Tjänsteutlåtande
Utfärdat 2023-10-13
Diarienummer SFF-2023-01812

Handläggare
Lotta Åström

Beslut om konsekvensbedömning samt egen användning av Digitala navet

Förslag till beslut

I stadsfastighetsnämnden

1. Stadsfastighetsnämnden godkänner konsekvensbedömningen och därmed användandet av Digitala navet för stadsfastighetsförvaltningen.

Sammanfattning

Digitala navet är ett nytt intranät som ska ersätta nuvarande intranät. Arbete med att utveckla det nya intranätet har pågått sedan 2019 för att möta Göteborgs Stads behov av relevant och kvalitetssäkrad information till stadens anställda och för att bättre uppfylla de krav tillgänglighetslagstiftningen ställer. Arbetet med att ta fram det nya intranätet har letts av Intraservice men har skett i nära samarbete med stadens förvaltningar och bolag.

Digitala navet införs i olika etapper inom staden med start under hösten. Stadsfastighetsförvaltningen är en av de åtta aktörer som ingår i den grupp som är först ut med införandet. Intraservice är först ut med införandet och stadsfastighetsförvaltningen går, efter nämndbeslut, in i Digitala navet i slutet av november.

Inför att en verksamhet ska påbörja en ny personuppgiftsbehandling där det kan förekomma risker för de registrerade ska en konsekvensbedömning enligt dataskyddsförordningen genomföras.

Efter genomförd konsekvensbedömning konstateras att ett fåtal höga risker kvarstår gentemot de registrerade efter skyddsåtgärder och därmed krävs enligt dataskyddsförordningen en begäran om samråd hos Integritetsskyddsmyndigheten (IMY). Förvaltningen bedömer att ett sådant samråd inte är praktiskt genomförbart utifrån stadens organisering och de beslut om utrullningsplan som redan fattats för Digitala navet. De risker som kvarstår har en enskild förvaltning svårt att eliminera även om IMY skulle förelägga förvaltningen att vidta åtgärder.

Nämnden rekommenderas därför att lämna sitt godkännande för att inleda personuppgiftsbehandlingen och därmed lanseringen av Digitala navet då den sammantagna bedömningen är att fördelarna med införandet av Digitala navet överväger riskerna som identifierats i konsekvensbedömningen. Stadsfastighetsförvaltningen bör som en del av stadens organisation fullfölja de beslut som Intraservice fattat kring valet av teknisk plattform och tidsplan för införandet av Digitala navet.

Bedömning ur ekonomisk dimension

Digitala navet baseras på Microsoft 365-plattformen som redan används av Göteborgs Stad vilket innebär att ingen ny plattform behöver upphandlas för ändamålet. Förvaltningen bedömer att det lokala införandet ryms inom befintlig ekonomisk ram.

Bedömning ur ekologisk dimension

Förvaltningen har inte funnit några särskilda aspekter på frågan utifrån denna dimension.

Bedömning ur social dimension

Kommunikation och tillgänglighet skapar möjligheter till ökad transparens och insyn i information och beslut. Det stärker demokratin. Digitala navet är ett modernt verktyg för att ge medarbetaren tillgång till relevant och aktuell information, som hen behöver för att kunna utföra sina arbetsuppgifter.

Med Digitala navet kan förvaltningen på ett bättre sätt möte de behov som tillgänglighetslagstiftningen från 2018 lyfter. Det handlar till exempel om att det finns stödverktyg som kan läsa upp skriftlig information.

Ett tydligare ansvar för informationen på varje sida i Digitala navet höjer kvaliteten och aktualiteten på innehållet. Arbetet med texterna, tydligare ansvar, nya rutiner för livscykelhantering och den utökade utbildningen för redaktörerna höjer även den språkliga kvaliteten på informationen. Digitala navet har utvecklats för att möta behovet av kvalitetssäkrad information till stadens anställda och är därmed en del av måluppfyllnaden.

Samverkan

Information har skett med förvaltningens samverkansgrupp den 23 oktober 2023.

Bilagor

1. Konsekvensbedömning enligt dataskyddsförordningen – Personuppgiftsbehandlingen informera och kommunicera i intranät – stadsfastighetsförvaltningen
2. Göteborgs Stads riktlinje för informationssäkerhet

Ärendet

Stadsfastighetsförvaltningen planerar, efter nämndbeslut, att införa Digitala navet i slutet november. En konsekvensbedömning av personuppgiftsbehandlingen har genomförts i enlighet med dataskyddsförordningen.

Intraservice är pilot och den förvaltning som först planerar att börja använda det nya intranätet. Nämnden för Intraservice har den 21 juni 2023 beslutat att införa Digitala navet på sammanträdet. Även stadsledningskontoret har beslutat att införa det nya intranätet med information till kommunstyrelsen den 23 augusti 2023.

Beskrivning av ärendet

Bakgrund och arbete inför planerad lansering

Intranätet är en av Göteborgs Stads gemensamma, prioriterade kommunikationskanaler. Digitala navet är ett nytt intranät som ska ersätta nuvarande intranät. Arbete har pågått sedan 2019 för att möta Göteborgs Stads behov av relevant och kvalitetssäkrad information till stadens anställda och för att bättre uppfylla de krav tillgänglighetslagstiftningen ställer. Digitala navet införs i olika etapper och stadsfastighetsförvaltningen är bland de första förvaltningar och bolag som inför Digitala navet. Planen är för närvarande att det nya intranätet, efter nämndbeslut, ska lanseras i slutet av november på stadsfastighetsförvaltningen.

Lanseringen av Digitala navet planerades ske redan år 2022 men pausades när projektet uppmärksammade oklarheter kopplade till personuppgiftsbehandlingarna i Digitala navet och den överföring av personuppgifter till USA som sker i Microsoft 365-miljön. I och med att ett så kallat adekvansbeslut gällande överföring av personuppgifter till USA fattades under sommaren 2023 har de höga risker för registrerade som identifierats till stor del inaktualiserats. Intraservice har även fått i uppdrag att utreda utträdesstrategi om rättsläget skulle förändras för överföring av personuppgifter till USA.

Syftet med Göteborgs Stads intranät

Syftet med det Digitala navet är att kunna kommunicera och sprida information på ett enkelt sätt till medarbetare inom staden. Stadens intranät är en transparent plattform för internkommunikation för att sprida stadens information och värderingar på ett enhetligt sätt till alla delar av organisationen samtidigt.

Digitala navet och Microsoft 365 plattformen (M365)

Den tekniska lösningen för Digitala navet bygger på SharePoint. SharePoint är en plattform som ingår som en del i den så kallade Microsoft 365-plattformen som licensieras av Microsoft (i det följande ”M365”). M365 licensieras till Göteborgs Stad via avtal med Atea.

Göteborgs Stad använder sedan 2016 flera delar i M365. I dagsläget använder staden bland annat Teams, Officeprogrammen och SharePoint. En stor mängd information, däribland personuppgifter, lagras och behandlas av staden i M365. Stadeninterna regler med uppgifter om vilken information som får finnas i M365 finns i Göteborgs Stads Riktlinje för informationssäkerhet, med tillhörande klassificeringsmodell. Riktlinjen tillåter att information i klasserna 0–2 enligt klassificeringsmodellen får finnas i M365. För information som innehåller personuppgifter gäller även alla tillämpliga bestämmelser

i dataskyddslagstiftningen. Notera att för Digitala navet tillåts endast information i klasserna 0 och 1.

Personuppgiftsbehandling i Digitala navet

Stadsfastighetsnämnden är personuppgiftsansvarig för behandlingarna i Digitala navet med Intraservice som personuppgiftsbiträde och Microsoft 365 som i sin tur är underleverantör.

Stadsfastighetsförvaltningen ansvarar för personuppgiftsbehandlingen i processen informera och kommunicera med anställda. Behandlingen innebär att stadsfastighetsförvaltningen är ansvarig för att producera kommungemensam information på ett antal sidor gällande verksamheten. Detta för att ge stadens medarbetare lättillgänglig information, samt för att ge stöd och vägledning inom fastighetsrelaterade frågor som planera, bygga, hyra in, förvalta och utveckla de lokaler och utemiljöer som Göteborgs Stads verksamheter behöver.

Stadsfastighetsförvaltningen ansvarar även för att som arbetsgivare ge medarbetare specifik information för förvaltningen, exempelvis information som rör anställningen eller krisinformation, tillvägagångssätt för olika typer av arbetsuppgifter, och nyheter om olika händelser och projekt inom förvaltningen. Det nya intranätet ska även ge ökad delaktighet samt möjlighet att påverka och skapa dialog hos anställda.

På artikelsidor förekommer namn på kontaktpersoner för olika frågor och i nyheter och annat redaktionellt material förekommer namn på kontaktuppgifter till medarbetare och chefer som kan ha olika typer av ansvar som exempelvis samordnare eller projektledare. Även andra personuppgifter kan förekomma i det redaktionella materialet beroende på textens inriktning och vad den ska förmedla.

För att det redaktionella materialet ska hanteras på ett korrekt sätt tar stadsfastighetsförvaltningen fram en rutin för publicering och hantering av personuppgifter i Digitala navet. Rutinen kommer beröra vilka typer av personuppgifter som kan publiceras samt hur medverkan kan ske för anställda utifrån den rättsliga grunden allmänt intresse. Kopplat till varje redaktionell publicering sker även en avstämning med den registrerade, för att säkerställa att innehållet är korrekt och publicerbart. Samtliga publiceringsansvariga (redaktörer) genomgår även ett gediget utbildningspaket, bland annat för att säkerställa kunskap om hur man förhåller sig till personuppgifter. Utbildningen är en förutsättning för att få behörighet att publicera innehåll i Digitala navet.

Riskbedömning av personuppgiftsbehandlingen

En riskbedömning av personuppgiftsbehandlingen har genomförts som en del i konsekvensbedömningen. Med hjälp av skyddsåtgärder som utbildning, tekniska åtgärder samt information till de registrerade har flera risker kunnat sänkas till en låg nivå.

För att minimera risken för tredjelandsöverföring är data i Microsoft365 till stor del flyttad till datacenter i Sverige och beställning på flytt av resterande data är gjord. Med dessa åtgärder genomförda kommer all Microsofts hantering av data flytta till Europa under 2023.

Intraservice, som leverantör av Digitala navet, har i sin konsekvensbedömning (daterad 2023-06-14) för införandet av det nya intranätet tagit upp risker gällande Microsoft som

underleverantör. Trots EU-kommissionens adekvansbeslut (10 juli 2023) anser stadsfastighetsförvaltningen att det kvarstår två identifierade risker.

En risk är potentiell spridning av data till olämpliga underleverantörer då Microsoft enligt sina användarvillkor har rätt att ensidigt byta ut och lägga till underleverantörer. Det ger förvaltningen begränsad insyn. En annan identifierad risk är övervakning av anställda genom analys och statistik av Microsoft där det inte är utrett vem eller vilka som får ta del av dessa uppgifter. Det skulle kunna innebära att personuppgifter används till andra ändamål än ursprungsändamålet. Intraservice har meddelat att de inte har någon ytterligare information gällande de två riskerna.

De två riskerna skulle kunna innebära att stadsfastighetsnämnden inte når upp till principer för behandling av personuppgifter i dataskyddsförordningen (artikel 5.1a om öppenhet samt artikel 5.1b och dess finalitetsprincip). Det skulle i förlängningen innebära att de registrerade inte får tillgång till behandlade personuppgifter eller tydlig information om personuppgiftsbehandlingen (artikel 13 respektive 15).

Dataskyddsombudets bedömning

Dataskyddsombudets bedömning är att de kvarvarande riskerna innebär att stadsfastighetsförvaltningen, enligt GDPR, ska begära förhandssamråd hos Integritetsskyddsmyndigheten innan personuppgiftsbehandlingen kan påbörjas.

Förvaltningens bedömning

Att införa ett nytt intranät med moderna funktioner effektiviserar förvaltningens interna kommunikation och möjliggör att anställda på förvaltningen har tillgång till relevant och aktuell information som behövs i tjänsten.

En konsekvensbedömning enligt dataskyddsförordningen har genomförts och mot bakgrunden av behovet av relevant och kvalitetssäkrad information till anställda, som når upp till tillgänglighetslagstiftningen, bedöms fördelarna överstiga nackdelarna och behandlingen anses alltså vara proportionerlig.

Vissa risker kvarstår kopplat till Microsoft som underleverantör och Intraservice utreder lämpliga skyddsåtgärder. Risknivåerna för den information som publiceras i Digitala navet och som delas inom Göteborgs Stad bedöms totalt sätt som låga, exempelvis behandlas inga känsliga personuppgifter så som hälsa eller facktillhörighet (artikel 9).

Dock kvarstår höga risknivåer i två fall vilket enligt dataskyddsförordningen borde föranleda begäran om förhandssamråd till Integritetsskyddsmyndigheten (IMY). IMY ger sedan ett skriftligt råd gällande behandlingen och dess risker. Förvaltningen bedömer att ett sådant samråd inte är praktiskt genomförbart utifrån stadens organisering och de beslut om utrullningsplan som redan fattats för Digitala navet. De risker som kvarstår har en enskild förvaltning svårt att eliminera även om IMY skulle förelägga förvaltningen att vidta åtgärder. Såsom förvaltningens dataskyddsombud påpekar (bilaga 2 till konsekvensbedömningen) beror riskerna på stadens organisering snarare än underlåtenhet från förvaltningens sida. Dessutom har Intraservice beslutat om en utrullningsplan där andra förvaltningar är direkt beroende av att stadsfastighetsförvaltningen inför Digitala navet i november. Det finns därmed inte något tidsmässigt utrymme för samråd med tillsynsmyndigheten.

Den sammantagna bedömningen är att fördelarna med införandet av Digitala navet överväger riskerna som identifierats i konsekvensbedömningen. Stadsfastighetsförvaltningen bör som en del av stadens organisation fullfölja de beslut som Intraservice fattat kring valet av teknisk plattform och tidsplan för införandet av Digitala navet.

Maria Hagberg	Martin Blixt
Avdelningschef	Förvaltningsdirektör

Göteborgs Stad

Konsekvensbedömning enligt dataskyddsförordningen

Informera och kommunicera i intranät

2023-10-10

Versionshantering

Datum	Version	Beskrivning	Ändrat av
2023-08-31	0.1	Överföring av information gällande behandlingar kopplade till Digitala navet från intraservice	Björn Alm
2023-09-13	0.1.1	Uppdatering av riskbedömning samt förtydliganden från intraservice	Karin Mondet Larsson, Björn Alm och Fredrik Andersson
2023-09-26	1.0	Första utkast skickat till dataskyddsombud	Björn Alm och Karin Mondet Larsson
2023-10-04	2.0	Andra utkast efter kommentarer från dataskyddsombud	Björn Alm
2023-10-10	3.0	Slutversion med dataskyddsombuds rekommendationer bifogade	Björn Alm

Innehåll

1 Inledning 4

1.1 Bakgrund och behov av behandling/behandlingar 4

1.2 Behov av konsekvensbedömning 4

1.3 Deltagare och roller 5

1.4 Personuppgiftsansvar 5

2 Beskrivning av behandlingen/ behandlingarna 5

2.1 Översiktlig beskrivning av behandlingen/behandlingarna..... 6

2.1.1 Tillgångar..... 8

2.1.2 Personuppgiftsbiträden och underbiträden 9

2.1.3 Mottagare 9

2.2 Översikt behandling/behandlingar..... 9

2.2.1 Personuppgifter om lagöverträdelser 10

2.2.2 Kategorier av registrerade 11

2.2.3 Behandlingens/behandlingarnas omfattning 11

2.3 Ändamål 11

2.4 Rättslig grund 11

2.4.1 Känsliga personuppgifter 12

3 Behov/proportionalitet 12

3.1 Ändamålsbegränsning 12

3.2 Uppgiftsminimering 12

3.3 Lagringsminimering 13

3.4 Åtgärder som stärker de registrerades rättigheter 14

3.4.1 Informationsplikt 14
3.4.2 Tillgång och dataportabilitet 14
3.4.3 Rättelse och radering 15
3.4.4 Invändningar och begränsning av behandlingen/behandlingarna 15
3.4.5 Personuppgiftsbiträdesavtal och instruktioner 15
3.5 Samlad bedömning av behovet av och proportionaliteten hos behandlingen/behandlingarna 16
4 Överföring av personuppgifter utanför EU/EES 17
4.1 Sker det en överföring av personuppgifter utanför EU/EES? . 17
4.2 Översikt överföringar 18
4.3 Lämpliga skyddsåtgärder.... **Fel! Bokmärket är inte definierat.**
4.3.1 Andra/extra skyddsåtgärder..... **Fel! Bokmärket är inte definierat.**
4.4 Undantag i särskilda situationer..... **Fel! Bokmärket är inte definierat.**
4.5 Samlad bedömning..... **Fel! Bokmärket är inte definierat.**
5 Risker och åtgärder 18
5.1 Generella åtgärder 18
5.1.1 Generella tekniska åtgärder 19
5.1.2 Generella administrativa åtgärder 20
5.2 Bedömning av specifika risker 21
5.2.1 Riskmatris 23
5.3 Samlad bedömning av risker och åtgärder 23
5.3.1 Kvarstående höga risker? 24
5.3.2 Förhandssamråd 24
6 Medverkan från berörda parter 25
6.1 Kommentarer/rekommendationer från dataskyddsombudet... 25
6.2 Synpunkter från de registrerade 25
7 Avslut 25
7.1 Beslut 25
7.2 Nästa steg 25
8 Bilagor 26

1 Inledning

1.1 Bakgrund och behov av behandling/behandlingar

Göteborgs Stad ska ersätta det nuvarande intranätet med det nya Digitala navet. Intraservice är leverantör av Digitala navet som är en gemensam tjänst till övriga förvaltningar, däribland stadsfastighetsförvaltningen som nu ska införa intranätet.

Det finns ett behov av att kunna publicera kontaktuppgifter, information och liknande till medarbetare i ett arbetssyfte. Samtidigt är den personliga integriteten viktig och därför ändras tidigare intranät genom införandet av Digitala navet från att vara en delvis öppen webbplats till att bli en enbart intern webb.

Syftet med Digitala navet är att skapa nyttor för medarbetare, chefer och organisationen i stort genom att:

- tillgängliggöra information om arbetssätt, rättigheter och skyldigheter kopplat till anställning, stöd och support i arbetet, pågående uppdrag och förändringar i staden.
- möjliggöra för medarbetare att kunna ta del av aktuell information på förvaltningen och för hela Göteborgs Stad.
- möjliggöra informationsspridning vid kris eller större händelse.
- samla länkar och enkel tillgång till verktyg och IT-stöd.
- tillgängliggöra information om stadens organisation och struktur samt kontaktpersoner för olika frågor.
- stärka och bygga den gemensamma bilden av Göteborgs Stad.
- möjlighet för redaktör att slå på kommentarfunktion på inlägg i kommunikativa kanaler finns.

1.2 Behov av konsekvensbedömning

Enligt datsskyddsförordningen ska en konsekvensbedömning genomföras när en personuppgiftsbehandling innebär hög risk för de registrerade. Anställda är en utsatt användargrupp då de anses vara i beroendeställning till arbetsgivaren. Då samtliga anställda (runt 650 personer) inom stadsfastighetsförvaltningen ska använda sig av Digitala navet är det stor en volym personuppgifter som behandlas. Med denna bakgrund bör därför en konsekvensbedömning genomföras.

1.3 Deltagare och roller

Ange vilka som deltar i arbetet med konsekvensbedömningen och vilken roll de har.

Björn Alm, dataskyddssamordnare stadsfastighetsförvaltningen, Karin Mondet Larsson, lokal projektledare för införandet av Digitala navet hos stadsfastighetsförvaltningen, samt Fredrik Andersson, teknisk bakgrund intraservice.

1.4 Personuppgiftsansvar

Ange vem som är personuppgiftsansvarig för behandlingen/behandlingarna. Om det är flera självständiga personuppgiftsansvariga eller om det är ett gemensamt ansvar (för delar eller hela behandlingen/behandlingarna), ange detta.

Stadsfastighetsnämnden är personuppgiftsansvarig för personuppgiftsbehandlingarna i Digitala navet.

2 Beskrivning av behandlingen/ behandlingarna

Personuppgiftsbehandlingarna är:

1. **Informera och kommunicera med anställda genom intranät**
Ge medarbetare internt på förvaltningen och i hela staden kunskap om organisationen, arbetssätt och rutiner, rättigheter och skyldigheter som anställd, information om förändringsarbeten och vid kris, samt ge ökad delaktighet och ge möjlighet att skapa dialog och påverka. Dessa behandlingar ska ske i intranätet Digitala navet.

