Johan Bålman
Johan.balman@pensionsmyndigheten.se
Telefonnummer

Analysverktyg och eget utrymme

Från många håll har framställts önskemål om vad som kan göras för att förbättra användarens upplevelse i *eget utrymme*.

I PMn tas upp vad som kan göras inom ramen för eget utrymme och vad som faller utanför. PMn avslutar med fem praktiska exempel på vad som är tillåtet och vad som inte är det.

Sammanfattning

För att myndigheter ska kunna erbjuda enklare, tydligare och mera ändamålsenliga digitala tjänster åt enskilda behövs teknisk och administrativ återkoppling om hur användare brukar dessa funktioner. Myndigheter inför därför digitala analysverktyg. Från juridiska utgångspunkter uppkommer frågan om myndigheten kan inhämta uppgifter utan att uppgifter i användares eget utrymme därmed hamnar utanför tillämpningsområdet för 2 kap. 13 § första stycket tryckfrihetsförordningen (TF).

eSams rättsliga expertgrupp bedömer att uppgifter som uppstår i anknytning till e-tjänster kan brukas av myndigheten för egen räkning utan att uppgifter i användares eget utrymme hamnar utanför 2 kap. 13 § första stycket TF, förutsatt att uppgifterna inte hämtas från nyttoinformation i eget utrymme och att myndigheten har begränsat den egna personalens tillgång till nytto-informationen i eget utrymme (jfr HFD 2018 ref. 48).

Som exempel på användning som inte bryter skyddet för eget utrymme kan nämnas att en myndighet i ett digitalt analysverktyg brukar uppgifter om

- antal besök och vilka funktioner som nyttjats, för att upprätta statistik,
- personnummer och IP-adresser som anges vid legitimering, för att granska flödet när identitetskontroller görs för tillträde till en e-tjänst, och

- hur ofta vissa alternativa funktioner väljs i en e-tjänst, för att granska om tjänsten har utformats på ett ändamålsenligt sätt.

Om myndigheten istället brukar nyttoinformation i användares eget utrymme bedöms detta däremot innebära att undantaget enligt 2 kap. 13 § första stycket TF från offentlighetsinsyn inte längre blir tillämpligt. Som exempel på sådan insamling av information kan nämnas att en myndighet, för analys, hämtar vissa svåra ord och uttryck ur de utkast som finns i användares eget utrymme. Detta gäller även om uppgifterna hämtas helt automatiserat och även om de helt har avidentifierats innan de brukas för myndighetens räkning i ett digitalt analysverktyg.

Den behandling av personuppgifter som sker vid användning av analysverktyget måste utföras i enlighet med de krav som ställs i EU:s dataskyddsförordning och kompletterande nationell lagstiftning, inklusive tillämpliga registerförfattningar. Om analysverktyget köps in som tjänst eller det finns andra omständigheter som medför att en extern leverantör kommer att hantera information för myndighetens räkning måste myndigheten säkerställa att sekretessbelagda uppgifter inte röjs i strid med offentlighets- och sekretesslagen.

Bakgrund

I 2 kap. 13 § (tidigare 10 §) första stycket TF föreskrivs att en handling som förvaras hos en myndighet endast som ett led i en teknisk bearbetning eller teknisk lagring för någon annans räkning inte anses som allmän handling hos den myndigheten. Med stöd av denna regel tillhandahåller myndigheter digitala tjänster som möjliggör för användare att behandla uppgifter i eget utrymme. Utkast och liknande handlingar förblir användarens egna och blir inte att anse som allmänna enligt tryckfrihetsförordningen eller inkomna enligt förvaltningslagen så länge de finns i utrymmet och kriterierna för sådant utrymme är uppfyllda.

Här ska genomlysas om bedömningen enligt 2 kap. 13 § första stycket TF av uppgifter i eget utrymme blir en annan ifall en myndighet inför ett digitalt analysverktyg.

