddsombudet gör en granskning.

Granskningens omfattning

Dataskyddombudet (DSO) för Danderyds kommun har valt att granska samtliga nämnders process för att använda samtycke som rättslig grund. Området har valts baserat på de frågor från verksamheterna som kommit till DSO och på Integritetsskyddsmyndighetens (IMY)[3] egen tillsynsplan för åren 2019–2020. Som utgångspunkt gäller att myndigheter ska ha en annan rättslig grund för behandling av personuppgifter än samtycke. Anledningen till det är att myndigheternas personuppgiftsbehandlingar i första hand sker till följd av förpliktelser och uppdrag enligt lag och andra offentligrättsliga regler. Behandling som sker till följd av enskilda personers samtycke utgör ett undantag.

Målet med granskningen har varit att bedöma om personuppgiftsansvariga i allt väsentligt har tillfredsställande kontroll över området som granskas, och om så inte är fallet följa upp de åtgärder som krävs för att rätta till eventuella brister.

Tillvägagångssätt och metod

Mottagarna var primärt avdelningscheferna inom kommunledningskontoret då avdelningscheferna, enligt kommunens anvisning för organisation för säkerhet och dataskydd, är operativt ansvariga för kommunens säkerhetsarbete inom ramen för sina ansvarsområden.[4]. Vissa enhetschefer har även involverats beroende på enhetens ansvarsområde.

Granskningen utfördes som en så kallad ”screening”, en granskning som sker på ytlig nivå. Via det digitala verktyget Microsoft forms skickades åtta ja-eller-nej-frågor ut i ett formulär. Mottagarna informerades om att DSO och kontaktombud kunde involveras för förtydliganden respektive tillgång till personuppgiftsansvarigs behandlingsregister. De mottagare som ännu inte besvarat frågorna vid årsskiftet erbjöds intervjuer med DSO för att granskningen skulle kunna avslutas.

Samtycke hos offentliga myndigheter

Den som ska behandla personuppgifter ska ha en rättslig grund för det. Det finns två huvudindelningar av rättsliga grunder. Den som primärt ska användas av myndigheter/offentliga organ är de situationer som räknas upp i artikel 6.1.b-e i dataskyddsförordningen[5]. Den andra, och den som normalt sett inte ska användas av myndigheter/offentliga organ, är samtycke enligt artikel 6.1.a i dataskyddsförordningen. Anledningen till att offentliga organ primärt inte ska använda samtycke är att personuppgiftsbehandlingarna i de allra flesta fall sker till följd av förpliktelser eller uppdrag enligt lag eller andra offentligrättsliga regler varför de lagliga grunderna i regel utgörs av ”myndighetsutövning” eller ”uppgifter av allmänt intresse”.

[3] Tidigare Datainspektionen
[4] KS 2020/0051
[5] Avtal med den registrerade, rättslig förpliktelse, skydd av grundläggande intressen, myndighetsutövning och uppgifter av allmänt intresse

Samtycke som laglig grund kan endast användas om andra rättsliga grunder inte är tillämpliga för behandlingen. Därutöver ska vissa förutsättningar vara uppfyllda. Extra restriktiva bedömningar om vilka behandlingar som är nödvändiga ska ske när behandlingen dessutom inbegriper extra skyddsvärda eller känsliga personuppgifter enligt artikel 9 i dataskyddsförordningen. Följande kriterier ska vara uppfyllda.

1. Förhållandet mellan registrerad och personuppgiftsansvarig är jämlikt och frivilligt.
2. Samtycket måste kunna dras tillbaka och hela behandlingen därmed raderas.
3. Samtycket måste kunna dokumenteras och organiseras.
4. Mycket tydlig information måste ges den registrerade.

Punkt 1 och 2 utgör de primära anledningarna till att samtycke inte ska användas av myndigheter. Ett helt jämlikt och frivilligt förhållande är svårt att åstadkomma mellan myndighet och medborgare. Personuppgifterna som behandlas behövs som huvudregel för att utföra ett lagstadgat uppdrag vilket omöjliggör radering av personuppgifter vid tillbakadraget samtycke.

Resultat

Statistik

Uppgivna risker i dataskyddsarbetet

Totalt antal mottagare: 8.

Antal som använder samtycke: totalt 5	
Använder samtycke vid behandling av känsliga/extra skyddsvärda personuppgifter	4
Ger inte all nödvändig information	2
Behöver rutiner för när samtycke dras tillbaka	3
Behöver rutiner för att säkerställa jämlikt maktförhållande	2
Behöver rutiner för att dokumentera och organisera	1

Svarsfrekvens

Antal mottagare: totalt 8	
Fullföljde processen inom utsatt tid	4
Fullföljde processen efter utsatt tid	1
Fullföljde processen efter utsatt tid via intervju med DSO	3

Bedömning efter genomförd screening

De största riskområdena som framträtt efter genomförd screening gällande användningen av samtycke har visat sig vara följande.