Utveckling och förvaltning av intranätet sker av intraservice för hela Göteborgs Stads användare, däribland stadsfastighetsförvaltningen. Behandlingen, där intraservice har personuppgiftsansvaret, finns i konsekvensbedömningen, se bilaga 3: *Intraservice Konsekvensbedömning enligt dataskyddsförordningen Personuppgiftsbehandling: Informera och kommunicera i Digitala navet samt Tillhandahålla och utveckla Digitala navet (Diarienummer 0564/22).*

2.1 Översiktlig beskrivning av behandlingen/behandlingarna

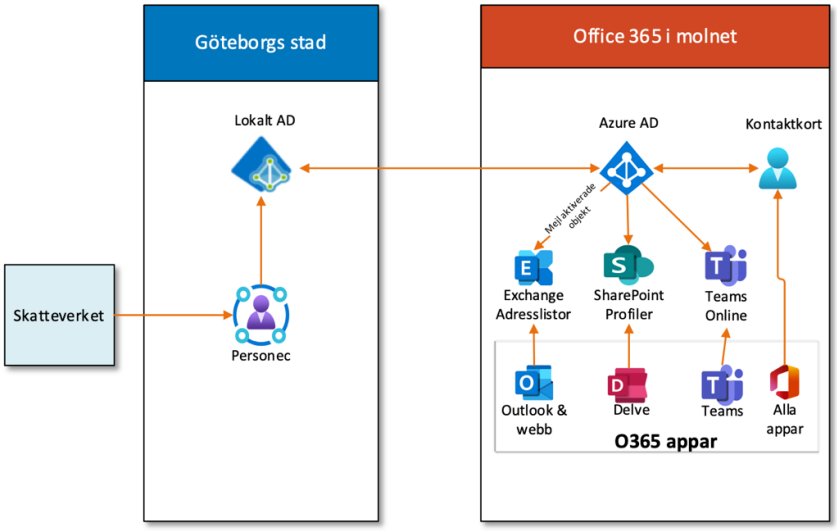
Stadsfastighetsförvaltningen är ansvarig för att producera kommungemensam information på ett antal sidor gällande verksamheten. Detta för att ge stadens medarbetare lättillgänglig information, samt för att ge stöd och vägledning inom fastighetsrelaterade frågor som planera, bygga, hyra in, förvalta och utveckla de lokaler och utemiljöer som Göteborgs Stads verksamheter behöver.

Stadsfastighetsförvaltningen ansvarar även för att som arbetsgivare ge medarbetare specifik information för förvaltningen, exempelvis information som rör anställningen eller krisinformation, tillvägagångssätt för olika typer av arbetsuppgifter, och nyheter om olika händelser och projekt inom förvaltningen. Det nya intranätet ska även ge ökad delaktighet samt möjlighet att påverka och skapa dialog hos anställda.

Digitala navet bygger på plattformen Sharepoint Online som är en del av Microsoft 365-plattformen inom Göteborgs Stad. När en användare loggar på sig på sin stadendator, har hen automatisk access till Microsoft 365 och till det Digitala navet.

Digitala navet hämtar uppgifter (förnamn, efternamn, e-postadress och av användaren publicerat foto) från den underliggande tjänsten Microsoft 365 (Delve/Azure) och publicering av sidor sker via den underliggande tjänsten Office365 (Sharepoint).

Personuppgifter publiceras i form av kontaktkort på sidor i Digitala navet. Uppgifter kommer från flera underliggande källor, som illustreras genom för kopplingen i O365 kontaktkortet, vilket finns genomgående i Microsoft 365-miljön.

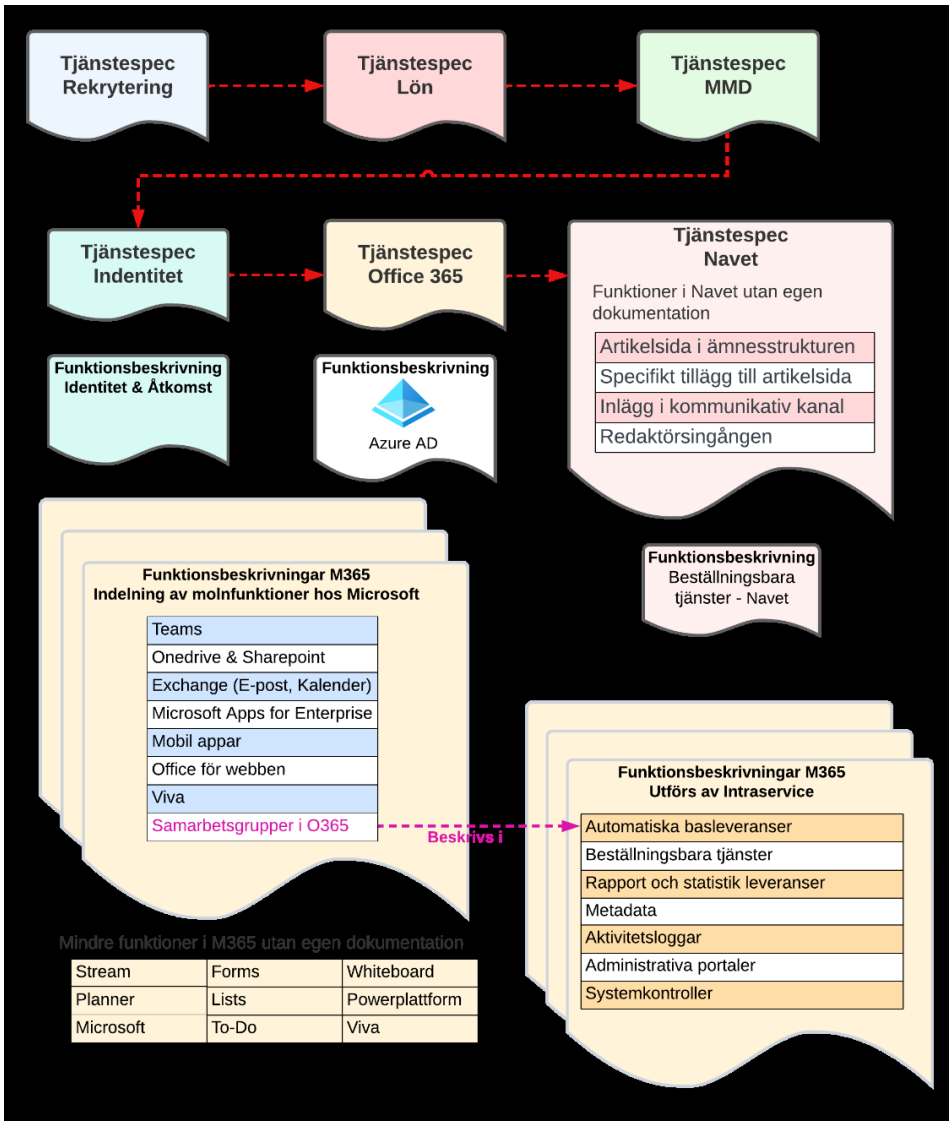


Hämtning av personuppgifter ur underliggande källor sker för att kvalitetssäkra och minimera risken för felaktiga personuppgifter.

Utöver inhämtning av personuppgifter från underliggande tjänster sker manuella tillägg där personuppgifter ska förekomma i redaktionellt bearbetade texter (exempel på detta kan vara av användaren publicerat namn, telefonnummer, foto, uppdrag/roll).

Dokumentation av olika delar, personuppgiftsflöden som ingår i Digitala navet beskrivs i ett stort antal dokument som förklarar hur tjänster fungerar med aspekter på säkerhet och dataskydd. Dokumentationen sker i två nivåer:

1. Tjänstespecifikationer (kopplad till intraservices tjänster – övergripande)
2. Funktionsbeskrivningar (underliggande funktioner som kan ingå i flera tjänster)



På startsidan för Digitala navet finns sju flikar: Service, support och stöd i arbetet, min anställning, ledning och styrning, organisation, stadsutveckling, kärnverksamheter samt aktuellt. Under dessa flikar finns sedan en rad artikelsidor där information om stadsfastighetsförvaltningens verksamheter.

På artikelsidor kommer det förekomma namn på kontaktpersoner och funktioner. De tre avdelningarna förvaltning och fastighetsutveckling, projekt och investering samt drift och underhåll kommer vara en viktig del in den information som kommer delas inom hela Göteborgs stad. Arbetet pågår med att ta fram vilken information med innehållande personuppgifter som ska göras tillgänglig via artikelsidorna för varje enhet tillsammans med kommunikationsenheten.

De personuppgifter som kan finnas med på det mer informativa artikelsidorna för verksamheterna är kontaktuppgifter som har hämtats från anställdas foto, telefonnummer, e-postadress uppdrag/roll.

Det kommer också publiceras nyheter om stadsfastighetsförvaltningens verksamhet där olika medarbetare eller chefer kan medverka. Texterna kommer delas med alla som har tillgång till Digitala navet. Utöver kontaktuppgifter och liknande kommer även andra personuppgifter förekomma i nyhetstexterna beroende på vad som ska förmedlas. Personuppgifter som kan förekomma är utbildning, tidigare arbeten, personliga förhållanden.

För att det redaktionella materialet ska hanteras på ett korrekt sätt tar stadsfastighetsförvaltningen fram en rutin för publicering och hantering av personuppgifter i Digitala navet. Rutinen kommer beröra vilka typer av personuppgifter som kan publiceras samt hur medverkan kan ske för anställda utifrån den rättsliga grunden allmänt intresse. Exempelvis kopplat till varje redaktionell publicering sker avstämning med den registrerade, för att säkerställa att innehållet är korrekt och publicerbart.

Samtliga publiceringsansvariga (redaktörer) genomgår även ett gediget utbildningspaket, bland annat för att säkerställa kunskap om hur man förhåller sig till personuppgifter. Utbildningen är en förutsättning för att få behörighet att publicera innehåll i Digitala navet.

Det finns olika behörighetsnivåer för redaktörer. Stadsfastighetsförvaltningens förvaltningsredaktör avgör vilken behörighet som ges till respektive redaktör på stadsfastighetsförvaltningen. Varje sida har en publiceringsansvarig (redaktör) som publicerar informationen och ansvarar för att informationen på sidan visas på korrekt sätt. Det finns även en innehållsansvarig för varje sida som ansvarar för att innehållet i informationen på sidan är korrekt.

2.1.1 Tillgångar

Informationsbärare och informationstillgångar är:

• Azure AD (hantering av behörighet och autentisering) – *se*

Funktionsbeskrivning Azure AD
• Sharepoint (publicering av sida) – *se Funktionsbeskrivning Sharepoint och Onedrive*
• Delve (presentation av organisatorisk information i Azure AD) – *se Funktionsbeskrivning Sharepoint och Onedrive*
• Digitala navet – se *Tjänstespecifikation Digitala navet*
• Office 365 - *se Tjänstespecifikation O365*
• Identitet och åtkomst, se *Tjänstespecifikation Identitet och Åtkomst*
• Kvalitetssäkrad information (Master Meta Data = MMD), Bilaga 4 – *Flöden - Digitala navet (O365, Identitet & Åtkomst, Lön samt MMD): bild 39. Personuppgiftsflöde MMD (Navet).*

Samtliga bilagor finns i Intraservice konsekvensbedömning som bifogas som kopia.

2.1.2 Personuppgiftsbiträden och underbiträden

Stadsfastighetsnämnden är personuppgiftsansvarig, intraservice är personuppgiftsbiträde och Microsoft är underbiträde med tjänsten M365.

2.1.3 Mottagare

Vid publicering av sidor och inlägg i kommunikativa kanaler (inklusive personuppgifter) i Digitala navet delas detta med förvaltningar och bolag i Göteborgs Stad. Då dessa lagras i Digitala navet och därmed Sharepoint delas den även med leverantören av plattformen (Microsoft).

2.2 Översikt behandling/behandlingar

Namn på behandling	Personuppgifter	Extra skyddsvärda person-uppgifter	Känsliga personuppgifter

<table>
<tr>
<td>Informera och kommunicera i intranätet</td>
<td>Manuella (redaktionella) tillägg: av användaren publicerat telefonnummer, foto, video, ljudupptagning, uppdrag/roll.

Utöver detta publicerar redaktör relevanta personuppgifter i kopplat till innehåll. Dessa uppgifter bestäms i samråd med den berörda personen.

En rutin för publicering och hantering av personuppgifter hos stadsfastighetsförvaltningen kommer tas fram. Rutinen kommer beröra vilka typer av personuppgifter som kan publiceras samt hur medverkan ska ske för anställda utifrån den rättsliga grunden allmänt intresse.

Generellt hanteras följande personuppgifter när användare använder Digitala navet:
<table>
<tr><th>Fält</th><th>Vad visas</th></tr>
<tr><td>Displayname</td><td>Förnamn + efternamn</td></tr>
<tr><td>First name</td><td>Förnamn</td></tr>
<tr><td>Last name</td><td>Efternamn</td></tr>
<tr><td>User principle name</td><td>E-postadress</td></tr>
<tr><td>Job title</td><td>Förvaltningsna-mn</td></tr>
<tr><td>Company name</td><td>Förvaltningsna-mn</td></tr>
<tr><td>Department</td><td>Förvaltningsna-mn</td></tr>
<tr><td>Manager</td><td>Chef</td></tr>
<tr><td>Email</td><td>E-postadress</td></tr>
<tr><td>AD-konto</td><td>Namn på kontot (staden-konto)</td></tr>
</table>
</td>
<td></td>
<td></td>
</tr>
</table>

2.2.1 Personuppgifter om lagöverträdelser

Nej det förekommer inte.

2.2.2 Kategorier av registrerade

Namn på behandling	Kategorier av registrerade
Informera och kommunicera i intranätet	Anställda på stadsfastighetsförvaltningen i Göteborgs Stad Konsulter med uppdrag inom stadsfastighetsförvaltningen och i Göteborgs Stad

2.2.3 Behandlingens/behandlingarnas omfattning

På stadsfastighetsförvaltningen finns cirka 650 anställda. Stadsfastighetsförvaltningen är hyresvärd till många andra verksamheter vilket innebär en stor efterfrågan på information. Potentiella personuppgifter som publiceras kan bli delade i hela staden vilket innebär att det kan spridas till över 50 000 användare i Digitala navet.

2.3 Ändamål

Namn på behandling	Ändamål
Informera och kommunicera i intranätet	Ändamålet är att informera och kommunicera via intranätet i syfte att ge service och stöd till anställda och konsulter inom förvaltningen och övriga verksamheter inom Göteborgs stad. Även möjliggöra informationsspridning vid kris eller större händelse.

2.4 Rättslig grund

Namn på behandling	Rättslig grund	Motivering och hänvisning
Informera och kommunicera i intranätet	Allmänt intresse	Enligt Göteborgs Stads policy för kommunikation (beslutad i kommunfullmäktige 2019-12-10) ska stadens intranät användas som den

		gemensamma kanalen för intern information och kommunikation.

2.4.1 Känsliga personuppgifter

Inga känsliga personuppgifter förekommer.

3 Behov/proportionalitet

3.1 Ändamålsbegränsning

Informera och kommunicera i intranätet
Samtliga publiceringsansvariga (redaktörer) genomgår ett gediget utbildningspaket, bland annat för att säkerställa kunskap om hur man förhåller sig till personuppgifter. Utbildningen är en förutsättning för att få behörighet att publicera innehåll i Digitala navet.

För att det redaktionella materialet ska användas på ett korrekt sätt tar stadsfastighetsförvaltningen fram en rutin för publicering och hantering av personuppgifter i Digitala navet. Rutinen kommer bland annat ta upp vilka personuppgifter som är aktuella och vad som ryms inom informera och kommunicera via intranätet för att minska risken för ändamålsglidning.

Det finns olika behörighetsnivåer för redaktörer. Stadsfastighetsförvaltningens förvaltningsredaktör avgör vilken behörighet som ges till respektive redaktör på stadsfastighetsförvaltningen.

Kopplat till varje redaktionell publicering sker avstämning med den registrerade, för att säkerställa att innehållet är korrekt och publicerbart.

Varje sida har:

• en publiceringsansvarig (redaktör) som publicerar informationen och ansvarar för att informationen på sidan visas på korrekt sätt.

• Samt en innehållsansvarig som ansvarar för att innehållet i informationen på sidan är korrekt.

3.2 Uppgiftsminimering

Kopplat till varje redaktionell publicering sker avstämning med eventuella registrerade, för att säkerställa att innehållet är korrekt.

Fält	Vad visas

Displayname	**Förnamn + efternamn**
First name	**Förnamn**
Last name	**Efternamn**
User principle name	**E-postadress**
Job title	**Förvaltningsnamn**
Company name	**Förvaltningsnamn**
Department	**Förvaltningsnamn**
Manager	**Chef**
Email	**E-postadress**
AD-konto	**Namn på konto (staden-konto)**

Redaktörer genomgår ett gediget utbildningspaket för att inte använda onödiga uppgifter. Där ingår delar som säkerställer kunskap om hur man förhåller sig till personuppgifter. Utbildningen är en förutsättning för att få behörighet att publicera innehåll i Digitala navet.

Det finns olika behörighetsnivåer för redaktörer. Intraservices ansvarig för Digitala navet avgör vilken behörighet som ges till respektive redaktör lokalt.

En rutin för personuppgiftsbehandling och publicering i Digitala navet tas fram hos stadsfastighetsförvaltningen. Där i beaktas bland annat hur personuppgifter ska behandlas i eget redaktionellt material i form av nyheter där exempel på detta kan vara av användaren publicerat namn, telefonnummer, foto, uppdrag/roll.

3.3 Lagringsminimering

Stadsfastighetsförvaltningen ska ta fram rutiner för förvaltning av innehåll. Rutinerna involverar en manuell livscykelhantering av innehållet i ämnesstrukturen. Årsvis kontaktas innehållsansvarig för att säkerställa att informationen på sidan är korrekt. Detta görs för allt gemensamt och lokalt innehåll hos stadsfastighetsförvaltningen.

Arbetet är påbörjat med en uppdaterad dokumenthanteringsplan för stadsfastighetsförvaltningen där processer för Digitala navet med arkivering och gallring ska finnas med. Dokumenthanteringsplanen kommer dock inte vara beslutad i nämnd vid lansering.

Alla som publicerar innehåll på Digitala navet måste ha utbildning, se Uppgiftsminimering 3.2.

3.4 Åtgärder som stärker de registrerades rättigheter

3.4.1 Informationsplikt

• Stadsfastighetsförvaltningen informerar om hur vi hanterar personuppgifter på den öppna webbplatsen goteborg.se, där finns den tillgänglig för såväl medarbetare som medborgare: Policyn kommer uppdateras så snart som möjligt för att lägga till eventuell information kopplat till Digitala navets lansering.

• Stadsfastigheters medarbetare informerar också om verksamhetens personuppgiftsbehandling via en länk i e-postsignaturen.

• När Digitala navet införs kommer anställda på stadsfastighetsförvaltningen få information för hur personuppgifter kommer behandlas. Det kommer hållas utbildningar och frågestunder för anställda.

• Information om hantering av anställda med sekretessmarkerade uppgifter i Digitala navet kommer också gå ut vid lanseringen. Även en fast information ska finnas lättillgängligt på Digitala navet.

• Vid anställning hos stadsfastighetsförvaltningen informeras den nya medarbetaren om hur förvaltningen hanterar dennes personuppgifter.

• För de som förekommer i Digitala navet sker publicering i samråd med berörd person (art 13). I den tillkommande rutinen för publicering och hantering av personuppgifter kommer det förtydligas vilka nivåer av anställda som kan medverka i nyhetsartiklar utifrån den rättsliga grunden allmänt intresse. Tydlig information kommer även finnas om rättslig grund och att i Digitala navet så publiceras inte artiklar utifrån den rättsliga grunden samtycke utan allmänt intresse.

3.4.2 Tillgång och dataportabilitet

De personuppgifter som behandlas i Digitala navet hämtas in ifrån de underliggande tjänsterna som digitala navet vilar på. Utöver detta kan en redaktör vid skapande av en sida påföra ytterligare information. Om uppgifter behöver flyttas hanteras detta av de underliggande tjänster där informationen lagras. Information som lagts in manuellt flyttas manuellt. Rätten till dataportabilitet för den registrerade är dock inte tillämpligt i de två aktuella personuppgiftsbehandlingarna då den rättsliga grunden inte bygger på avtal eller samtycke enligt artikel 20.

På goteborg.se: Så behandlar stadsfastighetsförvaltningen personuppgifter – Göteborgs Stad (goteborg.se), finns information om hur de registrerade ska göra för att få ut ett registerutdrag med sina uppgifter. Informationen kommer också finnas tillgänglig genom Digitala navet.

3.4.3 Rättelse och radering

Registerutdrag, rättelse, radering och begränsning av behandling hanteras efter begäran och enskilt ärende. Publiceringsansvarig kan rätta eller radera redaktionellt publicerat innehåll i Digitala navet. Beslut om hantering av individens rättigheter sker i enlighet med den fastställda delegationsordningen för stadsfastighetsförvaltningen. All hantering av information sker utifrån gällande lagar och styrande dokument. All radering av personuppgifter hanteras enligt arkivlagen och skall som huvudregel bevaras. Eventuella radering av personuppgifter sker i enlighet med gallringsbeslut exempelvis i form av en dokumenthanteringsplan. Arbetet är påbörjat med en uppdaterad dokumenthanteringsplan för stadsfastighetsförvaltningen där processer för Digitala navet ska finnas med, den kommer dock inte vara beslutad i nämnd vid lansering.

Alla sidor i Digitala navet har utsedda innehållsansvariga och publiceringsansvariga (redaktörer). På varje sida finns konataktformulär för att kontakta sidans innehållsansvarig eller publiceringsansvarig för synpunkter på innehållet eller presentation av informationen. Det går också att kontakta förvaltningsbrevlådan och dataskyddskontakter.

3.4.4 Invändningar och begränsning av behandlingen/behandlingarna

Alla sidor i Digitala navet har utsedda innehållsansvariga och publiceringsansvariga (redaktörer). På varje sida finns ett formulär man kan använda för att kontakta både sidans innehållsansvarig och publiceringsansvarig för synpunkter på innehållet eller presentation av informationen. Kontaktuppgifter till förvaltningsbrevlådan och dataskyddskontakt finns också. Publiceringsansvarig kan korrigera redaktionellt publicerat innehåll i Digitala navet. Beslut om hantering av individens rättigheter sker i enlighet med den fastställda delegationsordningen för stadsfastighetsförvaltningen.

