2023-05-17 Förvaltningen för funktionsstöd

# Dataskyddsombudets rekommendationer

Konsekvensbedömning: Netpublicator Sign - Elektronisk underskrift för nämnd- och utskottshandlingar

## Artikel 35 dataskyddsförordningen (GDPR)

Enligt artikel 35.2 GDPR ska den personuppgiftsansvarige rådfråga dataskyddsombudet vid genomförande av en konsekvensbedömning avseende dataskydd.

## Kriterier för en godtagbar konsekvensbedömning

Dataskyddsombudet utgår i bedömningen från artikel 35.7 GDPR, vilken anger att en konsekvensbedömning som minst ska innehålla:

a) en systematisk beskrivning av den planerade behandlingen och behandlingens syften, inbegripet, när det är lämpligt, den personuppgiftsansvariges berättigade intresse,
b) en bedömning av behovet av och proportionaliteten hos behandlingen i förhållande till syftena,
c) en bedömning av de risker för de registrerades rättigheter och friheter som avses i punkt 1, och
d) de åtgärder som planeras för att hantera riskerna, inbegripet skyddsåtgärder, säkerhetsåtgärder och rutiner för att säkerställa skyddet av personuppgifterna och för att visa att denna förordning efterlevs, med hänsyn till de registrerades och andra berörda personers rättigheter och berättigade intressen.

I övrigt utgår dataskyddsombudets rekommendationer och kommentarer från artikel 29-gruppens riktlinjer[1] om konsekvensbedömningar (se bilaga 1) samt material avseende konsekvensbedömningar framtaget av Europeiska datatillsynsmannen[2].

## Kommentarer och rekommendationer

### Beskrivning av behandlingen/behandlingarna

Förvaltningen för funktionsstöd planerar att införa digital signering av nämnd- och utskottshandlingar för att bland annat effektivisera handläggningsprocessen och korta ledtider från protokollföring till justering. Det rör sig om två nya behandlingar som ska införas. Det är dels digital signering av beslut som fattas av nämnd/utskott med stöd av kommunallag och/eller socialtjänstlag, dels digital signering vid myndighetsutövning mot

[1] Artikel 29-arbetsgruppen, *Riktlinjer om konsekvensbedömning avseende dataskydd och fastställande av huruvida behandlingen ”sannolikt leder till hög risk” i den mening som avses i förordning 2016/676*, WP 248 rev. 01, 4 oktober 2017
[2] European Data Protection Supervisor, *Accountability on the ground part II: Data Protection Impact Assessment & Prior Consultation*, februari 2018

enskild. Behandlingarna bedöms av förvaltningen vara så pass lika att de kan ingå i samma konsekvensbedömning och dataskyddsombudet instämmer i denna bedömning.

Förvaltningen beskriver i konsekvensbedömningen de planerade behandlingarna, vilka personuppgifter som ingår och syftet med behandlingarna. Avseende beskrivningen av personuppgifter så ska det av avsnitt 2.1.2 i konsekvensbedömningen framgå tillämpliga undantag för att få lov att behandla känsliga personuppgifter enligt artikel 9 i GDPR. Detta avsnitt bör förtydligas så att det klart framgår vilka undantag som hänför sig till vilka kategorier av känsliga personuppgifter. Förvaltningen bör även ta ställning till om samtliga kategorier av extra skyddsvärda personuppgifter som omfattas av behandlingarna har angetts i avsnitt 2.2 i konsekvensbedömningen.

Konsekvensbedömningen innehåller i övrigt en systematisk och tydlig redogörelse om hur handlingarna signeras digitalt. Det framgår även hur personuppgifter kommer att bevaras och vilka tillgångar som är nödvändiga för behandlingens utförande.

**En bedömning av behovet av och proportionaliteten hos behandlingen**

Denna del av rekommendationen syftar till att stämma av förvaltningens planerade åtgärder för att visa att GDPR efterlevs i de planerade behandlingarna. Hänsyn tas alltså till hur förvaltningen visar att principerna i artikel 5 i GDPR omhändertas och vilka åtgärder för att stärka de registrerades rättigheter som vidtas. Detta för att på så vis säkerställa behovet av behandlingen och dess proportionalitet. Inom ramen för bedömningen av behandlingens behov och proportionalitet beaktas även aspekter såsom förhållandet till personuppgiftsbiträden och skyddsåtgärder vid eventuella överföringar till tredjeland.

