

Rättsavdelningen
Soheil Roshanbin

2025-05-09

Infoklass: 1

Diarienummer:

KFM 9943-2025

Rättsutredning om olämplighetsrekvisitet i 10 kap. 2 a § offentlighets- och sekretesslagen vid utkontraktering av Kronofogdens it-arbetsplats

Innehåll

1	Sammanfattande slutsatser	2
2	Bakgrund och förutsättningar för bedömningarna	3
3	Användning av extern it-infrastruktur	3
3.1	Övergripande överväganden.....	3
3.2	Om sekretess vid utkontraktering	3
4	Bedömningen i detta fall.....	6
4.1	Utgångspunkt för bedömningen	6
4.2	Frågorna	7
5	Utkontraktering av Kronofogdens it-arbetsplats i övriga delar.....	11

1 Sammanfattande slutsatser

Kronofogden bedömer att en utkontraktering av hela eller stora delar av myndighetens e-post- och dokumenthantering till Microsofts infrastruktur är olämplig. Förutsättningarna enligt 10 kap. 2 a § offentlighets- och sekretesslagen (OSL) är därmed inte uppfyllda för att lämna ut sekretessreglerade uppgifter, vilket skulle kunna innebära ett otillåtet röjande.

Bedömningen av olämplighet vilar på informationens känslighet, svårigheter att kontrollera informationsflöden, aggregering av data, legala risker med utländsk lagstiftning, Kronofogdens beroende av ett enskilt bolag, myndighetens uppdrag och det faktum att Kronofogden kan få tillgång till likvärdiga produkter genom en lokal installation av tjänsterna.

Det bedöms däremot vara förenligt med sekretesslagstiftningen att Kronofogden implementerar specifika Microsoftprodukter på ett sådant sätt att endast ett fåtal uppgifter översänds till Microsoft.

En sådan begränsad implementering kan exempelvis innebära lokal lagring av e-post, filer och dokument kombinerat med användning av molnbaserade tjänster som Microsoft Entra ID för bland annat identitets- och åtkomsthantering. Denna modell tillämpas redan av flera andra statliga myndigheter.

2 Bakgrund och förutsättningar för bedömningarna

Skatteverket och Kronofogden samverkar kring it-tjänster med stöd av 15 § förordningen (2017:154) med instruktion för Skatteverket och 8 § förordningen (2016:1333) med instruktion för Kronofogdemyndigheten. Samverkan innebär att Skatteverket tillhandahåller it-tjänster åt Kronofogden, bl.a. tjänsten it-arbetsplats.

Skatteverket har beslutat att genomföra ett inköp av tjänster från Microsoft för produktivitet, artificiell intelligens, möten och molnplattform, samt att införa dessa tjänster i sin verksamhet (dnr 8-133224-2025 och 8-149137-2025).

Kronofogden har det rättsliga ansvaret för sin verksamhet även i de delar Kronofogden erhåller en tjänst från Skatteverket. Kronofogden behöver därför göra en självständig bedömning av de rättsliga förutsättningarna för användning av extern it-infrastruktur.

3 Användning av extern it-infrastruktur

3.1 Övergripande överväganden

Vid utkontraktering av uppgifter måste Kronofogden navigera i ett komplext juridiskt landskap med regler spridda i flera lagar. En noggrann juridisk prövning krävs, där även säkerhetsprinciper som konfidentialitet, riktighet och tillgänglighet måste beaktas. Relevanta regelverk omfattar bland annat arkivering och gallring av allmänna handlingar, sekretess och diarieföring enligt offentlighets- och sekretesslagen (inklusive tystnadsplikt) samt skydd för personuppgifter enligt dataskyddsförordningen. En analys ska baseras på uppgifternas art, hur de hanteras samt var och av vem de behandlas.

3.2 Om sekretess vid utkontraktering

I denna analys finns det särskilda skäl att kommentera den sekretessproblematik som uppstår om Kronofogden skulle utkontraktera hela eller stora delar av sin dokumenthantering till Microsoft.