3.4.5 Personuppgiftsbiträdesavtal och instruktioner

Något personuppgiftsbiträdesavtal har ännu inte tecknats med intraservice som personuppgiftsbiträde. I arbetet med anpassning till Göteborgs Stads nya riktlinje för styrning, samordning och finansiering av digital utveckling och förvaltningen pågår ett arbete med att ta fram PUB-avtal kopplat till Digitala navet. Digitala navet bygger på underliggande tjänster som finns inom Microsoft365. Avtal kopplat till Microsoft365 hanteras i ett huvudavtal, inte enskilt för Digitala navet. Detta inkluderar Microsofts personuppgiftsbiträdesavtal (Data Protection Addendum, DPA).

I kommunikation med intraservice finns ingen ny information om detta. Stadsfastighetsförvaltningen har inte någon möjlighet i praktiken att instruera intraservice som personuppgiftsbiträde i förhållande till Microsoft. Arbetet

med att få ett PUB-avtal på plats fortsätter under hösten men det är oklart om det kommer vara på plats vid lansering i början av december 2023.

Microsoft med M365 används av personuppgiftsbiträdet intraservice som underleverantör i leveransen av Sharepoint som Digitala navet baseras på. I denna konsekvensbedömning har två risker, kopplat till Microsoft som underleverantör, identifierats. Under avsnittet 4.1 beskrivs dessa risker som skulle kunna innebära att personuppgiftsansvarig förlorar kontrollen över vad som sker med personuppgifterna, vilket föranleder att stadsfastighetsförvaltningen inte kan leva upp till sina skyldigheter gentemot de registrerade enligt GDPR avseende de registrerades rätt till information och tillgång.

3.5 Samlad bedömning av behovet av och proportionaliteten hos behandlingen/behandlingarna

Digitala navet är ett nytt intranät som ska ersätta nuvarande intranät. Arbete med att utveckla det nya intranätet har pågått sedan 2019 för att möta Göteborgs Stads behov av relevant och kvalitetssäkrad information till stadens anställda och för att bättre uppfylla de krav tillgänglighetslagstiftningen ställer.

Digitala navet är den av kommunfullmäktige beslutade gemensamma kanalen för intern information och kommunikation. I Digitala navet ska anställda kunna ta del av information om arbetssätt, rättigheter och skyldigheter kopplat till anställning, stöd och support i arbetet, pågående uppdrag och förändringar i staden. Möjliggöra för medarbetare att kunna ta del av aktuell information på förvaltningen och för hela Göteborgs Stad samt informationsspridning vid kris eller större händelse.

För att tillhandahålla information och kommunikation via Digitala navet blir viss personuppgiftsbehandling nödvändig. Behandlingen medför vissa risker, exempelvis att redaktionellt material innehållande personuppgifter publiceras i form av nyhetsartiklar där anställda medverkande. För att säkerställa korrekt personuppgiftsbehandling kommer stadsfastighetsförvaltningen ge tydlig information till de registrerade om behandlingen. Det kommer även upprättas en rutin för publicering och personuppgiftsbehandling i Digitala navet.

Mot bakgrunden av behovet av relevant och kvalitetssäkrad information till anställda som når upp till tillgänglighetslagstiftningen bedöms fördelarna överstiga nackdelarna och behandlingen anses alltså vara proportionerlig.

4 Överföring av personuppgifter utanför EU/EES

4.1 Sker det en överföring av personuppgifter utanför EU/EES?

☒Ja

☐Nej

☒Risk för tredjelandsöverföring

Microsoft 365 är en SaaS-tjänst som levereras av Microsoft Corporation Inc. Lagring av innehållsdata sker inom EU, men överföring av vissa typer av metadata (funktionsdata och diagnosdata) sker till tredjeland, dvs Microsoft i USA samt till Microsofts underbiträden.

Sedan 1 januari 2023 genomför Microsoft införandet av EU-data boundry, vilket innebär att all data processas och lagras inom EU, inklusive metadata. Stora delar av metadatan är redan flyttade till EU, men det finns en backlog, som kommer att lösas under året.

Intraservice, som leverantör av Digitala navet, har i sin konsekvensbedömning (daterad 2023-06-14) för införandet av det nya intranätet tagit upp risker gällande Microsoft som underleverantör. Trots EU-kommissionens adekvansbeslut (10 juli 2023) så kvarstår vissa risker.

En potentiell risk är spridning av data till olämpliga underleverantörer på grund av ensidig förändring av vilka underleverantörer som används av Microsoft vilket ger en begränsad insyn. En annan identifierad risk är övervakning av anställda genom analys och statistik av Microsoft där det inte är utrett vem eller vilka som får ta del av dessa uppgifter. Det skulle kunna innebära att personuppgifter används till andra ändamål än ursprungsändamålet. Till konsekvensbedömningen som utförs hos stadsfastighetsförvaltningen har intraservice meddelat att de inte har någon ytterligare information gällande de två riskerna.

De två riskerna skulle kunna innebära att stadsfastighetsnämnden inte når upp till principer för behandling av personuppgifter i dataskyddsförordningen (artikel 5.1a och artikel 5.1b). Det skulle i förlängningen innebär att de registrerade inte får tillgång till eller information om vilka personuppgifter som behandlas (artikel 13 och 15).

4.2 Översikt överföringar

Beskriv varje identifierad överföring av personuppgifter till tredjeland.

Namn på behandling och var i behandlingen som överföringen sker	Vilka person-uppgifter?	Till vilket land överförs person-uppgifterna?	Finns det ett adekvans-beslut för mottagar-landet?
I behandlingen ”informera och kommunicera i intranätet” finns en risk för spridning av data till olämpliga underleverantörer på grund av ensidig förändring av vilka underleverantörer som används med dålig transparens av Microsoft.	Samtliga personuppgifter som behandlas i Digitala navet.	USA, Microsoft kan dock i sin tur dela uppgifter till andra länder.	Ja
I behandlingen ”informera och kommunicera i intranätet” finns en risk för en otillåten överföring då anställda skulle kunna övervakas genom analys och statistik av extern part där Microsoft använder informationen till andra ändamål än ursprungsändamålet.	Samtliga personuppgifter som behandlas i Digitala navet.	USA, Microsoft kan dock i sin tur dela uppgifter till andra länder.	Ja

5 Risker och åtgärder

5.1 Generella åtgärder

Risker vid delning av personuppgifter med underleverantören i den underliggande plattformen Microsoft Office 365, hanteras i riskanalys *O365 Riskanalys Dataskydd*, se bilagor Åtgärderna är kopplat till behandlingarna i Digitala navet.

5.1.1 Generella tekniska åtgärder

Ange vilka generella tekniska åtgärder som har införts eller planeras i syfte att minska eller eliminera de risker som identifierats.					
Genomförd	**Pågående**	**Planerad**	**Ej tillämplig**	**Åtgärd**	**Kommentar**
☒	☐	☐	☐	Autentisering	Digitala navet styrs genom behörighetsstyrning för publicering av innehåll.
☒	☐	☐	☐	Anti-malware	Ifrån underliggande funktion.
☐	☒	☐	☐	Detekteringsverktyg för personuppgiftsincidenter	Har ej fått information om detta från intraservice.
☒	☐	☐	☐	Säkerhetskopiering (backup)	Ifrån underliggande funktion.
☒	☐	☐	☐	Kryptering	Ifrån underliggande funktion.
☒	☐	☐	☐	Anonymisering	Ifrån underliggande funktion i MMD
☒	☐	☐	☐	Brandväggar	Ifrån underliggande funktion.
☒	☐	☐	☐	Detekteringsverktyg för intrång	Ifrån underliggande funktion.
☒	☐	☐	☐	Loggning	Ifrån underliggande funktion.
☒	☐	☐	☐	Logisk kontroll av åtkomst	Ifrån underliggande funktion.
☒	☐	☐	☐	Flerfaktorsautentisering	Ifrån underliggande funktion.
☒	☐	☐	☐	Nätverksautentisering	Ifrån underliggande funktion.
☒	☐	☐	☐	Pseudonymisering	Ifrån underliggande funktion.
☒	☐	☐	☐	Regelbundna mjukvaruuppdateringar (Patchning)	Ifrån underliggande funktion.
☒	☐	☐	☐	Detekteringsverktyg för sårbarheter	Ifrån underliggande funktion.
☒	☐	☐	☐	Mobile device management (MDM)	Ifrån underliggande funktion.
☐ **Inte säker** Kommentar: **Klicka eller tryck här för att ange text.**					
☐ **Annat** Kommentar: **Klicka eller tryck här för att ange text.**					

5.1.2 Generella administrativa åtgärder

Förutom de nedan generella administrativa åtgärderna kommer även stadsfastighetsförvaltningen införa en rutin för publicering och hantering av personuppgifter i Digitala navet. Rutinen kommer beröra vilka typer av personuppgifter som kan publiceras samt hur medverkan kan ske för anställda utifrån den rättsliga grunden allmänt intresse. Exempelvis kopplat till varje redaktionell publicering sker avstämning med den registrerade, för att säkerställa att innehållet är korrekt och publicerbart.

Ange de generella administrativa åtgärder som har införts eller planeras i syfte att minska eller eliminera de risker som identifierats.

Genomförd	Pågående	Planerad	Ej tillämplig	Åtgärd	Kommentar
☒	☐	☐	☐	Riktlinjer för datoranvändning	Göteborgs Stads regel för IT-användare
☒	☐	☐	☐	Utbildning och informationsinsatser	Utbildning för redatkör samt information till de registrerade under hösten inför lansering.
☐	☐	☒	☐	Kontinuitetsplan	Finns med i planen för kommande projekt på intraservice, utifrån anmärkningar i revisionsrapport 2021.
☐	☒	☐	☐	Incidenthanteringsplan	Finns rutiner för rappportering av personuppgiftsincidenter.
☐	☐	☒	☐	Katastrofberedskap (Disaster recovery plan)	Finns med i planen för kommande projekt på intraservice, utifrån anmärkningar i revisionsrapport 2021.
☐	☐	☐	☒	Behovsenlig behörighet (Need-to-know)	Publicerat innehåll är ämnat för hela staden. Dock är generell tillgång till Digitala navet behörighetsstyrd.
☒	☐	☐	☐	Sekretessavtal	Förvaltningsspecifika sekretessavtal skrivs under vid anställning. Förvaltningsspecifika sekretessavtal för konsulter skrivs under vid uppdragsstart.
☒	☐	☐	☐	Lösenordspolicy	

☐	☐	☐	☒	Penetrationstestning	Penetrationstestning sker på Microsoft M365-miljö, men inte applicerbart direkt.
☒	☐	☐	☐	Säkra fysiska lokaler	
☒	☐	☐	☐	Tillsyn/interna kontroller	Exempelvis genomförs efterlevnadskontroll en gång per år (efterlevnad av stadens styrande dokument)
☒	☐	☐	☐	Övervakning	Övervakning ur ett tekniskt perspektiv
☐	☐	☒	☐	Simulerings- och krisövningar	Finns med i planen för kommande projekt på intraservice, utifrån anmärkningar i revisionsrapport 2021.
☒	☐	☐	☐	Bakgrundskontroller	Utförs vid behov.
☒	☐	☐	☐	Åtkomstkontroll	Kontroll utförs vid fysisk åtkomst, behörighetskontroll för tillgång till Digitala navet och underliggande tjänster samt loggning av åtkomst.
☒	☐	☐	☐	Leverantörskontroller	
☐	☐	☐	☒	Riktlinjer för hantering av fysiska handlingar	Inga fysiska handlingar finns i Digitala Navet.
☐	☒	☐	☐	Arkivering	I enlighet med förvaltningens dokumenthanteringsplan samt regionarkivets anvisning för webbarkivering som är under uppdatering.
☐ **Inte säker** Kommentar: Klicka eller tryck här för att ange text.					
☐ **Annat** Kommentar: Klicka eller tryck här för att ange text.					

5.2 Bedömning av specifika risker

Efter riskbedömning har 32 risker identifierats i samband med de två personuppgiftsbehandlingarna. Totalt fem riskvärden bedöms som medelhöga respektive höga.

Risk -ID	Beskrivning av risk	Vidtagna skyddsåtgärder	Nytt risk-värde
8	PUA-/PUB-förhållanden inom Göteborgs stad är under utredning vilket kan leda till en annan biträdessituation.	Utredning pågår för att ta fram riktlinjer för hur personuppgiftsbehandlingar ska fungera i stadengemensamma tjänster som intraservice tillhandahåller.	6
10	Övervakning av anställda genom analys och statistik av extern part (Microsoft).	Intraservice har ej återkopplat vilka skyddsåtgärder som genomförts.	9
12	Tillgång/behandling AD/Azure AD kan användas för olämpliga ändamål.	Utreda vilken åtgärd som går att genomföra. Om möjligt, avgränsa tillgången till AAD och begränsa så att isa klienter inte går att installera. Intraservice har ej återkopplat vilka åtgärder som genomförts.	6
17	Spridning av data till olämpliga underleverantörer på grund av ensidig förändring av vilka underleverantörer som används med dålig transparens av Microsoft.	En skyddsåtgärd som är under utredning är att ett förtydligande bör inhämtas från Microsoft om vilka underleverantörer som avnänds för att säkerställa att personuppgifter ej sprids utanför EU/EES eller där det finns adekvansbeslut.Någon ny information finns inte så risken kvarstår på samma nivå.	9
23	Skapa anställning - utlämnande av personuppgifter av medarbetare själv eller under påtryckning från annan lämnar ut uppgifter.	Intraservice har ej återkopplat vilka skyddsåtgärder som genomförts.	6
27	Skadlig kod laddas upp i filarkviet och kan få stor spridning på grund av Digitala navet är en trovärdig källa.	Intraservice har ej återkopplat vilka skyddsåtgärder som genomförts.	6

5.2.1 Riskmatris

Detta avsnitt är en illustration av hur riskmatrisen ser ut och hur riskvärdena fördelar sig baserat på hur riskerna har bedömts i excelfilen. Ni behöver alltså inte fylla i något under detta avsnitt.

KONSEKVENS	Mycket allvarlig	4	8	12	16
	Allvarlig	3	6	9	12
	Måttlig	2	4	6	8
	Försumbar	1	2	3	4
		Osannolikt	Möjligt	Sannolikt	Mycket sannolikt
SANNOLIKHET					

5.3 Samlad bedömning av risker och åtgärder

Risknivåerna för den information som publiceras i Digitala navet och som delas inom Göteborgs Stad bedöms som låga. Det kommer exempelvis inte delas några känsliga personuppgifter (artikel 9).

Flera risker har sänkts till låga nivåer med hjälp av utbildningsinsatser för personer som är redaktörer och publicerar artiklar, nyheter, utbildningsmaterial och liknande i Digitala navet. Stadsfastighetsförvaltningen kommer även ta fram rutiner för personuppgiftsbehandling och publicering i det nya intranätet vilket också har sänkt risknivåer.

Det finns dock risker som ej har hanterats utifrån den information som varit tillgänglig vid denna konsekvensbedömning. Det gäller dels risker som intraservice identifierade i sin konsekvensbedömning (daterad 2023-06-23). Där finns ett drygt tiotal risker som saknar skyddsåtgärder och det är oklart om dessa har hanterats på adekvat sätt. En övervägande majoritet av dessa risker är på en lägre nivå.

Två av de kvarvarande har en hög risknivå (risk 10 och 17) och trots skyddsåtgärder har det inte varit möjligt att få till stånd sänkningar. För att få till stånd sänkningar krävs att Microsoft har en större transparens om vilka underleverantörer som använder samt att de informerade i större utsträckning om hur analys och statistik används och delas vidare med underleverantörer. Intraservice har som personuppgiftsbiträde och leverantör av Digitala navet kommunicerat detta till Microsoft men det finns ingen ny information att ge i dagsläget.

Som tidigare behandlat i avsnittet 4.1 så kvarstår risker gällande tredjelandsöverföring. De två riskerna skulle kunna innebära att stadsfastighetsnämnden inte når upp till principer för behandling av personuppgifter i dataskyddsförordningen (artikel 5.1a och artikel 5.1b). Och i förlängningen skulle det kunna innebära att de registrerade inte får tillgång till personuppgifter eller information om vilka personuppgifter som behandlas (artikel 13 och 15).

I kommunikation med intraservice har de höga risknivåerna påtalats. Som personuppgiftsbiträde har de inte lämnat någon ny information från Microsoft som underleverantör.

5.3.1 Kvarstående höga risker?

Risk 10 - Övervakning av anställda genom analys och statistik av extern part, i detta fall Microsoft.

Risk 17 - Spridning av data till olämpliga underleverantörer på grund av ensidig förändring av vilka underleverantörer som används med dålig transparens av Microsoft.

5.3.2 Förhandssamråd

Stadsfastighetsnämnden fattar beslut om personuppgiftsbehandlingen i Digitala navet vid sitt nämndsammanträde 2023-10-26.

6 Medverkan från berörda parter

6.1 Kommentarer/rekommendationer från dataskyddsombudet

Se bilaga 2.

6.2 Synpunkter från de registrerade

Om de registrerade har tillfrågats angående behandlingen ska deras synpunkter redogöras för här. Om de inte har tillfrågats, ange varför så inte har skett.

Synpunkter från de registrerade har ej inhämtats. Dock har information om och samverkan med fackliga organisationer skett sedan en tidsplan för införandet av Digitala navet startade under 2022.

7 Avslut

7.1 Beslut

Stadsfastighetsnämnden fattar beslut om personuppgiftsbehandlingen i Digitala navet vid sitt nämndsammanträde 2023-10-26.

7.2 Nästa steg

Beskriv vilket/vilka steg som ska tas härnäst.

Klicka eller tryck här för att ange text.

8 Bilagor

Bilaga 1 – Riskbedömning

Bilaga 2 – Dataskyddsombudets rekommendationer

Bilaga 3 – Intraservice Konsekvensbedömning enligt dataskyddsförordningen Personuppgiftsbehandling: Informera och kommunicera i Digitala navet samt Tillhandahålla och utveckla Digitala navet (Diarienummer 0564/22).

Mall framtagen av dataskyddsenheten (version 1)

Telefon: 031-365 00 00 (kontaktcenter)
E-post: dso@intraservice.goteborg.se

Senast uppdaterad 2022-09-25

Riskbedömning införa nytt intranät stadsfastighetsförvaltningen

Identifiering och bedömning av risker

Bedöm hur allvarliga och sannolika riskerna är på skalan 1–4.

Konsekvens
1 = Försumbar 2 = Måttlig 3 = Allvarlig 4 = Mycket allvarlig

Sannolikhet
1 = Osannolikt 2 = Möjligt 3 = Sannolikt 4 = Mycket sannolikt

Risk-ID	Namn på behandling	**Risk** *Obehörig åtkomst till personuppgifter, oönskad ändring av personuppgifter, förlust av personuppgifter eller annan form av risk*	Beskrivning av risk	Konsekvenserna av risken för den registrerade	Konsekvens	Sannolikhet	Riskvärde	Vidtagna skyddsåtgärder	Konsekvens efter åtgärd	Sannolikhet efter åtgärd	Riskvärde efter åtgärder	Uppföljning av vidtagna åtgärder ska göras
1	Informera och kommunicera i intranät	Annan form av risk	Risk att person utsätts för hot eller negativ uppmärksamhet efter publicering av kontaktuppgifter i samband med text som uppfattas negativt.	Kan leda till obehag eller hot mot kontaktperson.	3	1	3	Utbildning av redaktörer som publicerar texter i Digitala navet. I första hand ska förvaltningsbrevlådor användas för kontaktuppgifter.	2	1	2	
2	Informera och kommunicera i intranät	Annan form av risk	Risk att information publiceras som ej bör publiceras.	Risk för att personuppgifter sprids.	2	1	2	Utbildning av redaktörer som publicerar texter i Digitala navet. Samråd med berörd person innan text som innehåller personuppgift publiceras. Rutin för vilka personuppgifter som får publiceras tas fram.	1	1	1	
3	Informera och kommunicera i intranät	Annan form av risk	Risk att personuppgifter ligger kvar för länge.	Gammal information som kan vara inaktuell och som bör gallras ligger kvar.	1	2	2	Rutiner för att rensa och kontrollera all information på Digitala navet och kopplas till dokumenthanteringsplan.	1	1	1	
4	Informera och kommunicera i intranät	Annan form av risk	Övervakning av persons aktiviteter.	Otillåten övervakning av användare genom metadata. Chef övervakar anställda och anställda övervakar varandra.	3	2	6	Komminucera information till de registrerade för att minska risk. Gärna specifikt just-in-time.	1	1	1	
5	Informera och kommunicera i intranät	Obehörig åtkomst till personuppgifter, oönskad ändring av personuppgifter samt förlust av personuppgifter	Användare beställer felaktigt redaktörsbehörigheter i serviceportalen. Spårbarhet finns.	Individ kan inte lita till information.	2	2	4	Utbildning och tydlig rollfördlening vem som har redaktörsroll. Krav ställs på förvaltningsredaktör för behörigheter innan de godkänner.	2	1	2	
6	Informera och kommunicera i intranät	Förlust av kontroll av personuppgifter	Kommentarer på nyhetsinlägg kan användas felaktigt. Alla användare kan lämna kommentarer om funktionen är påslagen.	Obehag för aktuell person. Spridning av personuppgift utanför personens kontroll.	2	2	4	Funktionen för kommentarer är avslagen som standard och används ej inom stadsfastighetsförvaltningen.	2	1	2	
7	Informera och kommunicera i intranät	Annan form av risk	Risk för otydlig eller otillräcklig information till de registrerade.	Avsaknad av eller undermålig info gör att den registrerade kan inte utöva sina fri- och rättigheter.	2	2	4	Ge information de registrerade inför lansering av Digitala navet samt vid nyanställningar. Översyn av den information som finns på stadsfastigheters sida på goteborg.se samt vilken information som ska skickas ut inför lansering.	2	1	2	
8	Informera och kommunicera i intranät	Annan form av risk	PUA-/PUB-förhållanden inom Göteborgs stad är under utredning vilket kan leda till en annan biträdessituation.	Oklart vem som är PUA eller PUB.	2	3	6	En utredning pågår för att ta fram riktlinjer för hur personuppgiftsbehandlingar ska fungera i stadengemensamma tjänster som intraservice tillhandahåller.	2	3	6	.