När det kommer till hur principerna i artikel 5 efterlevs kan det konstateras att ändamålen med behandlingarna framgår av konsekvensbedömningen och varför ändamålen är berättigade. Det framgår även hur man avser att iaktta och tillgodose principerna om uppgiftsminimering och lagringsminimering. Dataskyddsombudet anser dock att förvaltningen behöver säkerställa att laglighetsprincipen är uppfylld genom att i konsekvensbedömningen förtydliga den rättslig grunden för respektive behandling och ange tillämpligt stöd i lag, förordning eller annan författning. Det behöver även framgå tydligare varför personuppgiftsbehandlingen är nödvändig för att utföra uppgift av allmänt intresse eller som ett led i myndighetsutövning.

Förvaltningen har angett vilka av de registrerades rättigheter i förordningen som aktualiseras för de aktuella behandlingarna. När det kommer till åtgärder för att stärka de registrerades rättigheter framgår det av avsnitt 3.3. i konsekvensbedömningen hur förvaltningen avser att uppfylla informationsplikten till de registrerade. Dataskyddsombudet vill i detta hänseende påminna om att de registrerade har rätt till information om behandlingen i enlighet med artikel 13–14 i GDPR. Förvaltningen behöver därför se över hur och på vilket sätt information ska ges till de olika kategorierna av registrerade.

När det gäller förhållandet till personuppgiftsbiträdet Intraservice har förvaltningen i konsekvensbedömningen hänvisat till att biträdesförhållandet är reglerat i de generella reglerna för kommungemensamma interna tjänster. De styrdokument som reglerade kommungemensamma interna tjänster upphörde dock att gälla den 31 december 2022. Numera delas de tjänster som erbjuds från bland andra Intraservice in i bastjänster, tilläggs- och specialisttjänster. Dataskyddsombudet rekommenderar därför förvaltningen

att identifiera vilken typ av tjänst de aktuella behandlingarna avser och att säkerställa att ett nytt personuppgiftsbiträdesavtal har tecknats med Intraservice samt att instruktioner avseende behandlingarna har lämnats.

Förhållandet till underbiträdet har beskrivits i konsekvensbedömningen. Utifrån de medskickade instruktionerna mellan personuppgiftsbiträdet och underbiträdet är dock dataskyddsombudet tveksam till om dessa verkligen avser Netpublicator Sign och inte enbart användningen av Netpublicator för publicering av handlingar till nämnd och utskott.

### Hantering av risker för de registrerades rättigheter och friheter

Dataskyddsombudet anser att förvaltningen har genomfört en väl avvägd riskbedömning. De risker som lyfts bedöms som rimliga och de åtgärder som vidtas framstår som relevanta för att minska riskerna för de registrerade.

Dataskyddsombudet har dock noterat att det av beskrivningen av risk 43 i bifogad riskanalys framgår att *det finns en osäkerhet om vad som gäller och certifikat förfaller* och risken verkar accepteras. Det är otydligt vad för certifikat som risken avser och förvaltningen rekommenderas därför att förtydliga detta.

Dataskyddsombudet har i samband med rekommendationer till andra förvaltningar uppmärksammat att Intraservice identifierat vissa säkerhetsrisker kopplat till klass 2-information i förhållande till Netpublicator. Detta med hänsyn till den stora omfattningen av behandlingar som kommer att ske i Netpublicator Sign i hela staden. Det gjordes en kontroll av Netpublicator 2017, vilken visade att det finns en risk vid användande av Netpublicator och öppna nät. Alltså att en ”man in the middle” eventuellt kan bereda sig tillgång när behandlingen sker över öppna nät. Förvaltningen bör därför utreda om denna risk kvarstår och om så är fallet bör risken inkluderas i riskanalysen.

I övrigt noterar dataskyddsombudet att flera av riskerna förefaller ha ett ganska högt riskvärde även efter åtgärder, men är ändå beredd att hålla med förvaltningen om att dessa inte medför att förhandssamråd bör genomföras. Däremot bör förvaltningen fundera över om ytterligare riskminimerande åtgärder bör vidtas.

### Medverkan från berörda parter

I de fall det är lämpligt ska synpunkter inhämtas från de registrerade eller deras företrädare (artikel 35.9 GDPR). Verksamheten har inte inhämtat de registrerades synpunkter i denna konsekvensbedömning.

## Sammanfattade rekommendationer

- Tydliggör behandlingen av extra skyddsvärda personuppgifter samt tillämpliga undantag för behandlingen av känsliga personuppgifter enligt artikel 9 i GDPR.
- Säkerställ att laglighetsprincipen är uppfylld genom att förtydliga den rättsliga grunden för respektive behandling och beskriv varför behandlingen är nödvändig.
- Säkerställ att samtliga registrerade får den information om behandlingen som de har rätt till enligt artikel 13–14 i GDPR.
- Identifiera vilken typ av tjänst de aktuella behandlingarna avser och säkerställ att förvaltningen har tecknat ett nytt personuppgiftsbiträdesavtal med Intraservice samt att instruktioner avseende behandlingarna har lämnats till Intraservice innan behandlingen påbörjas.

