2023-09-11 Göteborgs Stads Leasing AB

Dataskyddsombudets rekommendationer

Konsekvensbedömning: Informera och kommunicera i Digitala Navet

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].

Tidigare lämnade kommentarer och rekommendationer

Utöver detta dokument har dataskyddsombudet även kommit med synpunkter och lämnat rekommendationer under verksamhetens löpande arbete med nuvarande version.

Kommentarer och rekommendationer

Beskrivning av behandlingen/behandlingarna

Bolaget beskriver behandlingen med fokus på ett tjänsteperspektiv genom den information som lämnats av Intraservice som tjänsteleverantör. I beskrivningen finns syftet med behandlingen med, utifrån vad införandet av tjänsten ämnar åstadkomma. GSL uppger att de enbart identifierat en behandling som de är personuppgiftsansvariga för, och

[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

en behandling som tjänsteleverantören är personuppgiftsansvariga för. GSL ser sig som personuppgiftsansvariga för behandlingen ”informera och kommunicera i Digitala Navet”. Dataskyddsombudet vill här uppmärksamma bolaget på att eventuella tillkommande behandlingar kan vara aktuella när uppdaterat underlag ifrån Intraservice blir tillgängligt för Stadens verksamheter.

Det är också av vikt att bolaget är uppmärksamma på att en behandling av personuppgifter kan ske i ett eller flera system, och bedömningen av dess risker ska inte enbart vara hänförlig till den aktuella tekniken. I de fall bolaget i framtiden väljer en annan leverantör av tjänsten eller en annan typ av tjänst för samma behandling, bör konsekvensbedömningen ses över.

GSL redogör kortfattat för de tillgångar som är nödvändiga för behandlingen. Dataskyddsombudets uppfattning är, utifrån de beskrivningar av tjänsten som gjorts, att det är flera komponenter ur M365 miljön som är aktuella för behandlingen. Bolaget rekommenderas därför att säkerställa så de fått fullständig information ifrån tjänsteleverantören kopplat till underliggande tillgångar och uppdatera konsekvensbedömningen vid behov.

En bedömning av behovet av och proportionaliteten hos behandlingen

GSL har ett tydligt angivet ändamål som dataskyddsombudet anser vara berättigat. Dock vill dataskyddsombudet lyfta om det är lämpligt att behandlingsnamnet är kopplat till tjänsten Digitala Navet, utan i stället uppmanas bolaget benämna behandlingen och följaktligen också dess ändamål, till något kopplat till själva personuppgiftsbehandlingen. Användningen av intranätet, eller kommunicera med anställda genom användning av intranät, skulle kunna vara alternativ. GSL beskriver hur de ska jobba med ändamålsbegränsning genom olika typer av utbildning och redaktionella behörigheter.

Den rättsliga grunden som GSL har valt att stödja sin behandling på är intresseavvägning. Bolaget har inte bilagt någon dokumentation där de presenterar de avvägningar de gör mellan bolagets intressen och de registrerades intressen. Det är viktigt att bolaget har dokumenterat sina avvägningar för att kunna presentera vid eventuell tillsyn eller förfrågan från en registrerad. Dataskyddsombudet rekommenderar bolaget att förtydliga sin bedömning, antingen i konsekvensbedömningen eller i annan dokumentation.

De personuppgifter som behandlas är avgränsade och relevanta för syftet. Dock framkommer det inte vilka typer av personuppgifter det är som kan förekomma från redaktör och som publiceras i artiklar, utbildningsmaterial, nyheter och liknande. Bolaget rekommenderas att förtydliga detta under 2.2. Förslagsvis tas en rutin fram som förtydligar vilka typer av personuppgifter som får förekomma och vilka som inte får förekomma. Utbildning om personuppgifter/dataskydd är en skyddsåtgärd men rutiner en annan som kan vara bra att ha på plats. Det kan föreligga risker om man lämpar över det ansvaret på den enskilde, för då kan inte GSL som personuppgiftsansvarig säkerställa att behandlingen uppfyller kraven i GDPR. Här vill dataskyddsombudet också uppmärksamma bolaget på att användningen av eventuell kommentarsfunktion också är en situation där ytterligare personuppgifter riskerar att förekomma.