Vid en utkontraktering som medför att information hos myndigheten blir tillgänglig även för tjänsteleverantören måste begränsningarna i offentlighets- och sekretesslagen beaktas. Grundprincipen är att varje myndighet ansvarar för sin egen verksamhet. En myndighet som avser att genomföra en utkontraktering måste därför utreda vilka slags uppgifter som ska överlämnas till tjänsteleverantören och, i de fall det är fråga om sekretessreglerade uppgifter, noga överväga om det är tillåtet enligt offentlighets- och sekretesslagen.

Sekretess innebär inte bara begränsningar av rätten att ta del av allmänna handlingar utan även ett förbud att röja en uppgift, oavsett om det görs muntligen, genom utlämnande av allmän handling eller på något annat sätt, 3 kap. 1 § OSL.

Sekretess innebär således både handlingssekretess och tystnadsplikt och gäller inte bara för uppgifter i allmänna handlingar, utan även för uppgifter som finns hos en myndighet i handlingar som ännu inte är allmänna.

Otillåtet röjande av en sekretessbelagd uppgift är straffbelagt som brott mot tystnadsplikt, 20 kap. 3 § brottsbalken.

3.2.1 Utkontraktering för teknisk bearbetning eller teknisk lagring enligt 10 kap. 2 a § OSL

Av 10 kap. 2 a § OSL följer att sekretess inte hindrar att en uppgift lämnas till en enskild eller till en annan myndighet som för den utlämnande myndighetens räkning har i uppdrag att endast tekniskt bearbeta eller tekniskt lagra uppgiften, om det med hänsyn till omständigheterna inte är olämpligt att uppgiften lämnas ut. Bestämmelsen syftar till att ge förutsättningar för myndigheter att utkontraktera sin it-drift men är förenad med begränsningar.

I och med att bestämmelsen gäller uppgifter som mottagaren erhåller för teknisk bearbetning eller teknisk lagring omfattas uppgifterna även av sekretess hos mottagaren, i det här fallet tystnadsplikt enligt 4 § lagen (2020:914) om tystnadsplikt vid utkontraktering.

Av andra ledet i 10 kap. 2 a § OSL framgår att myndigheten vid prövning inför en utkontraktering av sekretessreglerade uppgifter ska bedöma om det med hänsyn till omständigheterna inte är olämpligt att uppgifterna lämnas ut. Det innebär att en myndighet, innan en uppgift lämnas ut, ska pröva om det finns skäl som talar emot att uppgiften lämnas ut.

Lämplighetsbedömningen är inte en fråga om vad som rent allmänt är rimligt utan ett kvalificerat rättsligt rekvisit som närmare utvecklas under avsnitt 3.2.2. Om det i efterhand konstateras att det var ett olämpligt utlämnande medför den lagtekniska konstruktionen i 10 kap. 2 a § OSL att det i stället har varit fråga om otillåtet röjande.

3.2.2 Lämplighetsprövningen

I förarbetena till 10 kap. 2 a § OSL framhålls att en bedömning av om ett utlämnande är olämpligt skiljer sig från och är mer omfattande än en traditionell intresseavvägning. Medan en intresseavvägning enbart prövar om intresset av att lämna ut en uppgift väger tyngre än det intresse som sekretessen ska skydda, ska lämplighetsbedömningen även omfatta andra omständigheter, såsom leverantörens förmåga att skydda uppgifterna.

För att avgöra om ett utlämnande är olämpligt behöver en rad olika omständigheter beaktas. Dessa kan generellt kategoriseras enligt följande.

- **Omständigheter kopplade till de uppgifter som övervägs att lämnas ut**

Exempelvis uppgifternas art, känslighet, skyddsintresse och skyddsvärde.

- **Omständigheter kopplade till den uppgiftslämnande myndigheten**

Exempelvis myndighetens egen organisation och interna rutiner.

- **Omständigheter kopplade till uppgiftsmottagaren**

Exempelvis tjänsteverantörens tekniska och organisatoriska förmåga att skydda uppgifterna, dess lokalisering och eventuella underleverantörer, samt om denne omfattas av en lag- eller avtalsreglerad tystnadsplikt.

- **Omständigheter kopplade till den aktuella it-driftstjänsten**

Exempelvis tjänstens utformning, säkerhetsarkitektur och de specifika funktioner som ska användas.

- **Omständigheter kopplade till avtalsförhållandet**

Exempelvis avtalets tydlighet gällande ansvar, säkerhetskrav, revision och hantering av incidenter.