- Säkerställ att det finns korrekta instruktioner mellan personuppgiftsbiträdet/ Intraservice och underbiträdet.
- Överväg om fler riskminimerande åtgärder kan vidtas för de risker som har ett relativt högt riskvärde även efter åtgärder.

Rekommendationer lämnade av:

Anna Bond-Taylor Boman
Dataskyddsombud

Bilaga 1 – utdrag ur artikel 29-gruppens riktlinje om konsekvensbedömningar

**Bilaga 2 – Kriterier för en godtagbar konsekvensbedömning**

Arbetsgruppen föreslår följande kriterier som kan användas av personuppgiftsansvariga för att bedöma huruvida en konsekvensbedömning, eller en metod för att utföra en konsekvensbedömning, är tillräckligt omfattande för att iaktta förordningen:

- ☐ En systematisk beskrivning av behandlingen tillhandahålls (artikel 35.7 a):
  - ☐ Behandlingens art, omfattning, sammanhang och ändamål beaktas (skäl 90).
  - ☐ Registrering av personuppgifter, mottagare och den period under vilken personuppgifterna kommer att lagras.
  - ☐ En funktionell beskrivning av behandlingen tillhandahålls.
  - ☐ De tillgångar som är nödvändiga för personuppgifterna (maskinvara, programvara, nätverk, personer, papper eller spridningskanaler för papper) är identifierade.
  - ☐ Efterlevnad av godkända uppförandekoder beaktas (artikel 35.8).
- ☐ En bedömning av behovet av och proportionaliteten hos behandlingen (artikel 35.7 b):
  - ☐ De planerade åtgärderna för att visa att förordningen efterlevs har fastställts (artikel 35.7 d och skäl 90), med beaktande av följande:
    - ☐ Åtgärder som bidrar till att behandlingen är proportionell och nödvändig på grundval av
      - ☐ särskilda, uttryckligt angivna och berättigade ändamål (artikel 5.1 b),
      - ☐ laglig behandling (artikel 6),
      - ☐ adekvata, relevanta och inte för omfattande uppgifter (artikel 5.1 c),
      - ☐ begränsad lagringstid (artikel 5.1 e).
    - ☐ Åtgärder som stärker de registrerades rättigheter:
      - ☐ Information till den registrerade (artiklarna 12, 13 och 14).
      - ☐ Rätt till tillgång och till dataportabilitet (artiklarna 15 och 20).
      - ☐ Rätt till rättelse och radering (artiklarna 16, 17 och 19).
      - ☐ Rätt att göra invändningar och till begränsning av behandling (artiklarna 18, 19 och 21).
      - ☐ Förhållandet till personuppgiftsbiträden (artikel 28).
      - ☐ Skyddsåtgärder för internationella överföringar (kapitel V).
      - ☐ Förhandssamråd (artikel 36).
- ☐ Hantering av risker för de registrerades rättigheter och friheter (artikel 35.7 c):
  - ☐ Uppskattning av riskens ursprung, art, särdrag och allvar (se skäl 84) eller, mer specifikt, för varje risk (obehörig åtkomst, oönskad ändring och att uppgifter försvinner) ur de registrerades perspektiv:
    - ☐ Beaktande av riskens ursprung (skäl 90).
    - ☐ Identifiering av möjliga konsekvenser för de registrerades rättigheter och friheter vid händelser, däribland obehörig åtkomst, oönskad ändring och förlust av uppgifter.
    - ☐ Identifiering av hot som kan leda till obehörig åtkomst, oönskad ändring och förlust av uppgifter.
    - ☐ Uppskattning av sannolikhetsgrad och allvar (skäl 90).
  - ☐ Fastställande av planerade åtgärder för att hantera dessa risker (artikel 35.7 d och skäl 90).
- ☐ Medverkan från berörda parter:
  - ☐ Rådfrågan av dataskyddsombudet (artikel 35.2).
  - ☐ När så är lämpligt, inhämtning av synpunkter från de registrerade eller deras företrädare (artikel 35.9).

[34] ISO/IEC 29134 (projekt), *Information technology – Security techniques – Privacy impact assessment – Guidelines*, Internationella standardiseringsorganisationen (ISO).

24