GSL redogör för sin syn på ansvaret för personuppgiftsbehandlingarna. I de fall bolaget anser att det är otydligt vilka behandlingar de är ansvariga för, bör detta lyftas till tjänsteleverantör och/eller andra ansvariga i Staden. Dataskyddsombudet ser stora risker med att frågan om personuppgiftsansvar för bastjänster/fd kommungemensamma tjänster

i Staden inte är utredda. Frågan har diskuterats i dialog med bolaget och kommenteras inte vidare i rekommendationen.

Under 3.3 beskriver GSL hur de ämnar jobba med lagringsminimering. Eftersom en konsekvensbedömning ska kunna stå för sig själv, och att tillsynsmyndighet och registrerad ska kunna läsa den utan att kolla i andra material, rekommenderar dataskyddsombudet bolaget att tydligt skriva ut lagringstid i stället för hänvisning till dokumenthanteringsplan. Alternativt ska dokumenthanteringsplanen biläggas konsekvensbedömningen. När de angivna rutinerna om livscykelhantering är framtagna bör denna konsekvensbedömning uppdateras med information om vad som framgår i dessa.

Åtgärder som stärker de registrerades rättigheter

Dataskyddsombudet anser att GSL åtgärder för att uppfylla informationsplikten är tillräckliga, förutsatt att dessa vidtas innan behandlingen påbörjas. Det är då viktigt att det är tydligt för medarbetarna var informationen finns att tillgå.

Gällande dataportabilitet bör bolaget förtydliga att rättigheten inte är tillämplig eftersom behandlingen som konsekvensbedömningen berör inte bygger på avtal eller samtycke enligt artikel 20. Dataskyddsombudet rekommenderar att bolaget är tydlig med vilka åtgärder som vidtas för att säkerställa rätten till registerutdrag, inte bara en hänvisning till hur den registrerade får informationen om rättigheten.

Under 3.4.4 framkommer brister i regleringen av personuppgiftsansvaret med personuppgiftsbiträden och underbiträden. Det är ett krav enligt GDPR att ha ett personuppgiftsbiträdesavtal på plats då det föreligger en biträdesrelation. I den mån bolaget saknar information och/eller tillgång till de biträdesavtal som används, bör krav riktas mot Intraservice om få ta del av dessa innan behandlingen påbörjas.

I den samlade bedömningen av behovet av och proportionaliteten hos behandlingen har GSL beskrivit varför de anser att användandet av Digitala Navet hjälper bolaget att kunna utföra sitt uppdrag. Dataskyddsombudet saknar den registrerades perspektiv i bedömningen och rekommenderar att bolaget beskriver varför behandlingen är nödvändig och proportionerlig utifrån de registrerades perspektiv. Här kan bolaget tex kortfattat beskriva de åtgärder som beskrivits i kapitel 3 och varför de säkerställer den registrerades integritet.

Slutligen rekommenderas bolaget att se över informationen som framkommer i avsnitt 4 om tredjelandsöverföring. Bedömningen verkar vara Intraservice och inte den egna verksamheten. Som personuppgiftsansvarig är det bolagets skyldighet att ha koll på om en tredjelandsöverföring sker och på vilka grunder. Dataskyddsombudet vill i sammanhanget också hänvisa till den rekommendation som skickades ut från dataskyddsenheten (2023-08-25) och då särskilt på risken med att ingå nya långa avtal. Det saknas även flera avsnitt ur mallen. Eftersom bolaget tagit bort några stycken ur mallen som inte är tillämpliga så saknas också den samlade bedömningen om huruvida den aktuella överföringen är möjlig. Dataskyddsombudet rekommenderar bolaget att komplettera konsekvensbedömningen med detta.