- **Det allmänna säkerhetsläget**

Bedömningar av risker kopplade till det nationella eller internationella säkerhetsläget som kan påverka uppgiftsskyddet.

Det ska alltså göras en samlad och allsidig prövning av samtliga omständigheter som har relevans i det enskilda fallet för att säkerställa att uppgiftshanteringen blir säker och förutsebar.

4 Bedömningen i detta fall

Kronofogdens bedömning: En utkontraktering av myndighetens e-post och dokumenthantering till Microsofts infrastruktur är olämplig.

Detta medför att förutsättningarna enligt 10 kap. 2 a § OSL för att lämna ut sekretessreglerade uppgifter till en extern it-leverantör i detta fall inte kan anses uppfyllda, vilket skulle kunna innebära ett otillåtet röjande.

I bedömningen har hänsyn tagits till informationens känslighet, svårigheterna att kontrollera informationsflöden, de legala riskerna kopplade till utländsk lagstiftning och dataöverföring, samt det faktum att Kronofogden kan få tillgång till likvärdiga produkter genom en lokal installation av tjänsterna.

4.1 Utgångspunkt för bedömningen

I denna del har Kronofogden inhämtat underlag från Skatteverket avseende Microsofts tjänster. Kronofogden har inte haft någon egen dialog med Microsoft.

Kronofogden ska ta ställning till om det finns rättsliga möjligheter att använda M365Apps (molnversionen), Teams, Copilot och Azure m.m. genom användning av Microsofts infrastruktur för merparten av myndighetens dokument och verksamhet.

För att pröva lämpligheten måste ett flertal frågor besvaras. Det är inte fråga om allmänna frågor, utan frågor som knyter an till offentlighets- och sekretesslagens förarbeten och som återges i avsnitt 3.2.2.

Frågorna stämmer delvis överens med det som framgår av eSamverkansprogrammets vägledning vid utkontraktering (ES 2023-06).

4.2 Frågorna

4.2.1 Är det fråga om uppgifter av känsligt slag?

I Kronofogdens verksamhet förekommer såväl offentlig information som mycket känslig information. Det omfattar uppgifter som tillhör gäldenärer, borgenärer, sökande, förvaltare med flera. Uppgifterna kan i många fall vara sekretessreglerade. I vissa fall gäller absolut sekretess för uppgifterna.

Genom bl.a. den samverkan som Kronofogden har med de brottsbekämpande myndigheterna, förekommer det i Kronofogdens verksamhet uppgifter av sådan art att myndigheten inte bör överlåta rådgivningen över dem.

Även i ärendehandläggningen förekommer uppgifter som är särskilt skyddsvärda, trots att det inte är fråga om sådana uppgifter som omfattas av säkerhetsskyddslagens (2018:585) regler.

4.2.2 Kan Kronofogden genom styrande dokument påverka vilken information som överförs till Microsoft?

Kronofogden har cirka 2 300 medarbetare. Även om myndigheten skulle besluta att medarbetarna inte får skriva in känsliga uppgifter eller mycket skyddsvärd information i dokument eller e-post, är detta i realiteten varken möjligt att verkställa eller fullt ut kontrollera. Än mindre är det realistiskt att styra innehållet i de dokument, eller de uppgifter i dokument, som myndigheten skulle få ta del av från enskilda och andra myndigheter. Skyddet för uppgifterna måste i en så stor verksamhet som Kronofogdens implementeras direkt i tjänsten.

4.2.3 Kan aggregering innebära att den totala informationsmängden blir mer skyddsvärd?

Om Kronofogden skulle använda en privat aktörs infrastruktur för stora delar av sin e-post- och dokumenthantering, frånhänder sig myndigheten kontrollen över en mycket stor mängd skyddsvärd information. Som aggregerad skulle denna information kunna ha betydelse för fler än enbart Kronofogden. I nuläget saknas skäl att närmare analysera om den aggregerade mängden uppgifter skulle ha betydelse för Sveriges säkerhet enligt säkerhetsskyddslagen, men det finns goda grunder att anta att

aggregeringen innebär att informationsmängden som helhet blir mer skyddsvärd.