9	Informera och kommunicera i intranät	Förlust av kontroll av personuppgifter	Information raderas ej från metadata, utan stannar kvar eftersom metadata är relaterat till objektet. Det kan leda till att otillräcklig gallring och kontroll över PUB samt oklara villkor avtal.	Förlust av kontroll över personuppgifter. Kan inte neka behandling.	1	3	3	Intraservice har ej återkopplat vilka skyddsåtgärder som genomförts.	1	3	3	
10	Informera och kommunicera i intranät	Förlust av kontroll av personuppgifter	Övervakning av anställda genom analys och statistik av extern part (Microsoft).	Förlust av kontroll över personuppgifter.	3	3	9	Intraservice har ej återkopplat vilka skyddsåtgärder som genomförts.	3	3	9	
11	Informera och kommunicera i intranät	Annan form av risk	Personer med sekretessmarkering riskerar att synliggörs under pågående anställning.	Känsliga personuppgifter skyddas inte tillräckligt.	4	3	12	Svår lösning i Digitala navet, utan hanteras utanför. En stark skyddsåtgärd är att ta bort användarens konto och skapa ett nytt (med pseudonym, likt de som har sekretessmarkering sedan tidgare). Från stadsfastigheters sida lämnas tydlig information till de registrerade i samband med lansering och nyanställningar samt övergripande information gällande Digitala navet och personer med sekretessmarkering.	4	1	4	
12	Informera och kommunicera i intranät	Annan form av risk	Tillgång/behandling AD/Azure AD kan användas för olämpliga ändamål.	Ändamålsglidning av personuppgifter. Läsa bearbeta, utlämna personuppgifter till alla användare	2	3	6	Utreda vilken åtgärd som går att genomföra. Om möjligt, avgränsa tillgången till AAD och begränsa så att isa klienter inte går att installera. Intraservice har ej återkopplat vilka åtgärder som genomförts.	2	3	6	
13	Informera och kommunicera i intranät	Förlust av kontroll av personuppgifter	Tilldelning av licens för opersonliga/gruppkonton på grund av manuell kontoadministration eftersom ett gruppkonto kan användas och då saknas det spårbarhet vem som tar ut information.	Det saknas spårbarhet vem som tar ut personuppgifter.	1	3	3	Intraservice har ej återkopplat vilka skyddsåtgärder som genomförts.	1	3	3	
14	Informera och kommunicera i intranät	Annan form av risk	Tillgänglighet Digitala Navet, utan licens går det ej att komma åt plattformen.	Otillåten/okontrollerad informationsspridning genom att andra sätt används än Digitala navet.	2	2	4	Intraservice har ej återkopplat vilka skyddsåtgärder som genomförts.	2	2	4	
15	Informera och kommunicera i intranät	Obehörig åtkomst till personuppgifter, oönskad ändring av personuppgifter	Intrång av obehöriga SQL i Azure för provensionering genom cyberintrång där man kan skapa nya behörigheter.	Osäkerhet för registrerades personuppgifter	3	1	3	Intraservice har ej återkopplat vilka skyddsåtgärder som genomförts.	3	1	3	
16	Informera och kommunicera i intranät	Obehörig åtkomst till personuppgifter, oönskad ändring av personuppgifter samt förlust av personuppgifter	Virus i Outlook och Teams kan ge attack av skadlig kod. Externt (antagonistiskt hot) med problem i miljön och datorer så resurser inte kan användas.	Osäkerhet för registrerades personuppgifter	2	2	4	Intraservice har ej återkopplat vilka skyddsåtgärder som genomförts.	2	2	4	
17	Informera och kommunicera i intranät	Obehörig åtkomst till personuppgifter	Spridning av data till olämpliga underleverantörer på grund av ensidig förändring av vilka underleverantörer som används med dålig transparens av Microsoft.	Spridning av data till olämplig underleverantörer vilket kan leda till förlust av kontroll av personuppgifter.	3	3	9	En skyddsåtgärd som är under utredning är att ett förtydligande bör inhämtas från Microsoft om vilka underleverantörer som avnänds för att säkerställa att personuppgifter ej sprids utanför EU/EES eller där det finns adekvansbeslut.Någon ny information finns inte så risken kvarstår på samma nivå.	3	3	9	
18	Informera och kommunicera i intranät	Förlust av kontroll av personuppgifter	Lista över alla sidor i Digitala navet för åtkomst genom information om vilka sidor redaktörer eller innehållsansvariga skapat själva	Ökad tillgänglighet, oönskad spridning av personuppgifter och därmed lättare att komma åt.	2	2	4	En skyddsåtgärd som är under utredning är kommunicera till de registrerade. Intraservice har dock inte återkopplat status.	2	2	4	

19	Informera och kommunicera i intranät	Förlust av kontroll av personuppgifter	Listan över ansvarig per förvalning används/visar vilka sidor redaktörer eller innehållsansvariga skapa och felaktig information sprids genom kapning/påverkan för att sprida missinformation.	Ökad tillgänglighet, oönskad spridning av personuppgifter och därmed lättare att komma åt. Förvrängning, lämna ut falsk information om en individ negativt som påverkar hur hen uppfattas av andra.	2	2	4	En skyddsåtgärd som är under utredning är kommunicera till de registrerade. Intraservice har dock inte återkopplat status.	2	2	4	
20	Informera och kommunicera i intranät	Förlust av kontroll av personuppgifter	Personuppgifter kvarstår efter redaktör slutat, eftersom metadata innehåller referenser till personer (redaktörer) som inte blir gallrade (om det ska gallras pga av det är av ringa betydelse).	Bevarar personuppgifter längre än nödvändigt som kan påverka hur en individ uppfattas av andra.	1	3	3	Intraservice har ej återkopplat vilka skyddsåtgärder som genomförts.	2	2	4	
21	Informera och kommunicera i intranät	Exkludering - personer som ska ha information får det inte	Felaktigt personnummer skapas vid vid anställning och medarbetare ej får rätt uppgifter/konto.	Personnummer kommer inte bli upplagd i lönesystemet eller övriga syste (AD/osv)	1	1	1	Intraservice har ej återkopplat vilka skyddsåtgärder som genomförts.	1	1	1	
22	Informera och kommunicera i intranät	Obehörig åtkomst till personuppgifter	Skapa anställning - utlämnande av personuppgifter av medarbetare själv eller under påtryckning från annan lämnar ut uppgifter.	Avslöjande - Lämna ut informationen om en person som negativt påverkar säkerheten.	3	2	6	Intraservice har ej återkopplat vilka skyddsåtgärder som genomförts.	3	2	6	
23	Informera och kommunicera i intranät	Obehörig åtkomst till personuppgifter, oönskad ändring av personuppgifter	Skapa anställning - Anställd med hög behörighet manipulerar anställningsinformation.	Osäkerhet - personuppgifter skyddas inte till räckligt och utsätts för risk.	2	1	2	Intraservice har ej återkopplat vilka skyddsåtgärder som genomförts.	2	1	2	
24	Informera och kommunicera i intranät	Exkludering - personer med åtkomst får inte det, oönskad ändring av personuppgifter	Kontaktkort fylls i med olämplig fritext i artikelsidor eller nyhetsinlägg i sidor i sharepoint och kontaktkort.	Internt - medarbetare får fel information. Externt - eventuell otillbörlig påverkan/it-säkerheten.	2	1	2	Ett godkännande behöver ske (approval-flöde) innan en nyhet publiceras. Filer som ska bifogas kontrolleras av en person.	2	1	2	
25	Informera och kommunicera i intranät	Exkludering - personer med åtkomst får inte det, oönskad ändring av personuppgifter	Felaktig information används i kontaktformulären till publiceringsansvarig och innehållsansvarig hamnar därför fel.	Fel person får riktade frågor till sidansvarig.	1	2	2	Ett godkännande behöver ske (approval-flöde) innan en nyhet publiceras. Filer som ska bifogas kontrolleras av en person.	1	2	2	
26	Informera och kommunicera i intranät	Förlust av kontroll av personuppgifter	Kommentarer på nyhetsinlägg kan användas felaktigt. Alla användare kan läman kommentarer om funktionen är påslagen.	Internt - om kommentatorsflödet är aktiverat kan alla användare kommentera på nyheten, känsliga uppgifter kan spridas.	3	2	6	Kommentatorsfunktion är ej påslagen som standard och behöver aktiveras. Bevakning av kommentarer dagligen i en moderatorsfunktion.	3	1	3	
27	Informera och kommunicera i intranät	Obehörig åtkomst till personuppgifter, oönskad ändring av personuppgifter samt förlust av personuppgifter	Skadlig kod laddas upp i filarkviet och kan få stor spridning på grund av Digitala navet är en trovärdig källa.	Skadlig kod kan spridas med olika nivåer av påverkan beroende på vilken skadlig kod som laddas upp och sprids.	3	2	6	Intraservice har ej återkopplat vilka skyddsåtgärder som genomförts.	3	2	6	
28	Informera och kommunicera i intranät	Obehörig åtkomst till personuppgifter, oönskad ändring av personuppgifter samt förlust av personuppgifter	Scopet av personuppgifter ändras för säkerhetsåtgärder på avsaknad av att process saknas, liksom definitioner för scopet. Bristande definitioner, otydliga krav och bristande information.	Osäkerhet - personuppgifter skyddas inte till räckligt och utsätts för risk. Uteslutning - personuppgifter behandlas utan individens vetskap eller delaktighet.	2	3	6	Skapa en process, regelverk på förvaltningen med anvisning för säkerhetsändamål så att det finns tydliga kravställningar. Information till de registrerade om vad som sker för att upprätthålla säkerhet i Digitala navet.	2	2	4	
29	Informera och kommunicera i intranät	Förlust av kontroll av personuppgifter	Användaren har inte medvetenhet om uppgifter som loggas av intraservice och loggning av vilka sidor som besöks.	Användaren exkluderas och kan uppleva övervakning. Utelslutning - Personuppgifter behandlas utan individens vetskap.	2	2	4	Information till den registrerade om vad som sker för att upprätthålla säkerhet i Digitala navet.	2	1	2	
30	Informera och kommunicera i intranät	Förlust av kontroll av personuppgifter	Det saknas information om vilken data Microsoft behöver för att upprätthålla säkerhet.	Avsaknad av information. Uteslutning - personuppgifter behandlas utan individens vetskap eller delaktighet.	3	2	6	Undersöka vilka åtgärder MS utför genom dialog.	3	1	3	
31	Informera och kommunicera i intranät	Sekundäranvändning	Microsoft anseriga vara PUA för personuppgifter för säkerhet. De kan hitta nya säkerhetslösningar genom AI eller sammanställningar som skulle kunna lämnas ut till tredje part.	Avsaknad av information. Uteslutning - personuppgifter behandlas utan individens vetskap eller delaktighet.	2	2	4	Undersöka vilka åtgärder MS utför genom dialog.	2	1	2	
32	Informera och kommunicera i intranät	Förlust av kontroll av personuppgifter	För mycket aggregerad data i loggen (M365-loggarna ingår i logghantering).	Ev insamling av för mycket info från användare, samt för vid åtkomst. Aggregering - kombinerar olika typer av personuppgifter (inkl profilering).	2	2	4	Undersöka vilka åtgärder MS utför genom dialog.	2	1	2	

33	Informera och kommunicera i intranät	Annan form av risk	Oklar biträdessituation med intraservice som leverantör och personuppgiftsbiträde och stadsfastighetsförvaltningen som personuppgiftsansvarig.	Oklar ansvarsfördelning som kan påverka de registrerades rättigheter.	2	2	4	I sitt uppdrag att tillhandahålla Digitala navet som tjänst har Intraservice fått i uppdrag att utreda ansvarsförhållandet för Digitala navet.	1	1	1	

Senast uppdaterad 2022-08-24

Sammanställning av identifierade risker

I tabellen nedan visas en sammanställning av de risker ni identifierat i riskbedömningen med det risktal som gäller efter vidtagna åtgärder.

Risk-ID	Beskrivning av risk	Konsekvens efter åtgärd	Sannolikhet efter åtgärd	Risktal
1	Risk att person utsätts för hot eller negativ uppmärksamhet efter publicering av kontaktuppg	2	1	2
2	Risk att information publiceras som ej bör publiceras.	1	1	1
3	Risk att personuppgifter ligger kvar för länge.	1	1	1
4	Övervakning av persons aktiviteter.	1	1	1
5	Användare beställer felaktigt redaktörsbehörigheter i serviceportalen. Spårbarhet finns.	2	1	2
6	Kommentarer på nyhetsinlägg kan användas felaktigt. Alla användare kan lämna kommentare	2	1	2
7	Risk för otydlig eller otillräcklig information till de registrerade.	2	1	2
8	PUA-/PUB-förhållanden inom Göteborgs stad är under utredning vilket kan leda till en annan	2	3	6
9	Information raderas ej från metadata, utan stannar kvar eftersom metadata är relaterat till ob	1	3	3
10	Övervakning av anställda genom analys och statistik av extern part (Microsoft).	3	3	9
11	Personer med sekretessmarkering riskerar att synliggörs under pågående anställning.	4	1	4
12	Tillgång/behandling AD/Azure AD kan användas för olämpliga ändamål.	2	3	6
13	Tilldelning av licens för opersonliga/gruppkonton på grund av manuell kontoadministration e	1	3	3
14	Tillgänglighet Digitala Navet, utan licens går det ej att komma åt plattformen.	2	2	4
15	Intrång av obehöriga SQL i Azure för provensionering genom cyberintrång där man kan skapa	3	1	3
16	Virus i Outlook och Teams kan ge attack av skadlig kod. Externt (antagonistiskt hot) med prob	2	2	4
17	Spridning av data till olämpliga underleverantörer på grund av ensidig förändring av vilka und	3	3	9
18	Lista över alla sidor i Digitala navet för åtkomst genom information om vilka sidor redaktöre	2	2	4
19	Listan över ansvarig per förvalning används/visar vilka sidor redaktörer eller innehållsansvarig	2	2	4
20	Personuppgifter kvarstår efter redaktör slutat, eftersom metadata innehåller referenser till pe	2	2	4
21	Felaktigt personnummer skapas vid vid anställning och medarbetare ej får rätt uppgifter/konto.	1	1	1
22	Skapa anställning - utlämnande av personuppgifter av medarbetare själv eller under påtryckning från annan lämnar ut uppgifter.	3	2	6
23	Skapa anställning - Anställd med hög behörighet manipulerar anställningsinformation.	2	1	2
24	Kontaktkort fylls i med olämplig fritext i artikelsidor eller nyhetsinlägg i sidor i sharepoint och kontaktkort.	2	1	2
25	Felaktig information används i kontaktformulären till publiceringsansvarig och innehållsansvarig hamnar därför fel.	1	2	2
26	Kommentarer på nyhetsinlägg kan användas felaktigt. Alla användare kan läman kommentarer om funktionen är påslagen.	3	1	3
27	Skadlig kod laddas upp i filarkviet och kan få stor spridning på grund av Digitala navet är en trovärdig källa.	3	2	6
28	Scopet av personuppgifter ändras för säkerhetsåtgärder på avsaknad av att process saknas, liksom definitioner för scopet. Bristande definitioner, otydliga krav och bristande information.	2	2	4
29	#REFERENS!	#REFERENS!	#REFERENS!	#REFERENS!
30	Användaren har inte medvetenhet om uppgifter som loggas av intraservice och loggning av vilka sidor som besöks.	2	1	2
31	Det saknas information om vilken data Microsoft behöver för att upprätthålla säkerhet.	3	1	3
32	Microsoft anseriga vara PUA för personuppgifter för säkerhet. De kan hitta nya säkerhetslösningar genom AI eller sammanställningar som skulle kunna lämnas ut till tredje part.	2	1	2
33	För mycket aggregerad data i loggen (M365-loggarna ingår i logghantering).	2	1	2
34	#REFERENS!	#REFERENS!	#REFERENS!	#REFERENS!
35	Oklar biträdessituation med intraservice som leverantör och personuppgiftsbiträde och stadsfastighetsförvaltningen som personuppgiftsansvarig.	1	1	1

2023-10-10 Stadsmiljöförvaltningen

Dataskyddsombudets rekommendationer

Konsekvensbedömning: Informera och kommunicera i intranät

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

Stadsfastighetsförvaltningen har lämnat en detaljerad redogörelse för personuppgifts-behandlingen, där det framgår hur den ska gå till samt dess innehåll och omfattning. Behandlingen är tydligt beskriven och dataskyddsombudet har inget att tillägga i denna del.

[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 bedömning av behovet av och proportionaliteten hos behandlingen

Förvaltningen redogör här för de överväganden som gjorts för att beskriva behovet av behandlingen och varför den är proportionerlig. Verksamheten redogör också för den rättsliga grunden för behandlingen.

Enligt den av fullmäktige beslutade policyn för Göteborgs Stads kommunikation framgår att stadens intranät ska användas som den gemensamma kanalen för intern information och kommunikation för att tillgängliggöra information om arbetssätt, rättigheter och skyldigheter kopplat till anställning, stöd och support i arbetet, pågående uppdrag och förändringar i staden. Vidare ska intranätet möjliggöra för medarbetare att kunna ta del av aktuell information på den enskilda förvaltningen och för hela Göteborgs Stad, samt möjliggöra informationsspridning vid kris eller större händelse.

Dataskyddsombudet delar förvaltningens uppfattning om att behandlingen så som den beskrivs är både proportionerlig och nödvändig för att utföra en uppgift av allmänt intresse. Ändamålet är tydligt avgränsat och förvaltningen har vidtagit adekvata uppgifts- och lagringsminimerande åtgärder i form av utbildningsinsatser och rutiner för de som publicerar innehåll i Digitala Navet, alternativt föreslagit åtgärder som kommer implementeras, till exempel gällande dokumenthanteringsplaner. Dataskyddsombudets bedömning är därför att behandlingen, under förutsättning att den utförs så som beskrivits och att relevanta åtgärder införs, uppfyller kraven på proportionalitet och nödvändighet.

Hantering av risker för de registrerades rättigheter och friheter

Behandlingen omfattar ett stort antal personer, anställda inom stadsfastighets-förvaltningen, som i kraft av sin anställning befinner sig i beroendeställning gentemot arbetsgivaren. Behandlingen innefattar inte känsliga eller extra skyddsvärda personuppgifter.

Förvaltningen har identifierat ett antal risker kopplade till behandlingen och dataskyddsombudet delar förvaltningens bedömning av dessa. Stadsfastighetsförvaltningen har föreslagit och vidtagit åtgärder som innebär att merparten av dessa risker har kunnat åtgärdas på ett sådant sätt att de inte innebär höga risker för de registrerades fri och rättigheter. Trots detta kvarstår två risker, risk ID 10 och 17 (se bilaga till konsekvensbedömning), som förvaltningen bedömer som höga. Bägge är knutna till Personuppgiftsbiträdet Intraservice (IS) användande av underbiträdet Microsoft (MS). Risk ID 10 handlar *om Övervakning av anställda genom analys och statistik av extern part (Microsoft)*, Risk ID 17 handlar om *Spridning av data till olämpliga underleverantörer på grund av ensidig förändring av vilka underleverantörer som används med dålig transparens av Microsoft*. Den 10 juli 2023 fattade EU-kommisionen beslut om adekvat skyddsnivå för EU:s och USA:s ramverk för dataskydd, the EU-U.S. Data Privacy Framework (DPF), för överföring av personuppgifter till USA. MS är ett av de företag/organisationer som anslutit sig till DPF och överföring av personuppgifter till MS i USA kan därmed ske med stöd av adekvansbeslutet, då EU-kommissionen gjort bedömningen att uppgifterna har samma skydd som om de skulle behandlas inom EU.

Av artikel 28 i GDPR framgår att när en personuppgiftsansvarig anlitar ett biträde för att å dess vägnar utföra en personuppgiftsbehandling *ska den personuppgiftsansvarige endast anlita personuppgiftsbiträden som ger tillräckliga garantier om att genomföra lämpliga tekniska och organisatoriska åtgärder på ett sådant sätt att behandlingen*

uppfyller kraven i denna förordning och säkerställer att den registrerades rättigheter skyddas.
Den så kallade omsorgsplikten. Det innebär att en personuppgiftsansvarig alltid måste göra en bedömning av huruvida de biträden och underbiträden som anlitas kan ge sådana tillräckliga garantier. Om den personuppgiftsansvarige gör bedömningen att sådana garantier inte kan lämnas, eller att det av olika skäl inte är möjligt för den personuppgiftsansvarige att göra en tillräcklig/korrekt bedömning av biträdets/underbiträdets lämplighet kan inte behandlingen inledas.