Användning av samtycke som rättslig grund vid behandling av känsliga eller extra skyddsvärda personuppgifter

De verksamheter som uppgett att man använder samtycke vid behandling av känsliga eller extra skyddsvärda personuppgifter har mottagit rekommendationen att inventera de aktuella

behandlingarna och att använda en annan rättslig grund för behandlingarna. Samtliga har återrapporterat att rekommendationerna kommer att följas.

Verksamheten kan inte garantera att den registrerade mottagit all nödvändig information som krävs vid ett korrekt samtycke
Två verksamheter har uppgett att man inte kan garantera att all nödvändig information tillgängliggjorts för den registrerade. Personuppgiftsansvarig bedöms därför ha en bristande efterlevnad inom det granskade området och därmed av dataskyddslagstiftningen vid tiden för granskningen. Samtliga aktuella verksamheter som mottagit rekommendationer för att åtgärda bristen har återrapporterat att rekommendationerna kommer att följas.

Resterande riskområden gällde alla fastställda rutiner för moment inom dataskyddsarbetet och samtycke. Personuppgiftsansvarig behöver både kunna uppvisa en fastställd rutin och, om uppgiften behövt utföras vid tillfälle, även bevis på hur och att den utförts. Detta enligt dataskyddsförordningens grundläggande princip om ansvarsskyldighet. Därmed ansågs verksamheterna brista i sitt utförande. Vid dialog med verksamheterna som uppgett att rutiner inte fanns fastställda visade det sig dock i majoritet att man inte förstått frågan, och egentligen redan utförde arbetet som kravställt. Samtliga aktuella verksamheter som mottagit rekommendationer har återkommit att de ämnar säkerställa att rutinerna är officiellt fastställda i verksamheterna.

Övrig notering:
Fem av de åtta verksamheterna som mottog frågorna för granskningen använder idag samtycke vilket uppgår till ca 62 procent. Då samtycke helst inte ska användas av myndigheter bedömer DSO andelen som hög. DSO kommer att följa upp arbetet avseende samtycke under 2021 med riktade informationsinsatser på regelbunden basis.

Rekommendationer
Kommunstyrelsens verksamhet har mottagit följande rekommendationer.

- Samtycke är en rättslig grund som normalt bör ses som en sista utväg. Verksamheten ska alltid beakta om en annan rättslig grund kan användas istället.
- Gå igenom behandlingar som sker med stöd av samtycke, och som rör extra skyddsvärda och känsliga personuppgifter, och därefter avgöra om personuppgifterna är helt nödvändiga för att bedriva verksamheten. Om så är fallet ska verksamheten säkerställa att rutiner finns för att skydda uppgifterna.
- För varje behandling som sker med stöd av samtycke säkerställa att de registrerade informeras om följande:
    - Vem som begär samtycke
    - Vilken typ av personuppgifter man ämnar behandla.
    - I vilket syfte personuppgifterna ska behandlas. Är det fler än ett syfte ska vart och ett beskrivas. Observera att syftet får ej ändras utan nytt samtycke.
    - Ett klargörande om att det är möjligt att återkalla sitt samtycke när som helst.
- Bestämma hur och vart en registrerad kan vända sig till kommunstyrelsen för att dra tillbaka samtycket. Informationen ska ges i samband med samtycket. Låt alla medarbetare ta del av informationen för att kunna vara behjälpliga för registrerade.
- Fastställ en rutin för hur ett korrekt samtycke kan säkerställas. Det kan innebära att alltid kontrollera den registrerades relation till personuppgiftsansvarig (exempelvis om personen är ett barn, eller sårbar på annat vis). Se till att rutinen finns med i resterande rutiner för inhämtning av samtycke.
- Fastställ en rutin för hur samtycken dokumenteras och organiseras. Kommunen har mallar för samtycke att använda som grund där informationen behöver anges. Om samtycket gäller en enklare behandling, såsom en e-postlista för nyhetsbrev, kan själva listan, om organiserbar, även användas som dokumentation av samtycket.

Övrig notering
Med anledning av granskningen visar erfarenheten att följande behöver förankras avseende DSO:s roll och uppdrag.

- Vilket mandat DSO innehar som intern tillsynsfunktion.
- Att inkomna kontroll- och granskningsärenden från DSO till personuppgiftsansvarig bör hanteras skyndsamt.
- Att frågor och funderingar angående dataskyddsarbetet, samt återkoppling gällande pågående ärenden, bör lyftas till DSO, direkt eller via kontaktombud, för möjlighet att få råd och utbildning.