4.2.4 Innebär användning av Microsofts infrastruktur en risk för störningar i myndighetens verksamhet?

Om Kronofogden använder Microsofts infrastruktur för sin dokumenthantering blir myndigheten beroende av bolagets drift för att kunna fullgöra sitt uppdrag. Användningen av Microsofts infrastruktur skulle därför kunna innebära en sårbarhet för Kronofogden.

4.2.5 Förekommer underleverantörer och kan i så fall skyddet upprätthållas hos dessa?

Det förekommer underleverantörer. Det innebär att kretsen av de som får tillgång till Kronofogdens information kommer att vara vidare än specifikt Microsoft. Dessa bolag granskas och kontrolleras av Microsoft. Någon avstämning med kunden sker inte, enligt den information som Kronofogden har tagit del av. Räckvidden av Kronofogdens tillit till dessa bolag hänger således samman med det förtroende Kronofogden skulle ha för Microsoft enligt parternas avtal.

4.2.6 Är den interna åtkomsten hos leverantören begränsad med tekniska eller med organisatoriska rutiner?

Microsoft synes ha välutvecklade tekniska och organisatoriska rutiner som bör hindra intern och extern obehörig åtkomst till Kronofogdens information. Utifrån detta perspektiv finns ingenting som talar mot bolaget i fråga om utkontraktering av myndighetens it-arbetsplats.

4.2.7 Kan leverantörens geografiska lokalisering och bindning till lagstiftning (inklusive extraterritoriell) hindra att skyddet för uppgifterna kan upprätthållas?

Var uppgifterna kommer att hanteras geografiskt kan ha betydelse. En viss geografisk lokalisering hos en leverantör kan vara olämplig med avseende på vissa känsliga uppgifter. I samband med utkontraktering, och i synnerhet när uppgifter riskerar att överföras till tredjeland, behöver

olämplighetsbedömningen ta hänsyn till om utkontrakteringen kan leda till att personuppgifter efter utlämnandet antas komma att behandlas i strid med dataskyddsförordningen.

Microsoft kan såvitt känt inte garantera att uppgifterna kommer att förvaras inom EU/EES. Bolaget är också amerikanskt. USA har ett annat regelverk än EU vad gäller skyddet för privatlivet, vilket kan påverka skyddet för uppgifterna. Härtill kan amerikanska myndigheter, med bindande verkan enligt amerikansk lag, bereda sig tillgång till Kronofogdens uppgifter.

Kronofogden skulle i vissa fall inte ens få vetskap om att informationen har lämnats ut till amerikanska myndigheter och har ingen möjlighet att överklaga ett sådant beslut. Denna risk ska inte överdrivas men behöver beaktas inom ramen för lämplighetsbedömningen.

4.2.8 Hur påverkas Kronofogden om dataskyddsavtalet mellan EU och USA underkänns?

Sedan 2023 finns ett beslut om adekvat skyddsnivå för USA. Beslutet är baserat på en överenskommelse mellan EU och USA om hur personuppgifter som överförs från EU- och EES-länderna ska skyddas i USA, det så kallade EU-U.S. Data Privacy Framework.

Adekvansbeslutet ger svenska myndigheter rätt att överföra uppgifter till Microsoft i de delar uppgifterna förs vidare till USA.

Dataskyddsavtalet mellan EU och USA har vid två tidigare tillfällen underkänts av EU-domstolen. Ett bärande skäl har varit att enskilda i Europa saknat tillräckliga möjligheter till effektiva rättsmedel gällande hur deras personuppgifter behandlas av amerikanska myndigheter.

I det nya beslutet om adekvat skyddsnivå för USA lyfter EU-kommissionen särskilt fram Privacy and Civil Liberties Oversight Board som kontrollorgan för att säkerställa att personuppgifter som överförs till USA behandlas på ett tillfredsställande sätt. Som Integritetskyddsmyndigheten har redogjort för finns dock en del omständigheter som skapat frågetecken kring kommissionens beslut om adekvat skyddsnivå.¹ Detta medför en osäkerhet

¹ <https://www.imy.se/blogg/overforing-av-personuppgifter-till-usa-vad-galler/>, kontrollerad 2025-05-09.

om EU-domstolen vid en ny prövning skulle underkänna kommissionens beslut.

Det är svårt att spekulera kring utfallet men om beslutet upphävs på nytt skulle den nuvarande rättsliga grunden för överföring av uppgifter till USA upphöra, vilket skulle begränsa Kronofogdens förmåga att använda tjänsterna.