För att bedöma risken med att MS behandlar personuppgifter för egen räkning (Risk ID 10) har stadfastighetsförvaltningen bett om ett klargörande ifrån IS om hur avtalsrelationen ser ut mellan IS och underbiträdet MS, avseende vilka eventuella egna ändamål som MS kan ha med behandlingen av personuppgifter för att: *informera och kommunicera i Digitala Navet.* Förvaltningen har också bett om ett förtydligande ifrån IS om vilka överföringar som MS genomför till tredjeland, inkluderat eventuella under-underbiträden som MS eventuellt använder (Risk ID 17). Av den nu aktuella konsekvensbedömningen och kommunikation med stadsfastighetsförvaltningen framgår det att IS har kommunicerat dessa synpunkter till MS, men att ingen klargörande information har framkommit som kommit stadsfastighetsförvaltningen till del. Detta medför att Risk ID 10 och 17 inte har kunnat åtgärdas och att höga risker därför kvarstår

Dataskyddsombudet delar förvaltningens bedömning av riskerna och konstaterar att många åtgärder har gjorts i samband med arbetet med konsekvensbedömningen. Vad gäller de kvarstående höga riskerna så gör dataskyddsombudet inte någon annan bedömning än förvaltningen i denna del. Som certifierad part omfattas MS av DPF, att det finns ett tillämpligt adekvansbeslut för en överföring befriar dock inte den personuppgiftsansvarige från sin omsorgsplikt enligt artikel 28. Viktigt att notera är också att endast risk ID 17 är direkt kopplad till en tredjelandsöverföring. Risk ID 10, att ett underbiträde kan behandla personuppgifter för egen räkning, i strid med den personuppgiftsansvariges instruktioner, är en problematik som kan uppstå alldeles oavsett om biträdet/underbiträdet befinner sig i ett tredjeland eller ej.

Dataskyddsombudet vill särskilt påpeka att även om behandlingen i sig, med hänsyn till behandlingens art och kategorin av personuppgifter, inte kan sägas vara av särskilt integritetskänslig natur, så innebär oklarheten kring underbiträdets eventuella egna ändamål och eventuella tredjelandsöverföringar till under-underbiträden att höga risker för de registrerades fri-och rättigheter ändå kan föreligga. Detta då Stadsfastighetsförvaltningen i egenskap av personuppgiftsansvarig inte har möjlighet att uppfylla sin informationsplikt enligt GDPR. En naturlig följd av att som personuppgiftsansvarig inte förstå hur ett personuppgiftsbiträde, eller i det här fallet underbiträde, hanterar de personuppgifter man är ansvarig för, är att det blir omöjligt att på ett korrekt sätt informera de registrerade om behandlingen i enlighet med artikel 12 och 13 i GDPR. Det är inte heller möjligt att säkerställa de registrerades rätt till tillgång enligt artikel 15.

Dessa risker kan inte åtgärdas med mindre än att IS/MS visar att personuppgifter inte kommer användas för andra ändamål än de avsedda, samt att IS/MS kan visa att MS inte kommer överföra personuppgifter till tredjeländer där det saknas adekvat skyddsnivå för

skyddet av dessa uppgifter. Eftersom detta inte har skett och personuppgiftsbiträdet IS inte kan påvisa att frågan avtalsmässigt reglerats gentemot underbiträdet MS kan inte dataskyddsombudet göra någon annan bedömning än att stadsfastighetsförvaltningen inte kunnat fullgöra sin omsorgsplikt enligt artikel 28 i GDPR och säkerställa att man har möjlighet att tillgodose de registrerades rätt till information om behandlingen enligt artikel 12 och 13, och rätt till tillgång enligt artikel 15. Då stadsfastighetsförvaltningen inte kan uppfylla sin informationsplikt enligt GDPR är det därför också tveksamt om den föreslagna behandlingen kan anses uppfylla öppenhetsprincipen enligt artikel 5.1a[3]. Dataskyddsombudet vill i sammanhanget särskilt påtala att detta är en brist som härrör ur det sätt Göteborgs Stad är organiserad på snarare är på grund av en underlåtenhet ifrån stadsfastighetsförvaltningens sida. Tvärtom är dataskyddsombudets bedömning att förvaltningen gjort ett mycket gediget arbete med sin konsekvensbedömning och att man så långt det är möjligt försökt utreda sakförhållandena kring biträdesrelationen. Med detta sagt så delar dataskyddsombudet förvaltningens bedömning att det finns kvarstående höga risker med den föreslagna personuppgiftsbehandlingen.

Av artikel 36:1 i GDPR framgår att: *den personuppgiftsansvarige ska samråda med tillsynsmyndigheten före behandling om en konsekvensbedömning avseende dataskydd enligt artikel 35 visar att behandlingen skulle leda till en hög risk om inte den personuppgiftsansvarige vidtar åtgärder för att minska risken.*

Från denna regel i GDPR finns inget undantag. Dataskyddsombudet har tidigt i processen informerat förvaltningen om att ett sådant förhandssamråd kommer behöva begäras i det fall kvarstående höga risker finns. Dataskyddsombudets rekommendation är därför att stadsfastighetsförvaltningen ska ansöka om förhandssamråd med tillsynsmyndigheten om inte de kvarstående höga riskerna kan åtgärdas.

Medverkan från berörda parter

Förvaltningen uppger att synpunkter från de registrerade ej har inhämtats. Dock har information om och samverkan med fackliga organisationer skett sedan en tidsplan för införandet av Digitala navet startade under 2022.

Sammanfattade rekommendationer

- Dataskyddsombudet anser att förvaltningen, om den vill inleda den föreslagna behandlingen, ska ansöka om förhandssamråd hos tillsynsmyndigheten då det kvarstår höga risker med behandlingen.

Rekommendationer lämnade av:

[3] Se IMY:s beslut DI-2019-4062 *Beslut efter tillsyn enligt dataskyddsförordningen – Klarna Bank AB* s.10

Martin Lindén
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

Intraservice
[Diarienummer 0564/22]

Göteborgs Stad

Konsekvensbedömning enligt dataskyddsförordningen

Personuppgiftsbehandlingarna:
Informera och kommunicera i Digitala navet samt Tillhandahålla och utveckla Digitala navet

2023-06-14

Versionshantering

Datum	Version	Beskrivning	Ändrat av
2022-10-07	0.1	Överföring från gammal mall	Mindy Lind
2022-10-07-2022-12-19	0.1.1	Flertalet uppdateringar i versioner av arbetsgrupper främst bestående av:	Sara Herlitz, Mindy Lind, Fredrik Andersson, Robin Johansson, Sara Marin, Eva Rockmyr
2022-12-19	0.2	Komplettering	Fredrik Andersson
2023-01-09	0.3	Uppdaterad med förtydliganden	Sara Herlitz
2023-01-12	0.4	Hantering av kommentarer + riskbedömning	Sara Herlitz, Fredrik Andersson, Mindy Lind, Robin Johansson
2023-01-13	0.5	Uppdatering och förtydliganden av texter	Sara Herlitz, Mindy Lind
2023-01-17	0.6	Uppdaterad utifrån kommentarer från DSO – nytt dokument pga fel i tidigare fil.	Sara Herlitz, Mindy Lind, Fredrik Andersson, Robin Johansson, Anna-Lena Björk
2023-05-19	0.7	Uppdaterad med information från riskanalyser gjorda i maj 2023, refererar till tjänstespecifikationer och funktionsbeskrivningar. Omdisposition och tillägg.	Fredrik Andersson, Marcus Broman
2023-05-23	0.8	Rättningar och korrektur.	Mindy Lind, Marcus Broman.
2023-05-24	0.9	Korrigering kring risker.	Robin Johansson, Elias Örjefelt, Anna-Lena Björk, Mindy Lind.
2023-06-14	1.0	Slutlig genomgång av dokumentet	Fredrik Andersson Anna-Lena Björk

Innehåll

1 Inledning 4

1.1 Bakgrund och behov av behandling/behandlingar 4

1.2 Behov av konsekvensbedömning 5

1.3 Deltagare och roller 5

1.4 Personuppgiftsansvar 6

2 Beskrivning av behandlingarna 6

2.1 Översiktlig beskrivning av behandlingarna 6

2.1.1 Tillgångar 8

2.1.2 Personuppgiftsbiträden och underbiträden 9

2.1.3 Mottagare 9
2.2 Översikt behandling/behandlingar 9
2.2.1 Personuppgifter om lagöverträdelser 11
2.2.2 Kategorier av registrerade 11
2.2.3 Behandlingens/behandlingarnas omfattning 11
2.3 Ändamål 11
2.4 Rättslig grund 12
2.4.1 Känsliga personuppgifter 12
3 Behov/proportionalitet 13
3.1 Ändamålsbegränsning 13
3.2 Uppgiftsminimering 13
3.3 Lagringsminimering 14
3.4 Åtgärder som stärker de registrerades rättigheter 15
3.4.1 Informationsplikt 15
3.4.2 Tillgång och dataportabilitet 15
3.4.3 Rättelse och radering 15
3.4.4 Invändningar och begränsning av behandlingen/behandlingarna 16
3.4.5 Personuppgiftsbiträdesavtal och instruktioner 16
3.5 Samlad bedömning av behovet av och proportionaliteten hos behandlingen/behandlingarna 16
4 Överföring av personuppgifter utanför EU/EES 17
4.1 Sker det en överföring av personuppgifter utanför EU/EES? 17
4.2 Översikt överföringar 17
4.3 Lämpliga skyddsåtgärder 18
4.3.1 Andra/extra skyddsåtgärder 19
4.4 Undantag i särskilda situationer 19
4.5 Samlad bedömning 19
5 Risker och åtgärder 20
5.1 Generella åtgärder 20
5.1.1 Generella tekniska åtgärder 20
5.1.2 Generella administrativa åtgärder 21
5.2 Bedömning av specifika risker 23
5.2.1 Riskmatris 25
5.3 Samlad bedömning av risker och åtgärder 26
5.3.1 Kvarstående höga risker? 26
5.3.2 Förhandssamråd 26
6 Medverkan från berörda parter 26
6.1 Kommentarer/rekommendationer från dataskyddsombudet 26
6.2 Synpunkter från de registrerade 27

7 Avslut 27
7.1 Beslut 27
7.2 Nästa steg 27
8 Bilagor 27

1 Inledning

1.1 Bakgrund och behov av behandling/behandlingar

Göteborgs Stad arbetar på ett systematiskt och öppet sätt för att sprida information, kunskaper och erfarenheter både internt och externt. Staden utvecklar och effektiviserar kommunikationen genom att använda en gemensam kommunikationsplattform för alla förvaltningar och bolag.

Det finns ett behov av att publicera information, kontaktuppgifter och liknande till medarbetare i Göteborgs stad, som de behöver för att kunna utför sitt arbete. Intranätet är stadens prioriterade kommunikationskanal för intern kommunikation och kriskommunikation.

Det är samtidigt viktigt att staden är restriktiv med att publicera uppgifter om medarbetare för att skydda den personliga integriteten. Därför ändras tidigare intranät genom införandet av Digitala navet från att vara en delvis öppen webbplats bli en enbart intern webb.

Digitala navet tillhandahåller gemensam och lokal information inom ämnena Service, support och stöd i arbetet, Ledning och styrning, Organisation, Min anställning samt ett antal olika kärnämnen. I Digitala navet publiceras också kommunikativ aktuell information i form av Nyheter, Vi delar med oss, Nytt från och Kommande händelser (kallas för nyheter i detta dokument).

Syftet med Digitala navet är att skapa nyttor för medarbetare, chefer och organisationen i stort genom att:

- tillgängliggöra information om arbetssätt, rättigheter och skyldigheter kopplat till anställning, stöd och support i arbetet, pågående uppdrag och förändringar i staden.
- möjliggöra för medarbetare att kunna ta del av aktuell information på förvaltningen och för hela Göteborgs Stad.
- möjliggöra informationsspridning vid kris eller större händelse.
- samla länkar och enkel tillgång till verktyg och IT-stöd.
- tillgängliggöra information om stadens organisation och struktur samt kontaktpersoner för olika frågor.

- stärka och bygga den gemensamma bilden av Göteborgs Stad.

Möjlighet för redaktör att slå på kommentarfunktion på inlägg i kommunikativa kanaler finns.

1.2 Behov av konsekvensbedömning

I enlighet med datsskyddsförordningen skall en konsekvensbedömning genomföras när en personuppgiftsbehandling innebär hög risk för de registrerade. Förvaltningen har identifierat att så är fallet. I samband med behandling av personuppgifter i Digitala navet ser man anställda som en utsatt användargrupp, utifrån att anställda anses vara i beroendeställning till arbetsgivaren. Det är också en stor volym av personuppgifter som behandlas.

I samråd med representanter från flera delar av Intraservice (bland annat Digital infrastruktur) har förvaltningen enats om att göra en konsekvensbedömning för personuppgiftsbehandlingarna.

1.3 Deltagare och roller

- Sara Herlitz, kommunikationschef Intraservice
- Mindy Lind, kommunikatör/projektledare för att införa Digitala navet på Intraservice
- Eva Rockmyr, projektledare Lansera Digitala navet
- Fredrik Andersson, enhetschef intern och extern kommunikation
- Patrik Skog, kanslichef Intraservice
- Henrik Hoffmeister, förvaltningsjurist Intraservice
- Robin Johansson, IT-säkerhetsspecialist, Intraservice
- Sara Marin, IT-säkerhetsspecialist, Intraservice
- Anna-Lena Björk, informationssäkerhetschef (CISO), Intraservice
- Marcus Broman, Stöd informationssäkerhet och dataskydd, Intraservice
- Elias Örjefelt, IT-säkerhetsspecialist, Intraservice
- Niclas Törnqvist, IT-säkerhetsspecialist, Intraservice
- Mikael Schou Maegaard, Teknisk IT-strateg, Intraservice
- Robert Hansson, Service delivery manager (SDM) för Office365, Intraservice
- Andreas Öien Jons, Verksamhetsutvecklare, Intraservice
- Charlott Johansson, Tjänsteansvarig, Intraservice
- Fredrik Nikander Finman, Service delivery manager (SDM) för Identitet och åtkomst, Intraservice
- Anders Björk, Teknisk IT-strateg, Intraservice
- Bodil Olofsson, Utvecklingsledare HR, Intraservice
- Christian Petersson, Förvaltningsledare IT, Intraservice
- Nicholas Chizari, Systemanalytiker, Intraservice

1.4 Personuppgiftsansvar

Nämnden för Intraservice är personuppgiftsansvarig för sitt eget innehåll som Intraservice publicerar.

2 Beskrivning av behandlingarna

Personuppgiftsbehandlingarna är:

1. **Informera och kommunicera i Digitala navet**
   Ge medarbetare internt på förvaltningen och i hela staden kunskap om organisationen, arbetssätt och rutiner, rättigheter och skyldigheter som anställd, information om förändringsarbeten och vid kris, samt ge ökad delaktighet och ge möjlighet att skapa dialog och påverka.

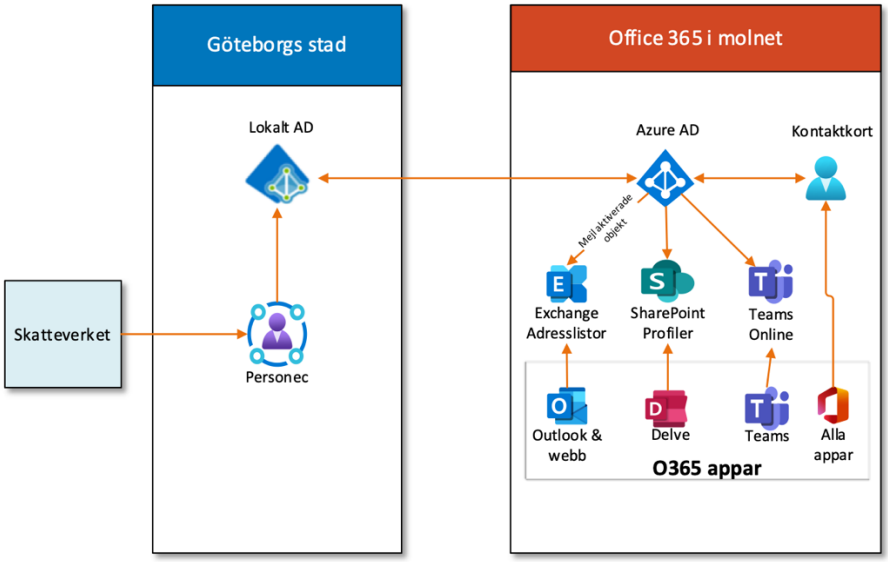
2. **Tillhandahålla och utveckla Digitala Navet**
   Utveckling och förvaltning av tjänsten sker av Intraservice för stadens användare inom följande områden:
   a. Funktionalitet levererad genom ny kod
   b. Funktionalitet levererad genom nya konfigurationer
   c. Övergripande strukturella förändringar och relaterat gemensamt innehåll
   d. Utbildning och hantering av behörigheter för redaktörer
   e. Säkerhetsfunktioner.

2.1 Översiktlig beskrivning av behandlingarna

Digitala navet bygger på plattformen Sharepoint Online som är en del av O365-plattformen inom Göteborgs Stad. När en användare loggar på sig på sin stadendator, har hen automatisk access till Office365 och till det Digitala navet.

Digitala navet hämtar uppgifter (förnamn, efternamn, e-postadress och av användaren publicerat foto) från den underliggande tjänsten Office365 (Delve/Azure) och publicering av sidor sker via den underliggande tjänsten Office365 (Sharepoint). Risker som är specifika för personuppgiftsbehandlingarna i Digitala navet behandlas i Riskbedömning Digitala navet på Intraservice.

Personuppgifter publiceras i form av kontaktkort på sidor i Digitala navet. Uppgifter kommer från flera underliggande källor, som illustreras genom för kopplingen i O365 kontaktkortet, vilket finns genomgående i O365-miljön.



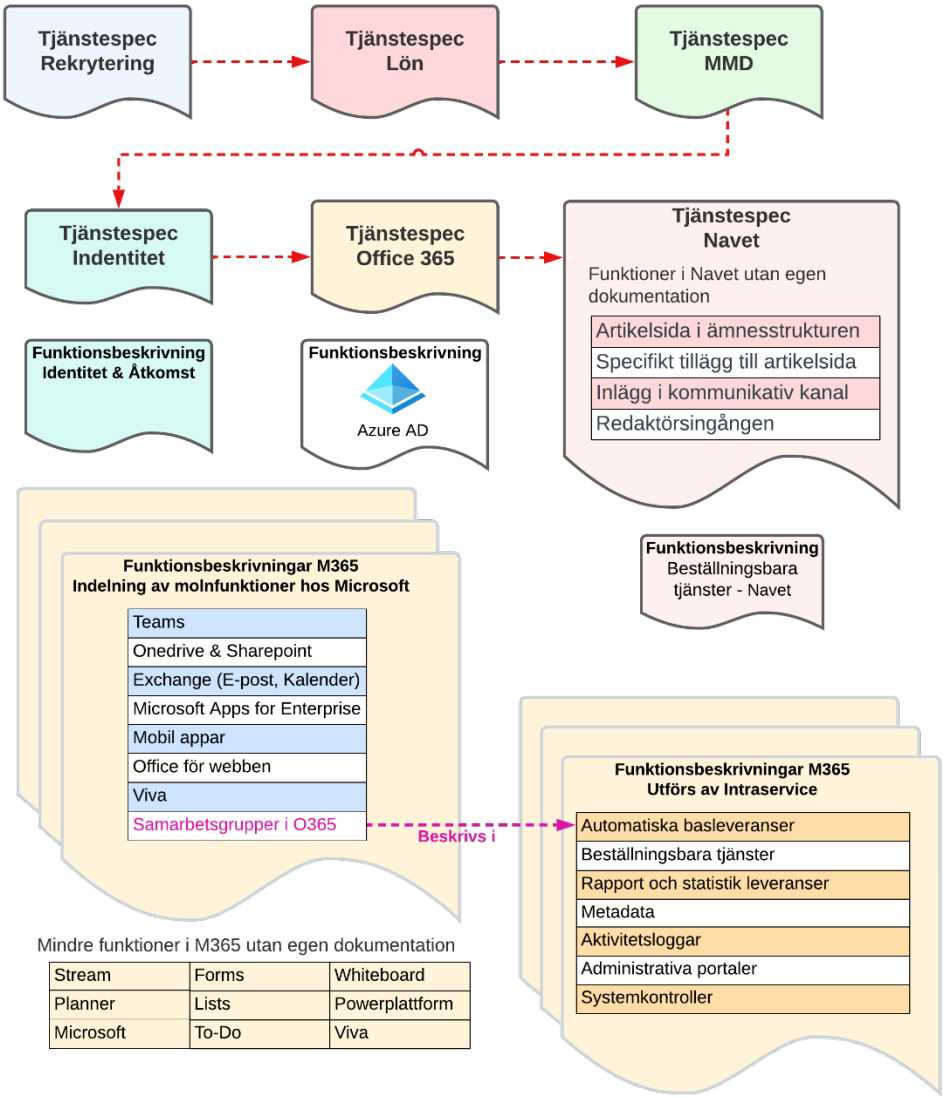
Hämtning av personuppgifter ur underliggande källor sker för att kvalitetssäkra och minimera risken för felaktiga personuppgifter.

Utöver inhämtning av personuppgifter från underliggande tjänster sker manuella tillägg där personuppgifter ska förekomma i redaktionellt bearbetade texter (exempel på detta kan vara av användaren publicerat telefonnummer, foto, uppdrag/roll och för förtroendevalda facklig tillhörighet).

Dokumentation av olika delar, personuppgiftsflöden som ingår i Digitala navet beskrivs i ett stort antal dokument som förklarar hur tjänster fungerar med aspekter på säkerhet och dataskydd. Dokumentationen sker i två nivåer:

1. Tjänstespecifikationer (kopplad till Intraservice tjänster - övergripande)
2. Funktionsbeskrivningar (underliggande funktioner som kan ingå i flera tjänster)

Tjänstespecifikationer och funktionsbeskrivningar med teknisk dokumentation



För fördjupad relevant teknisk beskrivning med flöden för personuppgiftsbehandlingarna, se *Tjänstespecifikation Digitala navet samt bilagor som listas nedan under Tillgångar 2.1.1*.