I ett betänkande, tre vägledningar[1] och ett rättsligt uttalande har E-delegationen och eSam redovisat sina juridiska bedömningar av den hantering som äger rum när myndigheter tillhandahåller digitala tjänster med eget utrymme. Dessa bedömningar har numera visst stöd i regeringens motivuttalanden i två lagstiftningsärenden, ett om ny förvaltningslag och ett om utökat sekretesskydd i verksamhet för teknisk bearbetning och lagring.[2]

Den syn på eget utrymme som E-delegationen och eSam fört fram har också visst stöd i en dom från Högsta förvaltningsdomstolen (HFD 2018 ref. 48). Beträffande handlingar i ett elektroniskt verksamhetssystem fann Högsta förvaltningsdomstolen att det bör krävas att myndigheten såväl administrativt som tekniskt har begränsat den egna personalens tillgång till uppgifter, så att de inte blir tillgängliga för dem i läsbart skick. Myndighetens personal ska enbart kunna ta del av *den drifts- och säkerhetsrelaterade informationen.*[3] De får alltså inte ha tillgång till *nyttoinformation* i eget utrymme om den informationen ska omfattas av undantaget i 2 kap. 13 (tidigare 10) § första stycket TF från handlingsoffentlighet.[4]

Dessa bedömningar har gjorts trots invändningar som tidigare förts fram, bland annat om att det inte skulle finnas legalt utrymme för att ”isolera” ett tekniskt delmoment under den tid en handling förvaras hos myndigheten och betrakta detta separat (2 kap 13 § första stycket TF skulle ta sikte på hela den tid som myndigheten förvarar en handling). Förvarades en handling av en myndighet inom ramen för myndighetens e-tjänst för att användaren av tjänsten skulle fullgöra en uppgiftsskyldighet eller för att myndigheten skulle ha möjlighet att ge användaren upplysningar eller råd, påstods det att handlingen

---

[1] Se SOU 2014:39 samt E-delegationen, Juridisk vägledning för verksamhetsutveckling inom e-förvaltningen och eSams publikationer, Eget utrymme hos myndighet – en vägledning, Digitalisera rätt En praktisk juridisk vägledning och rättsligt uttalande den 22 november 2017 Eget utrymme, med till.

[2] Se regeringens propositioner 2016/17:180 En modern och rättssäker förvaltning – ny förvaltningslag och 2016/17:198 Utökat sekretesskydd i verksamhet för teknisk bearbetning och lagring.

[3] Det är en annan sak att drift- och säkerhetspersonal — utan att detta hindrar tillämpningen av 2 kap. 13 § andra stycket TF — måste kunna rätta fel i använda system och utföra åtgärder för att säkerställa informationssäkerheten, även om detta i princip ger teknisk tillgång även till eget utrymme (jfr Kammarrätten i Stockholms dom den 26 oktober 2015 i mål nr 7369-15).

[4] Eftersom personal inom myndigheten tagit del av uppgifterna och lagt dem till grund för den statistik som myndigheten tog fram var det inte fråga om endast teknisk bearbetning eller lagring i den mening som avses i 2 kap. 13 (tidigare 10) § första stycket TF. — Det är en annan sak att enstaka särskilt betrodda personer måste kunna få sådan teknisk tillgång till system att de kan rätta fel och vidta åtgärder som är nödvändiga från informationssäkerhetssynpunkt (eSams publikation Eget utrymme hos myndighet – en vägledning, s. 44).

inte förvaras av myndigheten *endast* som led i teknisk bearbetning eller teknisk lagring för annans räkning.