4.2.9 Kan Kronofogden genom en s.k. exit-strategi lämna tjänsten?

Om Kronofogden använder Microsofts infrastruktur för sin dokumenthantering blir myndigheten beroende av bolagets drift för att kunna fullgöra sitt uppdrag. Det går delvis att minska riskerna för ett sådant beroende genom att myndigheten har en lösning för avbrott i tjänsten och en så kallad exitstrategi. Det bör dock beaktas att Kronofogdens verksamhet de facto kommer att utsättas för vissa störningar, beroende på hur väl en sådan strategi kan tillämpas.

4.2.10 Ger en allsidig bedömning utfallet att ett utlämnande inte är olämpligt?

Kronofogden ser betydande svårigheter med att fullt ut kontrollera vilken information som överförs till Microsofts infrastruktur, både internt från medarbetare och externt från enskilda och andra myndigheter.

En övergång till Microsoft för e-post och dokumenthantering skulle innebära att en stor mängd aggregerad data, som därmed blir mer skyddsvärd, hamnar utanför myndighetens direkta kontroll.

Denna situation kompliceras ytterligare av att Microsoft, som amerikanskt bolag, är underställt amerikansk lagstiftning, vilket kan medföra att amerikanska myndigheter får tillgång till Kronofogdens uppgifter, ibland utan svensk insyn. Till det kommer omständigheten att bolaget har flera underleverantörer i en struktur och geografisk spridning som är svår för Kronofogden att överblicka.

Beroendet av Microsofts tjänster medför en risk för Kronofogdens förmåga att utföra sitt uppdrag om tjänsterna av olika skäl blir otillgängliga. Den nuvarande rättsliga grunden för dataöverföring till USA är osäker. Ett nytt underkännande skulle begränsa användningen av tjänsterna. Att implementera en fungerande exitstrategi från ett sådant system bedöms

också vara komplext och skulle sannolikt medföra störningar i verksamheten.

Redan dessa omständigheter talar mot en utkontraktering av Kronofogdens it-arbetsplats till Microsoft. Härtill får beaktas att Kronofogden inte enbart ska ta hänsyn till de uppgifter som genereras i myndighetens egen verksamhet, utan också uppgifter som myndigheten får ta del av genom sina kontakter med utomstående och andra myndigheter. Kronofogden blir inte alltid i förväg underrättad om innehållet i dessa dokument, och myndigheten skulle därmed överföra detta innehåll till Microsofts infrastruktur.

En viktig faktor i bedömningen är att Kronofogden kan utföra sitt uppdrag med i stort sett likvärdiga produkter genom en lokal installation av tjänsterna. Det finns således inget avgörande behov av att exponera myndighetens information för ett enskilt bolag.

Vissa funktioner, såsom användning av stora språkmodeller (AI) som möjliggörs genom extern databehandling, skulle vara fördelaktiga, men i avvägningen mellan de intressen som sekretesslagstiftningen syftar till att skydda och de nyttoeffekter som myndigheten skulle få tillgång till genom att överlämna stora och känsliga informationsmängder till Microsoft, talar övervägande skäl mot en sådan utkontraktering.

Under sådana förhållanden framstår det som olämpligt att Kronofogden frånhänder sig rådigheten över myndighetens uppgifter till Microsoft. Om rekvisiten i 10 kap. 2 a § OSL inte uppfylls, saknas grund för att överlämna sekretessreglerad information till Microsoft. En utkontraktering skulle under sådana förhållanden vara otillåten.

5 Utkontraktering av Kronofogdens it-arbetsplats i övriga delar

Den bedömning som nu gjorts tar sikte på utkontraktering av hela eller stora delar av Kronofogdens it-arbetsplats genom extern behandling av dokument och e-post.

Det är dock förenligt med sekretesslagstiftningen att Kronofogden implementerar de aktuella produkterna på ett sådant sätt att endast ett fåtal uppgifter översänds till Microsoft. Detta kan exempelvis ske genom en kombination av lokal lagring av e-post, filer och dokument samt användning av Microsoft Entra ID för bland annat identitets- och åtkomsthantering. Det

är också den implementering som ett flertal statliga myndigheter har tillämpat.

Soheil Roshanbin