(Under arbetets gång har Microsoft bytt namn på sin tjänst Office365 till Microsoft365. Därför benämns tjänsten ibland som Microsoft365 eller M365 i materialet.)

2.1.1 Tillgångar

Informationsbärare och informationstillgångar är:

- Azure AD (hantering av behörighet och autentisering) – se *Funktionsbeskrivning Azure AD*
- Sharepoint (publicering av sida) – se *Funktionsbeskrivning Sharepoint och Onedrive*
- Delve (presentation av organisatorisk information i Azure AD) – se *Funktionsbeskrivning Sharepoint och Onedrive*

- Digitala navet – se *Tjänstespecifikation Digitala navet*
- Office 365, se *Tjänstespecifikation O365*
- Identitet och åtkomst, se *Tjänstespecifikation Identitet och Åtkomst*
- Kvalitetssäkrad information (Master Meta Data = MMD), *Bilaga 4 – Flöden - Digitala navet (O365, Identitet & Åtkomst, Lön samt MMD): bild 39. Personuppgiftsflöde MMD (Navet).*

2.1.2 Personuppgiftsbiträden och underbiträden

Enligt tidigare praxis som utgår ifrån tidigare styrmodellen (Riktlinje för kommungemensamma interna tjänster beslutad av stadsdirektör på delegation 2018-02-14 bilaga 1) är:

- Nämnden för Intraservice är personuppgiftsansvarig (PUA).
- Nämnden för Intraservice personuppgiftsbiträde (PUB) när vi levererar digitala navet till andra förvaltningar. (I dessa fall är respektive nämnd PUA).
- Microsoft är personuppgiftsbiträde för den underliggande plattformen Microsoft 365. För underbiträden till Microsoft, se *Tjänstespecifikation O365*.

Utredning pågår kring personuppgiftsansvar respektive personuppgiftsbiträde och delat personuppgiftsansvar. Resultatet av utredningen kan komma att påverka ovan beskrivning.

I arbetet med anpassning till Göteborgs Stads nya riktlinje för styrning, samordning och finansiering av digital utveckling och förvaltningen pågår arbete med att ta fram PUB-avtal med de förvaltningar och bolag som ska nyttja Digitala navet. Digitala navet bygger på underliggande tjänster som finns inom Microsoft Office 365. Avtal kopplat till Microsoft Office 365 hanteras i ett huvudavtal, inte enskilt för Digitala navet. Detta inkluderar Microsofts personuppgiftsbiträdesavtal (Data Protection Addendum, DPA).

2.1.3 Mottagare

Vid publicering av sidor och inlägg i kommunikativa kanaler (inklusive personuppgifter) i Digitala navet delas detta med förvaltningar och bolag i Göteborgs Stad. Då dessa lagras i Digitala navet och därmed Sharepoint delas den även med leverantören av plattformen (Microsoft).

2.2 Översikt behandling/behandlingar

Namn på behandling	Personuppgifter	Känsliga person-uppgifter

<table>
<tr>
<td>Informera och kommunicera i Digitala Navet</td>
<td>Manuella (redaktionella) tillägg: av användaren publicerat telefonnummer, foto, uppdrag/roll och för förtroendevalda facklig tillhörighet

Utöver detta publicerar redaktör relevanta personuppgifter i kopplat till innehåll. Dessa uppgifter bestäms i samråd med den berörda personen.

Generellt hanteras följande personuppgifter när användare använder Digitala navet:
<table>
<tr><th>Fält</th><th>Vad visas</th></tr>
<tr><td>Displayname</td><td>Förnamn + Efternamn</td></tr>
<tr><td>First name</td><td>Förnamn</td></tr>
<tr><td>Last name</td><td>Efternamn</td></tr>
<tr><td>User principle name</td><td>E-postadress</td></tr>
<tr><td>Job title</td><td>Förvaltningsnamn</td></tr>
<tr><td>Company name</td><td>Förvaltningsnamn</td></tr>
<tr><td>Department</td><td>Förvaltningsnamn</td></tr>
<tr><td>Manager</td><td>Chef</td></tr>
<tr><td>Email</td><td>E-postadress</td></tr>
<tr><td>AD konto</td><td>Namn på kontot (Staden-konto</td></tr>
</table>
</td>
<td>Facklig tillhörighet (enbart förtroendevalda som åtagit sig att utåt representera den fackliga organisationen)

Publicering av facklig tillhörighet sker i huvudsak mot bakgrund av skyldigheter inom arbetsrätt.

Publicering av den här information sker i samråd med berörd person.</td>
</tr>
<tr>
<td>Tillhandahålla och utveckla Digitala Navet</td>
<td>Maskinell hämtning: förnamn, efternamn, e-postadress, organisatorisk tillhörighet på förvaltningsnivå, chefer och av användaren publicerat foto.

Arbetsrelaterade kontaktuppgifter som redan finns i Office 365 (se tabell ovan) kan visas på en publicerad sida i Digitala navet.

Indirekta personuppgifter, såsom Metadata. Dessa kan vara MAC-adress, IP-adress, UID eller användarnamn.</td>
<td></td>
</tr>
</table>

2.2.1 Personuppgifter om lagöverträdelser

Nej

2.2.2 Kategorier av registrerade

Namn på behandling	Kategorier av registrerade
Informera och kommunicera i Digitala Navet	Anställda på Intraservice och i Göteborgs Stad Konsulter med uppdrag på Intraservice och i Göteborgs Stad
Tillhandahålla och utveckla Digitala Navet	Anställda på Intraservice samt på övriga förvaltningar och bolag i Göteborgs Stad Konsulter med uppdrag på Intraservice och i Göteborgs Stad

2.2.3 Behandlingens/behandlingarnas omfattning

För båda behandlingarna är omfattningen mer än 50 000 personer.

Det finns ingen behörighetsstyrning av publicerat innehåll, vilket innebär att allt publicerat innehåll är sökbart för samtliga anställda och konsulter i Göteborgs Stad.

2.3 Ändamål

Namn på behandling	Ändamål
Informera och kommunicera i Digitala Navet	Det är nödvändigt att utföra personuppgiftsbehandling genom publicering av anställdas kontaktinformation och utöva serviceskyldighet som stöd till anställda och konsulter på Intraservice och i staden, samt kunna bedriva förändringsarbete, tillhandahålla krisinformation samt ge ökad delaktighet och ge möjlighet att skapa dialog och påverka.
Tillhandahålla och utveckla Digitala Navet	Det är nödvändigt att utföra personuppgiftsbehandling för att kunna tillhandahålla och utveckla det

	Digitala navet som en plattform för nyheter, information om förändringar och aktuella händelser. Ändamålen innefattar även att tillhandahålla och utveckla krisinformation, säkerhetsfunktioner, förbättrad funktionalitet i tjänsten och utbildning av redaktörer.

2.4 Rättslig grund

Namn på behandling	Rättslig grund	Motivering och hänvisning
Informera och kommunicera i Digitala Navet	Myndighetsutövning	Intranätet/Digitala navet är stadens prioriterade kanal för intern kommunikation (se *Göteborgs Stads policy för kommunikation beslutad i kommunfullmäktige 2019-12-10*).
Tillhandahålla och utveckla Digitala Navet	Myndighetsutövning	Intraservice har ett uppdrag att leverera gemensamma tjänster till staden (se *Göteborgs Stads riktlinje för styrning, samordning och finansiering av digital utveckling och tjänster beslutad i kommunfullmäktige 2022-12-08*).

2.4.1 Känsliga personuppgifter

Namn på behandling	Känslig personuppgift som behandlas	Tillämpligt undantag och motivering/ hänvisning
Informera och kommunicera i Digitala Navet	Facklig tillhörighet för förtroendevalda kontaktpersoner inom fackligt förbund.	Det är ett uttryckt och samfällt ställningstagande från de fackliga organisationerna att fackliga förtroendevalda har i sitt uppdrag att vara synliga med

		namn, så att medlemmar/medarbetare ska kunna ta kontakt. Denna fråga är avstämd med fackförbundens jurister, enligt uppgift från stadsledningskontoret. Publicering av den här information sker i samråd med berörd person.

3 Behov/proportionalitet

3.1 Ändamålsbegränsning

Informera och kommunicera i Digitala Navet
Samtliga publiceringsansvariga (redaktörer) genomgår ett gediget utbildningspaket, bland annat för att säkerställa kunskap om hur man förhåller sig till personuppgifter. Utbildningen är en förutsättning för att få behörighet att publicera innehåll i Digitala navet.

Det finns olika behörighetsnivåer för redaktörer. Intraservices ansvarig för Digitala navet avgör vilken behörighet som ges till respektive redaktör.

Kopplat till varje redaktionell publicering sker avstämning med den registrerade, för att säkerställa att innehållet är korrekt och publicerbart.

Varje sida har:

- en publiceringsansvarig (redaktör) som publicerar informationen och ansvarar för att informationen på sidan visas på korrekt sätt, och
- en innehållsansvarig som ansvarar för att innehållet i informationen på sidan är korrekt.

Tillhandahålla och utveckla Digitala Navet
Vid maskinell hämtning av uppgifter från Office365 (exempelvis organisatorisk tillhörighet) kommer uppgifterna från kvalitetssäkrade källor, till exempel MMD (Master Meta Data).

3.2 Uppgiftsminimering

Kopplat till varje redaktionell publicering sker avstämning med eventuella registrerade, för att säkerställa att innehållet är korrekt.

Fält	Vad visas
Displayname	Förnamn + Efternamn
First name	Förnamn
Last name	Efternamn
User principle name	E-postadress
Job title	Förvaltningsnamn
Company name	Förvaltningsnamn
Department	Förvaltningsnamn
Manager	Chef
Email	E-postadress
AD konto	Namn på kontot (Staden-konto

För behandlingen ”Tillhandahålla och utveckla Digitala Navet” sker maskinell hämtning av uppgifter från O365 (se tabell ovan) uppgifterna kommer från kvalitetssäkrad information (MMD). För kvalitetsändamål sker inhämtning begränsat till enbart de personuppgifter som är nödvändiga för ändamålet. Inhämtning sker på ett standardiserat och effektivt sätt, samt personuppgifter uppgiftsminimeras och är pseudonymiserade av säkerhetsskäl i de fall sekretessmarkerade personer förekommer. Kvalitetssäkrade data innebär informationsförsörjning rörande grunddata såsom information om person, organisation, plats och tjänst i hela staden.

Samtliga redaktörer genomgår ett gediget utbildningspaket för att inte använda onödiga uppgifter. Där ingår delar som säkerställer kunskap om hur man förhåller sig till personuppgifter. Utbildningen är en förutsättning för att få behörighet att publicera innehåll i Digitala navet.

Det finns olika behörighetsnivåer för redaktörer. Intraservice ansvarig för Digitala navet avgör vilken behörighet som ges till respektive redaktör.

3.3 Lagringsminimering

Förvaltningsorganisationen, både centralt på Intraservices enhet *intern och extern kommunikation* samt lokalt på Intraservice kommunikationsavdelning tar fram rutiner för förvaltning av innehåll.

Rutinerna involverar en manuell livscykelhantering av innehållet i ämnesstrukturen. Årsvis kontaktas innehållsansvarig för att säkerställa att informationen på sidan är korrekt. Detta görs för allt gemensamt och lokalt innehåll som Intraservice ansvarar för.

Innan Digitala navet införs på Intraservice ska den lokala förvaltningsorganisationen ta fram en rutin för hur publicerade nyheter ska tas om hand i en livscykelhantering med gallring.

Information i Digitala navet enligt behandlingen *Informera och kommunicera i Digitala navet* ska hanteras enligt Intraservice dokumenthanteringsplan (Punktnotation 2.10 Informera, kommunicera och omvärldsbevaka).

Information i Digitala navet enligt behandlingen *Tillhandahålla och utveckla Digitala navet* ska hanteras enligt Intraservice dokumenthanteringsplan under verksamhetsområdena (VO) 3 Utveckla och leverera kommungemensamma IT-lösningar samt VO 4: Besluta och ta fram standardiseringar avseende arbetssätt och verktyg för kommungemensamma interna tjänster.

Alla som publicerar innehåll på Digitala navet måste ha utbildning, se Uppgiftsminimering 3.2.

3.4 Åtgärder som stärker de registrerades rättigheter

3.4.1 Informationsplikt

- Intraservice informerar om hur vi hanterar personuppgifter på den öppna webbplatsen goteborg.se, där finns den tillgänglig för såväl medarbetare som medborgare: Så behandlar Intraservice personuppgifter - Göteborgs Stad (goteborg.se).
- Intraservices medarbetare informerar också om verksamhetens personuppgiftsbehandling via en länk i e-postsignaturen.
- Vid anställning hos Intraservice informeras den nya medarbetaren om hur förvaltningen hanterar dennes personuppgifter.
- För de som förekommer i Digitala navet sker publicering i samråd med berörd person (art 13).

Åtgärd för att uppdatera Intraservice integritetspolicy finns med i planen för kommande projekt på förvaltningen, utifrån anmärkningar i revisionsrapport 2021–2022.

3.4.2 Tillgång och dataportabilitet

De personuppgifter som behandlas i digitala navet hämtas in ifrån de underliggande tjänsterna som digitala navet vilar på. Utöver detta kan en redaktör vid skapande av en sida påföra ytterligare information. Om uppgifter behöver flyttas hanteras detta av de underliggande tjänster där informationen lagras. Information som lagts in manuellt flyttas manuellt.

3.4.3 Rättelse och radering

Registerutdrag, rättelse, radering och begränsning av behandling hanteras efter begäran. Publiceringsansvarig kan rätta eller radera redaktionellt publicerat innehåll i Digitala navet. Beslut om hantering av individens rättigheter sker i enlighet med den fastställda delegationsordningen för Intraservice. All hantering av information sker utifrån gällande lagar och styrande dokument. All radering av personuppgifter hanteras enligt arkivlagen och skall som huvudregel bevaras. Eventuella radering av personuppgifter sker i enlighet med gallringsbeslut exempelvis i form av en dokumenthanteringsplan.

Alla sidor i Digitala navet har utsedda innehållsansvariga och publiceringsansvariga (redaktörer). På varje sida finns ett formulär man kan använda för att kontakta sidans innehållsansvarig eller publiceringsansvarig för synpunkter på innehållet eller presentation av informationen. Man kan också kontakta förvaltningsbrevlådan och dataskyddskontakter på kansliavdelningen.

3.4.4 Invändningar och begränsning av behandlingen/behandlingarna

Alla sidor i Digitala navet har utsedda innehållsansvariga och publiceringsansvariga (redaktörer). På varje sida finns ett formulär man kan använda för att kontakta både sidans innehållsansvarig och publiceringsansvarig för synpunkter på innehållet eller presentation av informationen. Man kan också kontakta förvaltningsbrevlådan och dataskyddskontakt på kansliavdelningen.

Publiceringsansvarig kan korrigera redaktionellt publicerat innehåll i Digitala navet. Beslut om hantering av individens rättigheter sker i enlighet med den fastställda delegationsordningen för Intraservice.

3.4.5 Personuppgiftsbiträdesavtal och instruktioner

I arbetet med anpassning till *Göteborgs Stads nya riktlinje för styrning, samordning och finansiering av digital utveckling och förvaltningen* pågår arbete med att ta fram PUB-avtal kopplat till Digitala navet.

Digitala navet bygger på underliggande tjänster som finns inom Microsoft Office 365. Avtal kopplat till Microsoft Office 365 hanteras i ett huvudavtal, inte enskilt för Digitala navet. Detta inkluderar Microsofts personuppgiftsbiträdesavtal (Data Protection Addendum, DPA).

3.5 Samlad bedömning av behovet av och proportionaliteten hos behandlingen/behandlingarna

Utifrån att intranätet är stadens prioriterade kanal för intern kommunikation och information, samt att det är en viktig kanal för krisinformation anses stadens behov av intranätet för alla medarbetare stå i proportion till behandlingen.

4 Överföring av personuppgifter utanför EU/EES

4.1 Sker det en överföring av personuppgifter utanför EU/EES?

OBS! Här krävs det att ni noggrant har kontrollerat alla personuppgiftsbiträden och underbiträden i hela kedja.

☒Ja

☐Nej

☒Risk för tredjelandsöverföring

Om svaret är Nej, gå direkt till avsnitt 5.

Om ni har kryssat i ”Risk för tredjelandsöverföring”, beskriv hur ni har kommit till den slutsatsen.

Se Riskanalys *O365 Riskanalys Dataskydd*

4.2 Översikt överföringar

Beskriv varje identifierad överföring av personuppgifter till tredjeland.

Namn på behandling och var i behandlingen som överföringen sker	Vilka person-uppgifter?	Till vilket land överförs person-uppgifterna ?	Finns det ett adekvans-beslut för mottagar-landet?
Informera och kommunicera i Digitala navet	För redogörelse av tredjelandöverföring se *Tjänstespecifikation O365*, *Tjänstespecifikation Digitala navet*, *O365 Riskanalys dataskydd*, *Digitala navet Riskanalys dataskydd och Riskbedömning Digitala navet på Intraservice*.	USA	Nej.

Tillhandahålla och utveckla Digitala Navet	För redogörelse av tredjelandöverföring se *Tjänstespecifikation O365*, *Tjänstespecifikation Digitala navet*, *O365 Riskanalys dataskydd* och *Digitala navet Riskanalys dataskydd och Riskbedömning Digitala navet på Intraservice*.	USA	Nej.

Om adekvansbeslut finns, gå direkt till avsnitt 5.

4.3 Lämpliga skyddsåtgärder

Andra överföringsverktyg än adekvansbeslut.

Namn på behandling	Lämpliga skyddsåtgärder	Motivering av lämpliga skyddsåtgärder
Informera och kommunicera i Digitala navet	Standardavtalsklausuler För skyddsåtgärder *Tjänstespecifikation O365*, *Tjänstespecifikation Digitala navet*, *O365 Riskanalys dataskydd* och *Digitala navet Riskanalys dataskydd och Riskbedömning Digitala navet på Intraservice*.	Den så kallade Schrems II-domen från 2020 anger att den överföringsmekanism som finns att tillstå när tidigare adekvansbeslut blev ogiltigförklarat är Standardavtalsklausuler. I dagsläget saknas rättsligt stöd för behandlingar av personuppgifter i de underliggande tjänsterna. EU-kommissionen har kommit med ett utkast till ett så kallat adekvansbeslut, och det slutgiltiga beslutet väntas under sommaren 2023.
Tillhandahålla och utveckla Digitala Navet	Standardavtalsklausuler	Den så kallade Schrems II-domen från 2020 anger att den

	För skyddsåtgärder *Tjänstespecifikation O365*, *Tjänstespecifikation Digitala navet*, *O365 Riskanalys dataskydd* och *Digitala navet Riskanalys dataskydd*.	överföringsmekanism som finns att tillstå när tidigare adekvansbeslut blev ogiltigförklarat är Standardavtalsklausuler. I dagsläget saknas rättsligt stöd för behandlingar av personuppgifter i de underliggande tjänsterna. EU-kommissionen har kommit med ett utkast till ett så kallat adekvansbeslut, och det slutgiltiga beslutet väntas under sommaren 2023.

4.3.1 Andra/extra skyddsåtgärder

Om den vidtagna skyddsåtgärden som angetts under 4.3 inte på egen hand är tillräcklig för att säkerställa en skyddsnivå som är likvärdig den som garanteras inom EU/EES genom GDPR behöver extra skyddsåtgärder vidtas. Ange dessa här:

En åtgärd är att data är flyttad i stora delar till datacenter i Sverige, beställning på flytt av resterande data ligger. Under 2023 kommer all Microsofts hantering av data flytta till Europa och Q4 2023 ska dessa kvarvarande delar hanteras inom EU.

I övrigt, se skyddsåtgärder i *Tjänstespecifikation O365*, *Tjänstespecifikation Digitala navet*, *O365 Riskanalys dataskydd* och *Digitala navet Riskanalys dataskydd och Riskbedömning Digitala navet på Intraservice.*

4.4 Undantag i särskilda situationer

Om det inte finns ett tillämpligt överföringsverktyg och ni bedömer att det finns ett tillämpligt undantag i artikel 49 GDPR, ange vilket undantag och varför det är tillämpligt:

Vi ser inga särskilda undantag.

4.5 Samlad bedömning

Lansering av digitala navet innebär fortsatt användning av den etablerade tjänsten Office365 och risker kopplat till tjänsten. Risker kopplade till de underliggande tjänsterna berör hela staden och kan inte bedömas enskilt utifrån Digitala navet.

Dessa risker beskriv i *O365 Riskanalys dataskydd*, där risker kring bland annat ”tredjelandsöverföring” finns. Dessa risker kan inte bedömas enskilt för Digitala Navet, utan tillhör den samlade riskbilden för Intraservice som förvaltning och tjänsteleverantör.

I dagsläget saknas rättsligt stöd för behandlingar av personuppgifter i den underliggande tjänsten Office 365.

5 Risker och åtgärder

5.1 Generella åtgärder

Ange vilka generella åtgärder som har vidtagits för att hantera mer generella risker som alltid finns i en verksamhet, oavsett vilken personuppgiftsbehandling som utförs.

Risker vid delning av personuppgifter med underleverantören i den underliggande plattformen Microsoft Office 365, hanteras i riskanalys *O365 Riskanalys Dataskydd,* se bilagor.

Åtgärderna är alltså kopplat till digitala navet.