Regeringen använde sig emellertid av begreppet eget utrymme i det lagstiftningsärende genom vilket ett utökat sekretesskydd infördes (se prop. 2016/17:198 s. 7) och förklarade att det finns stöd i rättspraxis för att myndigheter tillhandahåller digitala tjänster som uppfyller kraven i 2 kap. 10 (numera 13) § första stycket TF (a.prop. s. 16). Regeringen fann också att eget utrymme är mera ändamålsenligt än de alternativ som framförts i remissvar (a.prop. s 15 f. och s. 19).[5]

Ett och samma informationsinnehåll i form av *nyttoinformation* kan finnas både i eget utrymme (utan att vara allmän handling där), och i myndighetens verksamhetssystem (som allmän handling), efter att den färdiga handlingen skickats till myndighetens funktion för att ta emot inkommande elektroniska handlingar. På samma sätt kan en handling som bevaras (i ett exemplar) i myndighetens verksamhetssystem lämnas ut till eget utrymme (i form av ett annat exemplar).[6]

Dessa olika exemplar av en handling, dels i eget utrymme, dels i myndighetens verksamhetssystem, ska bedömas var för sig från offentlighets- och sekretessynpunkt. Detta är av betydelse för skyddet av enskildas nyttoinformation när myndigheter inför analysverktyg.

Säkerhetsrelaterad information

För att en myndighet ska kunna tillhandahålla teknisk lagring och teknisk bearbetning för annans räkning behöver vissa säkerhetsåtgärder vidtas av myndigheten. Vanligtvis måste användaren logga in med e-legitimation och när en inloggning skett får *myndigheten* identitetsintyg och annan säkerhetsrelaterad information till sig.

Samtidigt uppkommer säkerhetsrelaterad information i brandväggar och andra hjälpmedel som myndigheten behöver för att skydda såväl sig som användare av eget utrymme. Denna hantering av säkerhetsrelaterad information hindrar

[5] För en närmare beskrivning, se bilagan i eSams promemoria den 22 november 2017 Eget utrymme är numera accepterat i lagmotiv – men vilka juridiska krav ställs på eget utrymme? och det i fotnot 1 nämnda rättsliga uttalandet.
[6] Här kan en jämförelse också göras med ett utkast till beslut som en handläggare tar fram respektive en därefter upprättad beslutshandling.

inte att 2 kap. 13 § första stycket TF blir tillämplig på den nyttoinformation som användare har i eget utrymme.

Den säkerhetsrelaterade informationen ska bedömas för sig från offentlighets- och sekretessynpunkt och inte sammanblandas med användarens nyttoinformation i eget utrymme.

Driftrelaterad information för att tillhandahålla bra tjänster

För att en myndighet ska kunna tillhandahålla enkla, tydliga, väl fungerande och i övrigt ändamålsenliga e-tjänster med eget utrymme behöver myndigheten teknisk och administrativ återkoppling om hur tjänsterna brukas och om eventuella komplikationer vid användningen. För detta brukas olika typer av digitala analysverktyg som hämtar sitt underlag från olika källor av driftrelaterad information.

Detta underlag består av tekniska och administrativa uppgifter om exempelvis vilka alternativa inställningar som väljs för att bruka en e-tjänst, hur navigering sker mellan funktioner, om hanteringen tar ovanligt lång tid i något skede eller annars motverkas eller förhindras, om användningen avslutas i förtid och varifrån användaren kommer. Driftrelaterade uppgifter av detta slag uppkommer när användare besöker och brukar en myndighets e-tjänst. Dessa uppgifter finns inte i eget utrymme utan i myndighetens tekniska hjälpmedel för att tillhandahålla e-tjänsten eller användarens tekniska hjälpmedel för att bruka den. Uppgifterna ingår därmed inte i handlingar som utgör nyttoinformation i eget utrymme.

Den driftrelaterade informationen ska bedömas för sig från offentlighets- och sekretessynpunkt och inte sammanblandas med användares nyttoinformation i eget utrymme.