Hantering av risker för de registrerades rättigheter och friheter

Bolaget beskriver under 5.1.1 Generella tekniska åtgärder att de bedömer att ansvaret på att säkerställa tekniska åtgärder för behandlingen faller på personuppgiftsbiträdet

Intraservice. Det är förståeligt att bolaget gör detta uttalande med tanke på hur Staden är organiserad, men enligt reglerna i GDPR åligger det både personuppgiftsansvarige och personuppgiftsbiträdet att säkerställa en lämplig säkerhetsnivå i förhållande till risken, se artikel 32 i GDPR. Bolaget behöver därmed bedöma om de åtgärder som Intraservice vidtar är tillräckliga. Om bolaget anser att det saknas information för att kunna göra den bedömningen, behöver de ställa krav på Intraservice om att få ta del av korrekt underlag vilket är en rättighet bolaget har som PUA.

Dataskyddsombudet enda synpunkt på de risker som bolaget identifierat är angående risk 8 och 9. Där har GSL uppgett att den vidtagna skyddsåtgärden är att Intraservice fått i uppdrag att utreda ansvarsförhållandet för Digitala Navet. Dataskyddsombudet vill här påpeka vikten av att GSL som personuppgiftsansvarig säkerställer att bolaget kan ta sitt ansvar enligt GDPR genom att ställa konkreta krav på personuppgiftsbiträdet. Dataskyddsombudet rekommenderar bolaget att, utifrån gällande rättsläge och den föränderliga status som adekvansbeslutet har, ändock ta höjd för en risk för otillåten tredjelandsöverföring som kan ske. Relevanta åtgärder skulle härtill kunna vara att GSL varje år säkerställer att underleverantören Microsoft fortfarande är certifierade enligt ramverket (EU-U.S. data privacy framework), eller om ramverket upphör, att det finns andra lämpliga överföringsmekanismer.

GSL bedömer att inga kvarstående höga risker finns och därför är inget förhandssamråd nödvändigt, och dataskyddsombudet instämmer i bedömningen.

Medverkan från berörda parter

Verksamheten har inte inhämtat de registrerades synpunkter i denna konsekvensbedömning med hänvisningen till att behandlingen inte är valbar för de anställda/konsulter som omfattas. Dataskyddsombudets uppfattning är att de registrerades synpunkter på behandlingen är än mer viktiga i de fall den registrerade inte har möjlighet att invända eller tacka nej till behandlingen.

Sammanfattade rekommendationer

- Dataskyddsombudet vill här uppmärksamma bolaget på att eventuella tillkommande behandlingar kan vara aktuella att lägga till i konsekvensbedömningen när uppdaterat underlag ifrån Intraservice blir tillgängligt för Stadens verksamheter.
- GSL rekommenderas att säkerställa så bolaget fått fullständig information ifrån tjänsteleverantören kopplat till underliggande tillgångar och om nödvändigt uppdatera konsekvensbedömningen.
- Dataskyddsombudet rekommenderar bolaget att förtydliga sin bedömning, antingen i konsekvensbedömningen eller i annan dokumentation, kopplat till den rättsliga grunden intresseavvägning.
- Bolaget rekommenderas ta fram en rutin som förtydligar vilka typer av personuppgifter som får förekomma och vilka som inte får förekomma vid publicering. Här vill dataskyddsombudet också uppmärksamma bolaget på att användningen av eventuell kommentarsfunktion också är en situation där ytterligare personuppgifter riskerar att förekomma.
- Bolaget rekommenderas att tydligt skriva ut lagringstid i stället för hänvisning till dokumenthanteringsplan. Alternativt ska dokumenthanteringsplanen biläggas konsekvensbedömningen.

- Dataskyddsombudet saknar den registrerades perspektiv i bedömningen och rekommenderar att bolaget beskriver varför behandlingen är nödvändig och proportionerlig utifrån deras perspektiv. Här kan bolaget tex kortfattat beskriva de åtgärder som beskrivits i kapitel 3 och varför de säkerställer den registrerades integritet.

- Dataskyddsombudet rekommenderar bolaget att komplettera konsekvensbedömningen med en sammanfattande bedömning huruvida den föreslagna överföringen till tredjeland är möjlig.
- Dataskyddsombudet rekommenderar bolaget att, utifrån gällande rättsläge och den föränderliga status som adekvansbeslutet har, tar höjd för risken för att en otillåten tredjelandsöverföring kan uppstå vid förändrat rättsläge och aktivt utreder en möjlig utträdesstrategi.

Rekommendationer lämnade av:

Andréa Bergqvist
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