5.1.1 Generella tekniska åtgärder

Ange vilka generella tekniska åtgärder som har införts eller planeras i syfte att minska eller eliminera de risker som identifierats.					
Genomförd	**Pågående**	**Planerad**	**Ej tillämplig**	**Åtgärd**	**Kommentar**
☒	☐	☐	☐	Autentisering	Digitala navet styrs genom behörighetsstyrning för publicering av innehåll.
☒	☐	☐	☐	Anti-malware	Ifrån underliggande funktion.
☐	☐	☐	☐	Detekteringsverktyg för personuppgiftsincidenter	
☒	☐	☐	☐	Säkerhetskopiering (backup)	Ifrån underliggande funktion.
☒	☐	☐	☐	Kryptering	Ifrån underliggande funktion.
☒	☐	☐	☐	Anonymisering	Ifrån underliggande funktion i MMD

☒	☐	☐	☐	Brandväggar	Ifrån underliggande funktion.
☒	☐	☐	☐	Detekteringsverktyg för intrång	Ifrån underliggande funktion.
☒	☐	☐	☐	Loggning	Ifrån underliggande funktion.
☒	☐	☐	☐	Logisk kontroll av åtkomst	Ifrån underliggande funktion.
☒	☐	☐	☐	Flerfaktorsautentisering	Ifrån underliggande funktion.
☒	☐	☐	☐	Nätverksautentisering	Ifrån underliggande funktion.
☒	☐	☐	☐	Pseudonymisering	Ifrån underliggande funktion.
☒	☐	☐	☐	Regelbundna mjukvaruuppdateringar (Patchning)	Ifrån underliggande funktion.
☒	☐	☐	☐	Detekteringsverktyg för sårbarheter	Ifrån underliggande funktion.
☒	☐	☐	☐	Mobile device management (MDM)	Ifrån underliggande funktion.
☐ **Inte säker** Kommentar: **Klicka eller tryck här för att ange text.**					
☒ **Annat** Kommentar: Flera av dessa skyddsåtgärder hanteras av underliggande tjänster. Se tjänstespecifikation Digitala navet, tjänstespecifikation MMD samt tjänstespecifikation Office 365 och underliggande funktionsbeskrivningar.					

5.1.2 Generella administrativa åtgärder

Ange de generella administrativa åtgärder som har införts eller planeras i syfte att minska eller eliminera de risker som identifierats.

Genomförd	Pågående	Planerad	Ej tillämplig	Åtgärd	Kommentar
☒	☐	☐	☐	Riktlinjer för datoranvändning	
☒	☐	☐	☐	Utbildning och informationsinsatser	Utbildningsinsatser för de som har rollen Redaktör

☐	☐	☒	☐	Kontinuitetsplan	Finns med i planen för kommande projekt på förvaltningen, utifrån anmärkningar i revisionsrapport 2021.
☒	☐	☐	☐	Incidenthanteringsplan	Förvaltningens processer för incidenthantering och personuppgiftsincidenter samt utpekade roller i förvaltningsteam.
☐	☐	☒	☐	Katastrofberedskap (Disaster recovery plan)	Finns med i planen för kommande projekt på förvaltningen, utifrån anmärkningar i revisionsrapport 2021.
☐	☐	☐	☒	Behovsenlig behörighet (Need-to-know)	Publicerat innehåll är ämnat för hela staden. Dock är generell tillgång till Digitala navet behörighetsstyrd.
☒	☐	☐	☐	Sekretessavtal	Förvaltningsspecifika sekretessavtal skrivs under vid anställning. Förvaltningsspecifika sekretessavtal för konsulter skrivs under vid uppdragsstart.
☒	☐	☐	☐	Lösenordspolicy	
☐	☐	☐	☒	Penetrationstestning	Penetrationstestning sker på Microsoft M365-miljö, men inte applicerbart direkt.
☒	☐	☐	☐	Säkra fysiska lokaler	
☒	☐	☐	☐	Tillsyn/interna kontroller	Exempelvis genomförs efterlevnadskontroll en gång per år (efterlevnad av stadens styrande dokument)
☒	☐	☐	☐	Övervakning	Övervakning ur ett tekniskt perspektiv

☐	☐	☒	☐	Simulerings- och krisövningar	Finns med i planen för kommande projekt på förvaltningen, utifrån anmärkningar i revisionsrapport 2021.
☒	☐	☐	☐	Bakgrundskontroller	Utförs vid behov
☒	☐	☐	☐	Åtkomstkontroll	Vi har kontroll vid fysisk åtkomst, behörighetskontroll för tillgång till Digitala navet och underliggande tjänster samt loggning av åtkomst.
☒	☐	☐	☐	Leverantörskontroller	
☐	☐	☐	☒	Riktlinjer för hantering av fysiska handlingar	Inga fysiska handlingar i Digitala navet.
☒	☐	☐	☐	Arkivering	I enlighet med förvaltningens dokumenthanteringsplan samt regionarkivets anvisning för webbarkivering.
☐ **Inte säker** Kommentar: Klicka eller tryck här för att ange text.					
☐ **Annat** Kommentar: Klicka eller tryck här för att ange text.					

5.2 Bedömning av specifika risker

Riskbedömningen finns i excelfilen ”Riskbedömning Digitala navet på Intraservice” och biläggs konsekvensbedömningen som bilaga 1.

Riskbedömningen inkluderar 35 risker som (efter vidtagna åtgärder eller om ingen ny värdering skett). Risker som har ett värde mellan 6–16 och som innebär att de utgör medelhöga och höga risker är överförda till tabellen nedan. Fler risker finns i Excelfilen, men risker inkluderar även andra behandlingar vilka inte är relaterade till Navet.
Riskhantering har skett i två omgångar:

- Risker 1–6 hanterades i december 2022 och januari 2023
- Risker 7–35 hanterades under maj (4,5, 8 och 15 maj 2023)

Riskerna i Excelfilen är indelade i risker för Intraservice som PUA:

- ***Informera och kommunicera i Digitala navet*** som enbart gäller Intraservice som förvaltning. Dessa risker behöver motsvarande andra verksamheter även ta ställning till gällande innehåll i Digitala Navet.

Intraservice som PUA, men även som PUB i tjänsteleveransen till kund:

- ***Tillhandahålla och utveckla Digitala navet*** är risker som är relaterade till Intraservice tjänst (inkluderat cybersäkerhet) samt för att stödja eventuell riskidentifiering av andra verksamheter gällande egna ställningstaganden för användning av Digitala Navet.

  Risker i Excelfilen från maj 2023 illustreras i Personuppgifts-aktiviteter som finns i powerpoint-filen *Flöden - Digitala navet (O365, Identitet & Åtkomst, Lön samt MMD)*

Risk -ID	Beskrivning av risk	Vidtagna skyddsåtgärder	Nytt risk-värde
5	Lansering av digitala navet innebär fortsatt användning av office365 och dess underliggande risker	Digitala navet presenterar information som finns i underliggande tjänster. Risker kopplade till de underliggande tjänsterna berör hela staden och kan inte bedömas enskilt utifrån Digitala navet.	16
7	Risk för att PUA/PUB-förhållanden förändras utifrån pågående utredningar, vilket leder till behov av förändringar i konsekvensbedömningen.	Utredning av PUA/PUB pågår. Konsekvensbedömningen uppdateras vid behov.	6
10	Personer som får sekretessmarkering under pågående anställning riskerar att synliggöras (möjliga att identifiera).	Ta bort användarens konto och skapa upp ett nytt (med pseudonym, likt de som redan har sekretessmarkering sedan tidigare).	12 (Värdering avser före skyddsåtgärd. Lösningsförslag på åtgärd finns framtagen. Utredning ska ske om hur denna ska implementeras.)
11	Risk för sekundäranvändning. Tillgång/Behandling AD/Azure AD kan användas för andra ändamål än vad som ingår i behandlingen. Risk för användning av priviligierade verktyg för olovlig insamling	Utreda vilken åtgärd som går att genomföra. Om möjligt, avgränsa tillgången till Azure AD och begränsa så att vissa klienter inte går att installera.	6 (värdering avser före skyddsåtgärd)

17	Spridning av data till olämpliga underleverantörer på grund av ensidig förändring av vilka underleverantörer de använder, med dålig transparens från Microsofts sida.	Förtydligande behöver inhämtas från Microsoft för att säkerställa att inte personuppgifter sprids utanför EU/EES.	9
27	Kommentarer på nyhetsinlägg kan användas felaktigt. Alla användare kan lämna kommentarer om funktionen är påslagen.	Den är avslagen som standard idag, enligt beslut från SLK. Bevakning av inkomna kommentarer dagligen via en moderatorsfunktion.	6 (Värdering avser före skyddsåtgärd., ej värderad efter åtgärder)
28	Skadlig kod laddas upp i filarkivet och kan få stor spridning på grund av att Digitala navet är en trovärdig källa	Risk accepterad, då Microsoft ansvarar för skydd mot skadlig kod i M365. Samma risk finns för inkommande kommunikation e-post eller andra kanaler.	6 (Värdering avser före skyddsåtgärd. Risk accepterad, ej värderad efter åtgärder)

5.2.1 Riskmatris

Detta avsnitt är en illustration av hur riskmatrisen ser ut och hur riskvärdena fördelar sig baserat på hur riskerna har bedömts i excelfilen. Ni behöver alltså inte fylla i något under detta avsnitt.

KONSEKVENS	Mycket allvarlig	4	8	12	16
	Allvarlig	3	6	9	12
	Måttlig	2	4	6	8
	Försumbar	1	2	3	4
		Osannolikt	Möjligt	Sannolikt	Mycket sannolikt
SANNOLIKHET					

5.3 Samlad bedömning av risker och åtgärder

Riskerna med publicering av information i Digitala navet som delas inom Göteborgs Stad bedöms som låga utifrån att det inte är några känsliga personuppgifter som publiceras förutom facklig tillhöghet för fackligt förtroendevald. I den samlade bedömningen kopplat till risker gällande Digitala navet anses risker för den registrerade som låg.

Lansering av digitala navet innebär fortsatt användning av den etablerade tjänsten Office365 och risker kopplat till tjänsten. Risker kopplade till de underliggande tjänsterna berör hela staden och kan inte bedömas enskilt utifrån Digitala navet.

Dessa risker beskriv i Riskanalys Office 365, där risker kring bland annat ”tredjelandsöverföring” finns. Dessa risker kan inte bedömas enskilt för Digitala navet, utan tillhör den samlade riskbilden för Intraservice som förvaltning och tjänsteleverantör.

5.3.1 Kvarstående höga risker?

Risk 17 – Spridning av data till olämpliga underleverantörer på grund av ensidig förändring av vilka underleverantörer de använder, med dålig transparens från Microsofts sida.

Risk 10 – Personer som får sekretessmarkering under pågående anställning riskerar att synliggöras (möjliga att identifiera) är under utredning och förslag finns som minskar risken.

Risk 5 – Lansering av Digitala navet innebär fortsatt användning av Office365 och dess underliggande risker.

5.3.2 Förhandssamråd

Beslut om förhandssamråd kopplat till de underliggande tjänsterna rekommenderas att tas efter att pågående arbetet, med genomlysning och dokumentation av samtliga personuppgiftsbehandlingar, risker och säkerhetsåtgärder kopplade till dessa, är genomfört.

6 Medverkan från berörda parter

6.1 Kommentarer/rekommendationer från dataskyddsombudet

Infoga dataskyddsombudets kommentarer och rekommendationer eller hänvisa till aktuell bilaga.

Se separat skrivelse från dataskyddsombud: Skrivelse till nämnden för Intraservice 2023-06-14

6.2 Synpunkter från de registrerade

Om de registrerade har tillfrågats angående behandlingen ska deras synpunkter redogöras för här. Om de inte har tillfrågats, ange varför så inte har skett.

Frågan om känsliga uppgifter som facklig tillhörighet är avstämd med fackförbundens jurister. Publicering av informationen av facklig kontaktperson sker i samråd med berörd person.

7 Avslut

7.1 Beslut

Ange vilket/vilka beslut som har fattats kopplat till konsekvensbedömningen, vem som har tagit det och i vilken roll.

Klicka eller tryck här för att ange text.

7.2 Nästa steg

Beskriv vilket/vilka steg som ska tas härnäst.

Klicka eller tryck här för att ange text.

8 Bilagor

Bilaga 1 – Riskbedömning Digitala navet på Intraservice

Bilaga 2 – O365 Riskanalys Dataskydd 2022-12-08

Bilaga 3 – Digitala navet Riskanalys Dataskydd 2023-01-20

Bilaga 4 – Flöden - Digitala navet (O365, Identitet & åtkomst, Lön samt MMD)

Bilaga 5 – Tjänstespecifikation - Digitala navet

Bilaga 6 – Tjänstespecifikation - O365

Bilaga 7 – Tjänstespecifikation - Identitet och Åtkomst

Bilaga 8 – Funktionsbeskrivning - Azure AD

Bilaga 9 – Funktionsbeskrivning - Sharepoint och Onedrive

Mall framtagen av dataskyddsenheten (version 1)

Telefon: 031-365 00 00 (Göteborgs Stad, Kontaktcenter)
E-post: dso@intraservice.goteborg.se

Senast uppdaterad 2022-08-24

Riskbedömning Införa Digitala navet på intraservice

Identifiering och bedömning av risker

Bedöm hur allvarliga och sannolika riskerna är på skalan 1–4.

Konsekvens

1 = Försumbar 2 = Måttlig 3 = Allvarlig 4 = Mycket allvarlig

Sannolikhet

1 = Osannolikt 2 = Möjligt 3 = Sannolikt 4 = Mycket sannolikt

Se mallstödet för beskrivning av de olika nivåerna och instruktioner.

Risk-ID	Namn på behandling	PU-Flöden *PU-aktiviterer där risken finns*	PUA/PUB *Risk bedömd även för tjänsteleverans till andra veksamheter*	Risk *Obehörig åtkomst till personuppgifter, oönskad ändring av personuppgifter, förlust av personuppgifter eller annan form av risk*	Beskrivning av risk	Konsekvensern a av risken för den registrerade	Konsekvens	Sannolikhet	Riskvärde	Vidtagna skyddsåtgärder	Konsekvens efter åtgärd	Sannolikhet efter åtgärd	Riskvärde efter åtgärder	Uppföljning av vidtagna åtgärder ska göras
1	Informera och kommunicera i Digitala Navet		PUA	Annan form av risk	Risk att person utsätts för hot eller negativ uppmärksamhet efter publicering av kontaktuppgifter i samband med text som uppfattas negativ.	Kan leda till obehag eller hot mot kontaktpersonen.	3	1	3	Primärt ska funktionsbrevlådor användas som kontakt. Innan kontaktpersoner publiceras skall detta stämmas av. Utbildning av redaktörer säkerställer korrekt hantering.	2	1	2	Arbete som utförs av central och lokal förvaltningsorganisation. Dessa organsiationer är under uppbyggnad nu, i samband med att tjänsten ska införas.
2	Tillhandahålla och utveckla Digitala Navet		PUA/PUB	Ej PU-risk	Organisatoriskt: Risk för att Digitala navet är inte tillgängligt - antingen under längre tid eller vid kris - på grund av driftstörning, vilket leder till allvarlig skada för organisationen.	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
3	Informera och kommunicera i Digitala Navet		PUA	Annan form av risk	Risk att vi publicerar information som inte borde publiceras, på grund av handhavandefel eller mänskliga faktorn, vilket leder till personuppgiftsincident.	Medarbetares personuppgift riskerar att förekomma i ett felaktigt sammanhang.	2	1	2	Behörighet att publicera ges enbart till medarbetare som har fått utbildning. Den lokala förvaltningsorganisationen behöver sätta upp tydliga arbetssätt och rutiner för att säkerställa kunskapsnivå och kvalitetssäkring.	1	1	1	Arbete som utförs av central och lokal förvaltningsorganisation. Dessa organsiationer är under uppbyggnad nu, i samband med att tjänsten ska införas.

4	Informera och kommunicera i Digitala Navet		PUA	Annan form av risk	Risk att personuppgifter ligger kvar för länge.	Gammal information riskerar att bli inaktuell och/eller oönskad. Exempelvis att medarbetare som slutat fortfarande förekommer som kontaktperson för en funktion där hen inte längre arbetar.	1	2	2	Rutin för kontroll och rensning av information upprättas inom förvaltningen för att säkerställa att informationen är aktuell.	1	1	1	Arbete som utförs av central och lokal förvaltningsorganisation. Dessa organsiationer är under uppbyggnad nu, i samband med att tjänsten ska införas.
5	Informera och kommunicera i Digitala Navet		PUA	Annan form av risk	Lansering av digitala navet innebär fortsatt användning av office365 och dess underliggande risker.	Risk för tredjelandsöverföring av personuppgifter som visas i Digitala navet.	4	4	16	Digitala navet presenterar information som finns i underliggande tjänster. Risker kopplade till de underliggande tjänsterna berör hela staden och kan inte bedömas enskilt utifrån Digitala navet.	N/A	N/A	0	N/A
6	Informera och kommunicera i Digitala Navet		PUA	Annan form av risk	Risk för att PUA/PUB-förhållanden förändras utifrån pågående utredningar, vilket leder till behov av förändringar i konsekvensbedömningen.	Det behöver redas ut när Microsoft är personuppgiftsansvarig (PUA), när Intraservices nämnd är PUA, samt om stadsledningskontoret är PUA för viss gemensam information.	2	3	6	Utredning av PUA/PUB pågår. Konsekvensbedömningen uppdateras vid behov.	2	3	6	Risken är oförändrad eftersom skyddåtgärden ännu inte är genomförd.
7	Informera och kommunicera i Digitala Navet	Aktivitet 27 och 29	PUA/PUB	Övervakning av en persons aktiviteter	Otillåten övervakning av användare genom metadata. Chef övervakar anställda Anställda övervakar varandra.	Brist i information till registrerade Kan inte neka behandling	3	2	6	Kommunicera information till registrerade för att minska risken. Gärna specifikt just-in-time.	1	1	1	
8	Tillhandahålla och utveckla Digitala Navet	Aktivitet 10 och 16	PUA/PUB	Förlust av kontroll över personuppgifter	Information raderas ej från metadata, utan stannar kvar eftersom metadata är relaterat till objektet leder till otillräcklig gallring och kontroll över PUB samt oklara villkor/avtal	Förlust av kontroll över personuppgifter Kan inte neka behandling	1	3	3				0	
9	Tillhandahålla och utveckla Digitala Navet	Aktiviteter 23, 26, 28, 29, 30 och 33	PUA/PUB	Övervakning av en persons aktiviteter	Övervakning av anställda (Analys och statistik) av extern part (Microsoft)	Förlust av kontroll över personuppgifter	1	3	3				0	
10	Tillhandahålla och utveckla Digitala Navet	Aktivitet 10 och 34	PUA/PUB	Avslöjande av information om individer som negativt påverkar deras säkerhet	Personer med sekretessmarkering riskerar att synliggöras (möjliga att identifiera) under pågående anställning	Osäkerhet - Personuppgifter skyddas inte tillräckligt och utsätts för risk.	4	3	12	Svårt att lösa i DN, utan här gäller annan hantering. En stark skyddsåtgärd är att ta bort användarens konto och skapa upp ett nytt (med pseudonym, likt de som redan har sekretessmarkering sedan tidigare).	4	1	4	Riskägare ALB utreder implementation av åtgärd.
11	Tillhandahålla och utveckla Digitala Navet	Aktivitet 10	PUA/PUB	Sekundäranvändning	Tillgång/Behandling AD/Azure AD kan användas för olämpliga ändamål	Personuppgifter används för ett annat ändamål än vad som är avsett vid insamling. Läsa bearbeta, utlämna personuppgifter till alla användare	2	3	6	Utreda vilken åtgärd som går att genomföra. Om möjligt, avgränsa tillgången till AAD och begränsa så att vissa klienter inte går att installera. Fråga: Måste vi ha läsrättigheter? Om en del tekniker behöver, kan de få tillgång, annars inte.			0	
12	Tillhandahålla och utveckla Digitala Navet	Aktivitet 34	PUA/PUB	Förlust av kontroll av personuppgifter.	Tilldelning av licens för opersonliga/gruppkonton på grund av manuell kontoadministration eftersom man kan använda ett gruppkonto och då saknas det spårbarhet över vem som tar ut	Det saknas spårbarhet på vem som tar ut personuppgifter	1	3	3				0	
13	Tillhandahålla och utveckla Digitala Navet	Aktivitet 34	PUA/PUB	Exkludering - Personer som ska ha information får det inte samt ev följd av osäkerhet, att personuppgifter inte skyddas tillräckligt och utsätts för för risk.	Tillgänglighet Digitala Navet, utan licens kommer man inte inte åt Digitala Navet.	Otillåten/okontrollerad informationsspridning genom att man använder andra sätt än DN.	2	2	4				0	