Myndigheten använder inte nyttoinformation i eget utrymme

I ett rättsfall, där Högsta förvaltningsdomstolens fann att användningen av uppgifter inte kunde anses hänförlig till sådan teknisk bearbetning eller teknisk

lagring som avses i 2 kap. 10 (numera 13) § första stycket tryckfrihets-förordningen, hade Rikspolisstyrelsen inte bara administrerat hanteringen av berörda uppgifter från andra myndigheter. Rikspolisstyrelsen hade också använt *dessa uppgifter* för egen räkning för att ta fram statistik och producera rapporter (HFD 2011 ref. 52). Eftersom Rikspolisstyrelsen inte bara behandlat informationen tekniskt utan även har använt den ansågs dessa handlingar vara allmänna hos styrelsen.

Här är situationen emellertid en annan. Uppgifter som används i digitala analysverktyg hämtas inte från nyttoinformation i eget utrymme, dvs. sådan information som *användare* får se, skriver eller annars tar del av *i sitt utrymme*. Till analysverktygen hämtas istället uppgifter från myndighetens driftrelaterade information och i någon mån även från säkerhetsrelaterad information som uppstår i anknytning till en e-tjänst med eget utrymme.

Att drift- och säkerhetsrelaterad information hanteras på detta sätt av myndigheten exkluderar inte en tillämpning av 2 kap. 13 § första stycket TF med avseende på de handlingar som utgör nyttoinformation i användarens eget utrymme och som myndigheten endast hanterar som led i den tekniska bearbetningen och tekniska lagringen för användaren räkning. Nyttoinformation som en myndighet låter en användare hantera i eget utrymme blir därmed inte allmän hos myndigheten om utrymmen och informationsbehandling utformats på ett ändamålsenligt sätt. Detta gäller även när myndigheten använder ett analysverktyg, förutsatt att verktyget inte brukar uppgifter i handlingar som förvaras i eget utrymme.

Även här ska den drift- och säkerhetsrelaterade informationen bedömas för sig från offentlighets- och sekretessynpunkt och inte sammanblandas med nyttoinformation i utrymmet. Hämtas inga uppgifter för analyser från nyttoinformation, blir nyttoinformationen inte heller använd i det analysverktyg som en myndighet inför. Användningen av verktyget påverkar därmed inte bedömningen enligt 2 kap. 13 § första stycket TF av de handlingar som användaren har i sitt eget utrymme.

Inför en myndighet analysverktyg ändras inte bedömningen enligt 2 kap. 13 § första stycket TF av nyttoinformation i eget utrymme, om de uppgifter som myndigheten bygger analysen på hämtas från myndighetens tekniska hjälpmedel för att tillhandahålla tjänsten eller användares tekniska hjälpmedel för att bruka tjänsten, förutsatt att inga uppgifter hämtas från nyttoinformation i eget utrymme och att

myndigheten har begränsat den egna personalens tillgång till nyttoinformationen i eget utrymme (jfr HFD 2018 ref. 48).

Dataskyddet och sekretessen måste tillgodoses

I denna promemoria redogörs inte för samtliga krav som gäller enligt dataskyddsregelverket vid användning av analysverktyg som innebär behandling av personuppgifter. Eftersom myndigheten som utgångspunkt är personuppgiftsansvarig för den eventuella behandling av personuppgifter som utförs när den använder ett analysverktyg måste myndigheten se till att de krav som följer av EU:s dataskyddsförordning och kompletterande nationell lagstiftning, inbegripet tillämpliga registerförfattningar, efterlevs. Innebär användningen av ett analysverktyg att personuppgifter kommer att behandlas av en extern leverantör måste den personuppgiftsansvariga myndigheten sluta ett personuppgiftsbiträdesavtal med tillhandahållaren av analysverktyget. Myndigheten behöver också säkerställa att de eventuella överföringar som sker till tredjeland har stöd av dataskyddsförordningen.[7]

Om analysverktyget köps in som tjänst eller det finns andra omständigheter som medför att en extern leverantör kommer att hantera information för myndighetens räkning måste myndigheten säkerställa att sekretessbelagda uppgifter inte röjs i strid med offentlighets- och sekretesslagen. Vägledning kring vilka överväganden som myndigheten behöver göra i fråga om sekretess och dataskydd när en extern leverantör hanterar myndighetens information redogörs för i eSams vägledning Outsourcing 2.0, En vägledning om sekretess och dataskydd.

Exempel

Här ska genom några exempel beskrivas vad som närmare menas med att uppgifter för analys bara hämtas från andra källor än nyttoinformation i eget utrymme.

[7] Beträffande de frågor som kan uppkomma i förhållande till leverantörer som är bundna av rättsordningar i tredjeland, se Outsourcing 2.0 En vägledning om sekretess och dataskydd, s. 75 f.

1. Uppgifter hämtas från metadata och driftrelaterad information

En myndighet som behöver statistik över besök i myndighetens tjänster vill hämta uppgifter från en lastbalanseringsfunktion hos myndigheten. Lastbalanseringsfunktionen tar emot besökare, hanterar alla anrop och dirigerar dem till en ledig instans där myndigheten realiserar användares eget utrymme.

Utifrån de loggar som uppstår i lastbalanseringsfunktionen kan statistik produceras över besöken och vilka funktioner som nyttjats, utan att uppgifter hämtas från nyttoinformation i eget utrymme. De loggar som uppstår vid lastbalanseringen är normalt allmänna handlingar hos myndigheten. Denna användning av analysverktyg leder inte till att skyddet för användares nyttoinformation i eget utrymme bryts.

2. Uppgifter utläses automatiserat ur handlingar i eget utrymme

En myndighet som ska förbättra det stöd som ges i myndighetens e-tjänster vill ta reda på om användare genom förklarande texter i tjänsten, lockas att i onödan använda ett svårbegripligt språk. Myndigheten vill därför helt automatiserat, utan att någon individ tar del av informationsinnehållet, räkna användningen av vissa svåra ord och uttryck i de utkast som finns i användares eget utrymme och behandla dessa uppgifter i ett analysverktyg.

Den statistik som myndigheten skapar över svårbegripliga ord och uttryck tas fram genom att myndigheten hämtar uppgifter ur handlingar som utgör användares nyttoinformation i eget utrymme. Även om denna insamling av uppgifter sker helt automatiserat, utan att några andra individer än innehavare av eget utrymme tar del av den nyttoinformation som finns där, leder detta till att skyddet för användares nyttoinformation i eget utrymme bryts. Det beror på att myndigheten för egen räkning tar uppgifter från handlingar i användares eget utrymme. Dessa handlingar får myndigheten behandlas endast tekniskt för annans räkning om de ska omfattas av undantaget i 2 kap. 13 § första stycket TF (HFD 2011 ref. 52). Den rättsliga bedömningen blir densamma även om myndigheten skulle välja att anonymisera uppgifterna när de hämtas och ha nyckeln för identifiering endast som nyttoinformation i respektive användares eget utrymme.

3. Användarna lämnar uppgifter till myndighetens mottagningsfunktion

Här varieras exempel 2, om att få tillgång till uppgifter beträffande användningen av vissa svåra ord och uttryck, så att myndigheten ber sina användare att genom stöd som ges i tjänsten lämna ut uppgifter till myndigheten. Sker det på motsvarande sätt som när användare upprättar en vanlig inlaga och ger in den till myndighetens mottagningsfunktion blir 2 kap. 13 § första stycket TF alltjämt tillämplig på uppgifter i användares eget utrymme.

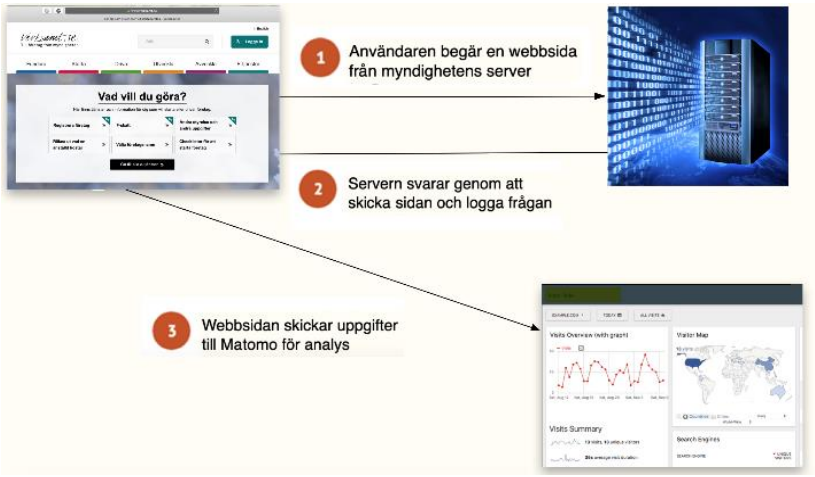
Det är då användaren som, genom att granska och klicka, väljer att lämna ut dessa uppgifter från sitt utrymme och att skicka dem till myndighetens mottagningsfunktion för sådana meddelanden. Den information som myndigheten på detta sätt har mottagit ska bedömas för sig från offentlighets- och sekretessynpunkt och inte sammanblandas med nyttoinformation i eget utrymme.

4. Uppgifter hämtas från användarens tekniska hjälpmedel

En myndighet vill för sin verksamhetsutveckling ta reda på hur användningen av en e-tjänst brukar utspela sig och i vilken omfattning olika alternativa funktioner brukas, allt i syfte att kunna förbättra funktionerna så att de blir enklare för enskilda att använda. Därför vill en myndighet samla in uppgifter om hur ofta vissa alternativa funktioner väljs (klickas) i e-tjänsten och hur ofta uppgifter sparas av användaren för att denne senare ska återkomma för att slutföra sitt ärende. Myndigheten planerar därför att helt automatiserat, utan att någon individ tar del av något informationsinnehåll, räkna antalet klick i vissa rutor för att gå vidare i tjänsten. Funktioner som alltför sällan används kan därmed identifieras och nyttjandegraden i övrigt beräknas så att tjänsten kan utformas mera ändamålsenligt.

Eftersom uppgifter i handlingar som utgör användares nyttoinformation i eget utrymme inte berörs när uppgifter om klick och andra liknande aktiviteter samlas in och används av myndighetens analysverktyg leder denna hantering inte till att skyddet för användares nyttoinformation i eget utrymme bryts. En myndighets driftrelaterade information av detta slag utgör normalt allmän handling hos myndigheten. Här förutsätts också att it-arkitekturen för eget utrymme har utformats så att det finns en separation från övriga verksamhets-system genom vilken myndigheten såväl administrativt som tekniskt har

begränsat den egna personalens tillgång till uppgifter i eget utrymme, så att de inte blir tillgängliga för dem i läsbart skick (HFD 2018 ref. 48).



5. Uppgifter hämtas från tillträdeskontroller

En myndighet vill för sin verksamhetsutveckling använda analysverktyg för att se om de tillträdeskontroller som myndigheten har infört är ändamålsenligt utformade. En del i detta är att knyta viss individ till en viss inloggning för att se att e-legitimationer inte missbrukas så att någon annan släpps in än den individ som har legitimerat sig. I detta syfte vill myndigheten samla in personnummer och ip-adresser som brukas för legitimering respektive tillträde till webbsidor i en e-tjänst — före och efter en autentisering. Myndigheten planerar därför att helt automatiserat hämta sådana uppgifter från identitetsintyg och loggar i syfte att granska flödet för legitimering och tillträde.

Eftersom de handlingar (exempelvis identitetsintyg med personnummer) som lämnas till myndigheten för tillträdeskontroll där blir en del av myndigheten allmänna handlingar leder denna hantering inte till att skyddet för användares nyttoinformation i eget utrymme bryts.