14	Tillhandahålla och utveckla Digitala Navet	Aktivitet 2 och 18	PUA/PUB	Obehörig åtkomst till personuppgifter, oönskad ändring av personuppgifter	Intrång av obehöriga SQL i Azure för provisionering genom cyberintrång där man kan skapa nya behörigheter	Osäkerhet - Personuppgifter skyddas inte tillräckligt och utsätts för risk	3	1	3				0	
15	Tillhandahålla och utveckla Digitala Navet	generellt	PUA/PUB	Obehörig åtkomst till personuppgifter, oönskad ändring av personuppgifter samt förlust av personuppgifter	Virus i Mail & Teams bli attackerad av skadlig kod. Externt (antagonistiskt hot) med problem i miljön och datorer och resurser kan inte användas.	Osäkerhet för registrerades personuppgifter.	2	2	4				0	
16	Tillhandahålla och utveckla Digitala Navet	Aktivitet 10	PUA/PUB	Obehörig åtkomst till personuppgifter	Sekretessbrott gällande i behandling av material i Digitala Navet genom att amerikanska rättsväsendet tar del av sekretessbelagda personuppgifter. Innehållsdata som är sekretessbelagt skrivs av en redaktör och publiceras i DN. Inga (bra) alternativa kontorsstöd för kommunikation av sekretessuppgifter.	Bryter ett löfte om att hålla personuppgifter hemliga (sekretessbrott).	2	1	2				0	
17	Tillhandahålla och utveckla Digitala Navet	Aktivitet 10	PUA/PUB	Obehörig åtkomst till personuppgifter,	Spridning av data till olämpliga underleverantörer på grund av ensidig förändring av vilka underleverantörer de använder, med dålig transparens från MS sida.	Risk för problematisk tredjelandsöveröri ng. Spridning av data till olämpliga underleverantörer/ annan användning	3	3	9	Förtydligande behöver inhämtas från Microsoft för att säkerställa att inte personuppgifter sprids utanför EU/EES.			0	
18	Informera och kommunicera i Digitala Navet	Aktivitet 2	PUA/PUB	Obehörig åtkomst till personuppgifter, oönskad ändring av personuppgifter samt förlust av personuppgifter	Felaktig behörighetshantering i Navet genom att användare beställer redaktörsbehörigheter i Serviceportalen felaktigt. Spårbarhet finns.	Individ kan inte lita på information	2	2	4	Ställa krav på att EC verifierar behörigheter innan de godkänner. Acceptera risken.			0	
19	Tillhandahålla och utveckla Digitala Navet	Aktivitet 3	PUA/PUB	Förlust av kontroll av personuppgifter.	Lista över alla sidor i Digitala navet har för vid åtkomst geom information om vilka sidor redaktören eller innehållsansvariga skapat själva	Ökad tillgänglighet, oönskad spridning av personuppgifter och därmed göra dem lättare åtkomliga	2	2	4	Kommunicera information till registrerade för att minska risken. Acceptera risken			0	
20	Tillhandahålla och utveckla Digitala Navet	Aktiviteter 4 och 5	PUA/PUB	Förlust av kontroll av personuppgifter.	Listan ansvarig per förvaltning används visar vilka sidor redaktören eller innehållsansvariga skapat och felaktig information sprids genom kapning/påverkan för att sprida missinformation.	Ökad tillgänglighet, oönskad spridning av personuppgifter och därmed göra dem lättare åtkomliga Förvrängning, Lämna ut falsk information om en individ som negativt påverkar hur denna uppfattas av andra	1	2	2	Kommunicera information till registrerade för att minska risken. Acceptera risken.			0	
21	Tillhandahålla och utveckla Digitala Navet	Aktivitet 27	PUA/PUB	Förlust av kontroll av personuppgifter.	PU kvarstår efter redaktör slutat, eftersom metadata innehåller referenser till personer (redaktörer) som inte blir gallrade (om det ska gallras pga av att det är av ringa betydelse)	Bevarar personuppifter längre än nödvändigt som kan påverka hur en individ uppfattas av andra	1	3	3				0	
22	Tillhandahålla och utveckla Digitala Navet	Aktivitet 36	PUA/PUB	Exkludering - Personer som åtkomst får det inte det.	Felaktigt personnummer skapas vid anställning leder till att medarbetare inte får rätt uppgifter/konto	Personnummer kommer inte bli upplagd i lönesystemet eller övriga system (AD/osv)	1	1	1				0	
23	Tillhandahålla och utveckla Digitala Navet	Aktivitet 36	PUA/PUB	Obehörig åtkomst till personuppgifter	Skapa anställning – Utlämnande av personuppgifter av medarbetare som själv eller under påtryckning från annan lämnar ut uppgifter.	Avslöjande - Lämna ut information om en individ som negativt påverkar säkerheten	3	2	6				0	
24	Tillhandahålla och utveckla Digitala Navet	Aktivitet 36	PUA/PUB	Obehörig åtkomst till personuppgifter, oönskad ändring av personuppgifter	Skapa anställning – Anställd med hög behörighet manipulerar anställningsinformation	Osäkerhet - Personuppgifter skyddas inte tillräckligt och utsätts för risk	2	1	2				0	

25	Tillhandahålla och utveckla Digitala Navet	Aktivitet 7 och 8	PUA/PUB	Exkludering - Personer som åtkomst får det inte det, ev oönskad ändring av personuppgifter	Kontaktkort ifylls med olämplig fritext i artikelsidor eller nyhetsinlägg i sidor i sharepoint och kontaktkort	Ingern - Medarbetare får fel information, extern – eventuellt otillbörlig påverkan/it-säkerhet	2	1	2	Ett godkännande behöver ske (Approval-flöde) innan en nyhet publiceras. Filer som ska bifogas ska kontrolleras av en person.			0	
26	Tillhandahålla och utveckla Digitala Navet	Aktivitet 7 och 8	PUA/PUB	Exkludering - Personer som åtkomst får det inte det, ev oönskad ändring av personuppgifter	Felaktig information används i kontaktformulären till publiceringsansvarig och innehållsansvarig hamnar därför fel	Fel person får frågor riktade till sidansvarig. Eller fel som är oavsiktligt.	1	2	2	Ett godkännande behöver ske (Approval-flöde) innan en nyhet publiceras. Filer som ska bifogas ska kontrolleras av en person.			0	
27	Informera och kommunicera i Digitala Navet	Aktivitet 8	PUA/PUB	Förlust av kontroll av personuppgifter.	Kommentarer på nyhetsinlägg kan användas felaktigt. Alla användare kan lämna kommentarer om funktionen är påslagen.	Intern: om kommentarsflödet är aktiverat kan alla användare kommentera på nyheten, känsliga uppgifter kan spridas.	3	2	6	Kommentarsfunktionen är inte påslagen som standard. Man behöver aktivera den. Bevakning av inkomna kommentarer dagligen till en moderatorsfunktion. Det finns kommungemensamma riktlinjer (förmodat ang kommentarsfält i social medier) som även ska gälla för navet.			0	
28	Tillhandahålla och utveckla Digitala Navet	Aktivitet 9	PUA/PUB	Obehörig åtkomst till personuppgifter, oönskad ändring av personuppgifter samt förlust av personuppgifter	Skadlig kod laddas upp i filarkivet och kan få stor spridning pga av att DN är en trovärdig källa	Skadlig kod kan spridas med olika nivåer av påverkan beroende på vilken skadlig kod som laddas upp och sprids.	3	2	6				0	
29	Tillhandahålla och utveckla Digitala Navet	generellt	PUA/PUB	Obehörig åtkomst till personuppgifter, oönskad ändring av personuppgifter samt förlust av personuppgifter	Scopet av PU ändras för säkerhetsåtgärder på avsaknad av att process saknas, liksom definition på scoopet, Bristande definitioner, Otydliga krav och bristande information	Osäkerhet - Personuppgifter skyddas inte tillräckligt och utsätts för risk. Uteslutning - Personuppgifter behandlas utan individens vetskap eller delaktighet (brist på	2	3	6	Skapa en process och regelverk på förvaltningen (anvisning, rutin, instruktioner) för säkerhetsändamål, så att det finns tydliga kravställningar. Riskägare CISO. Information till registrerade om vad som sker för att upprätthålla säkerhet i DN	2	2	4	
30	Tillhandahålla och utveckla Digitala Navet	generellt	PUA/PUB	oönskad ändring av personuppgifter	[redacted]	Osäkerhet - Personuppgifter skyddas inte tillräckligt och utsätts för risk. Förvrängning – Lämna ut falsk information om en individ som negativt påverkar hur denna uppfattas av andra	3	1	3	[redacted]			0	
31	Tillhandahålla och utveckla Digitala Navet	Aktivitet 30	PUA/PUB	Förlust av kontroll av personuppgifter.	Användaren har inte medvetenhet om uppgifter som loggas av Intraservice och loggning av vilka sidor man besöker	Användaren exkluderas och kan uppleva övervakning. Uteslutning - Personuppgifter behandlas utan individens vetskap eller delaktighet (brist på	2	2	4	Information till registrerade om vad som sker för att upprätthålla säkerhet i DN. HR-ansvarig	2	1	2	
32	Tillhandahålla och utveckla Digitala Navet	Aktivitet 26	PUA/PUB	Förlust av kontroll av personuppgifter.	Det saknas information om vilken data Microsoft behöver för att upprätthålla säkerheten.	Avsaknad av information. Uteslutning - Personuppgifter behandlas utan individens vetskap eller delaktighet (brist på	3	2	6	Undersöka vilka åtgärder MS utför genom dialog. Tjänsteägare	3	1	3	
33	Tillhandahålla och utveckla Digitala Navet	generellt	PUA/PUB	Sekundäranvändning	MS anser sig vara PUA för personuppgifter för säkerhet. De kan hitta på nya säkerhetslösningar typ AI eller problematiska sammanställningar som lämnas ut till tredje part.	Nya typer av behandlingar är inte förenligt med ändamålet som PU samlades in för	2	2	4	Undersöka vilka åtgärder MS utför genom dialog. Tjänsteägare			0	
34	Tillhandahålla och utveckla Digitala Navet	generellt	PUA/PUB	Förlust av kontroll av personuppgifter.	För mycket aggregerad data i loggen (O365-loggarna ingår i logghanteringen)	Ev insamling av för mycket info från användnare, samt för vid åtkomst. Aggregering - Kombinerar olika typer av personuppgifter (inkl profilering).	2	2	4	Skapa en process och regelverk på förvaltningen (anvisning, rutin, instruktioner) för säkerhetsändamål, så att det finns tydliga kravställningar. Riskägare CISO	2	1	2	

35	Tillhandahålla och utveckla Digitala Navet	Aktivitet 29	PUA/PUB	Obehörig åtkomst till personuppgifter. Förlust av kontroll av personuppgifter.	[redacted]	Osäkerhet - Personuppgifter skyddas inte tillräckligt och utsätts för risk. I värsta fall kan uppgifter presenteras i läsbara fält i Navet	3	2	6	[redacted]	3	1	3	
36									0				0	
36									0				0	

Riskanalys Dataskydd

Tjänsteleverans Microsoft Office 365

2022-12-04

Versionshantering

Datum	Version	Beskrivning	Ändrat av
2020-03-25	0.1 – 0.6	Utkast Riskanalys Dataskydd	Lena Ottermark, Per Gustavsson
2020-06-30	1.0	Fastställd version	Per Gustavsson
2021-07-09	1.91	Utökad och omarbetad med ny disposition, inkl nya aspekter ang tredjelandsöverföring, tekniska aspekter, uppdaterade kategorier av PU (kap 3), omarbetat riskkapital (kap 7) nya Appendix, förteckning av tidigare dokument, Översiktliga beskrivningar av O365-tjänsterna	Marcus Broman Jan Albinsson
2021-07-09	2.0	Fastställd version	Per Gustavsson
2021-10-04	2.91	Uppdaterad med nya risker baserat på datatyper baserad på ny kännedom om specifika risker för tredjelandöverföring, visualisering av riskmatrisen	Marcus Broman
2021-12-04	2.92	Reviderad efter återkoppling från DSO. Reducerade beskrivningar av vad som kan tolkas som vägledande ställningstaganden.	Marcus Broman
2021–12-XX	3.0	Fastställd version	Anna-Lena Björk

Medverkande i arbetet med Riskanalys Dataskydd för O365

Version 1 (2020-06-30)	
Fredrik Andersson	Enhetschef, Intern och Extern kommunikation, Intraservice
Josephine Andersson	Tjänsteansvarig Kommunikation, Intraservice
Johan Bergström	Dataskyddsombud för Intraservice
Charlott Johansson	Tjänsteansvarig IT, Intraservice
Robert Hansson	Service delivery manager O365, Intraservice
Per Gustavsson	Säkerhetsarkitekt, Intraservice
Lena Ottermark	Projektledare, konsult
Henrik Hoffmeister	förvaltningsjurist, Intraservice
Version 2 (2021-07-09)	
Per Gustavsson	Informationssäkerhetschef (CISO), Intraservice
Marcus Broman	Expertstöd informationssäkerhet- och dataskydd, konsult
Jan Albinsson	Expertstöd informationssäkerhet, konsult
Version 3 (2022-10-05)	
Anna-Lena Björk	Enhetschef IT-säkerhet (CISO), Intraservice
Marcus Broman	Expertstöd informationssäkerhet- och dataskydd, konsult
Fredrik Andersson	Enhetschef, Intern och Extern kommunikation, Intraservice
Josephine Andersson	Tjänsteansvarig Kommunikation, Intraservice
Charlott Johansson	Tjänsteansvarig IT, Intraservice
Robert Hansson	Service delivery manager O365, Intraservice
Robin Johansson	IT-säkerhetsarkitekt, Intraservice

Erik Vidén	IT-strateg, Intraservice
Elin Olsson	Dataskyddsombud, Enhetschef Dataskyddsenheten, Intraservice
Andréa Bergqvist	Dataskyddsombud, Intraservice
Jenny Henriksson	Dataskyddsombud, Intraservice
Henrik Hoffmeister	Förvaltningsjurist och dataskyddskontakt, Intraservice

Innehållsförteckning

1 Bakgrund och Metod 6

1.1 Bakgrund 6

1.2 Metod 6

1.3 Omfattning 8

2 Nulägesbeskrivning av tjänsteleveransen 12

2.1 Tjänstens namn 12

2.2 Tjänsteansvarig samt ansvar för riskanalys 12

2.3 Vilka regelverk omfattas tjänsteleveransen av? 12

2.4 Intraservice roll, PUA eller PUB 13

2.5 Personuppgiftsansvariga 14

2.6 Beskriv tjänstens användande i verksamheten (hos PUA) 15

2.7 Tjänstespecifikationer 15

2.8 Beskriv tjänstens IT-arkitektur 17

2.9 Behörigheter inom tjänsten 17

3 Personuppgifter, känslighet och tjänstens karaktär 19

3.1 Kategorier av registrerade 19

3.2 Kategorier av personuppgifter 19

3.3 Tillgång till personuppgifter 19

3.4 Omfattning av personuppgifter i tjänsten 20

3.5 Uppgifter om sårbara eller personer i beroendeställning ..... **Fel! Bokmärket är inte definierat.**

3.6 Särskilda kategorier av personuppgifter (art 9,10) **Fel! Bokmärket är inte definierat.**

3.7 Hantering av extra skyddsvärda personuppgifter. **Fel! Bokmärket är inte definierat.**

3.8 Sökningar i syfte att få fram sammanställningar .. **Fel! Bokmärket är inte definierat.**

3.9 Automatiskt beslutsfattande .... **Fel! Bokmärket är inte definierat.**

3.10 Systematisk övervakning ..... **Fel! Bokmärket är inte definierat.**

3.11 Utvärdering eller poängsättning ..... **Fel! Bokmärket är inte definierat.**

3.12 Samkörning av uppgifter ..... **Fel! Bokmärket är inte definierat.**

4 Individers rättigheter 21

4.1 Tillämpliga rättigheter 21

5 Säkerhet vid behandling av personuppgifter i tjänsten 23

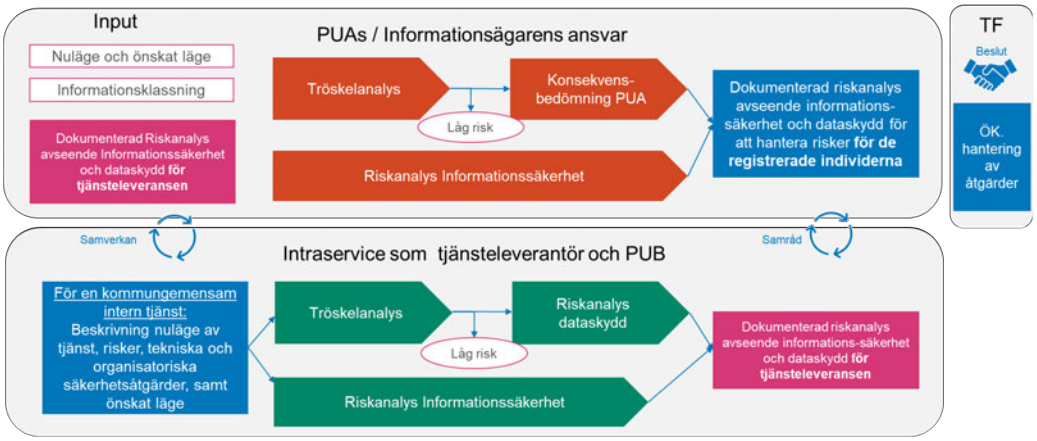
5.1 Administrativa åtgärder 23
5.2 Tekniska åtgärder 24
6 Tredjelandsöverföring 26
6.1 Förekomst 26
6.2 Grund för tredjelandsöverföring 26
6.3 Tolkning gällande Schrems II 27
6.4 Behov av Transfer Impact Assessment (TIA) 29
6.5 Hemtagning 31
7 Risker och åtgärder 33
7.1 Riskhanteringsmetod 33
7.2 Riskbeskrivningar 35
7.3 Riskmatriser 55
7.4 Kvarvarande risk 60
7.5 Rekommendation till PUA ang. användning av tjänsten 60
8 Bilagor 61
9 Referenser 62
10 Appendix 1 – Exempel konsekvenser och sannolikheter 65
10.1 Konsekvenser 65
10.2 Sannolikhet 66
11 Appendix 2 – Tidigare dokument 67
11.1 Förteckning av tidigare dokument gällande O365 67

1 Bakgrund och Metod

En *Riskanalys Dataskydd* är en systematisk och dokumenterad riskhantering med utgångspunkt i dataskyddsförordningen som utförs på en kommungemensam intern tjänst eller motsvarande. Konskenvensbedömningar kan ske i olika omfattning och former. Omfattning av riskanalysen görs från ett IT-perspektiv där personuppgiftsbehandlingarna är inte angivna i detalj.

1.1 Bakgrund

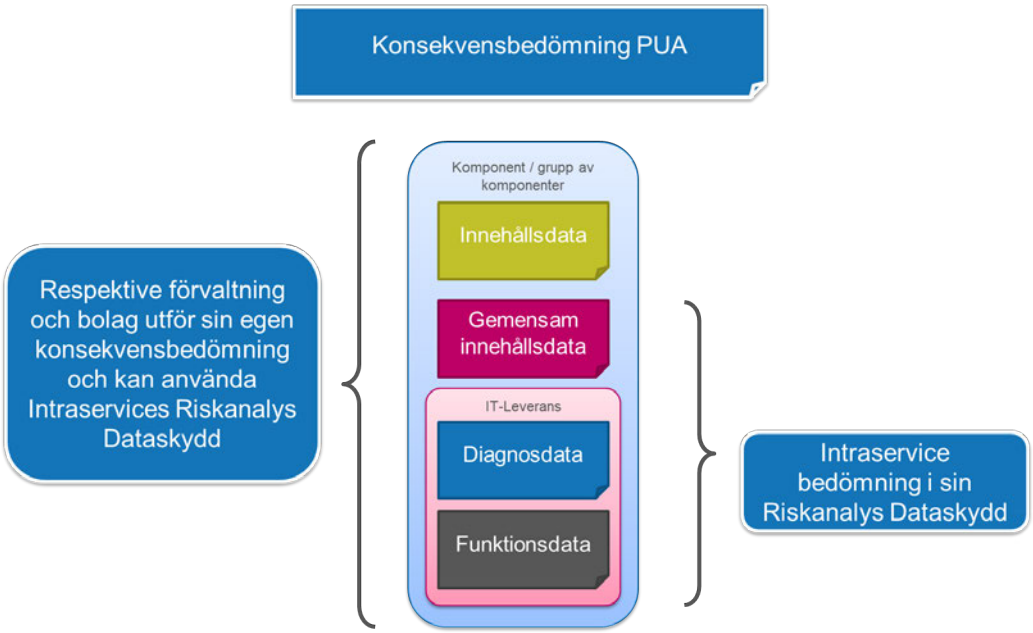
Riskanalys dataskydd för Microsoft Office 365 utförs av tjänsteleverantören Intraservice för kommungemensamma interna tjänster i egenskap av personuppgiftsbiträde. Riskanalys dataskydd är en beskrivning av tjänsten som levereras samt riskanalys med fokus på personuppgifter utifrån tjänsteleverans och tekniskt perspektiv. Tröskelanalys och eventuell Konsekvensbedömning av behandlingar av personuppgifter görs av Personuppgiftsansvarig (PUA).



Figur 1- Riskbedömning informationshantering

1.2 Metod

I kommungemensamma tjänster kan Intraservice bedöma hantering av vissa data men inte den innehållsdata som användare och personuppgiftsansvariga skapar. Som utgångspunkt kan man definiera fyra olika typer av data med personuppgifter och som behandlas i syfte att kunna leverera en tjänst med IT-stöd.



Figur 2- Riskanalys förhållande till innehållsdata, gemensamma innehållsdata, diagnosdata samt funktionsdata

- **Innehållsdata** (kunddata, Content data, Customer data) är data som användare hos personuppgiftsansvarig skapar genom att använda kontorsstödstjänsten. Exempelvis innehåll i filer, e-post, kommunikation etc.

- **Gemensamma innehållsdata**: exempelvis användarinformation som härrör från befolkningsregister, gemensamma metadatastrukturer, visualiseringar av organisation.

- **Diagnosdata** (telemetridata) är data som leverantören samlar in för att analysera hur tjänster, applikationer och operativsystem används. Datat är en förutsättning för analys av funktionaliteten och för att utveckla och uppdatera applikationen. Det kan förekomma att den organisation som tillhandahåller den gemensamma tjänsten i egenskap av PUB samlar in och lagrar data om den individuella användningen. Likaså kan en underleverantör av SaaS-tjänst samla in och behandla data för säkerhet och utvecklingstjänstens IT-stöd.

- **Funktions data** är data som är till för att säkerställa de grundläggande funktionerna i en applikation och är till exempel identiteter och inloggningsinformation, autentiseringsinformation, konfigurationsinformation, accessrättigheter, och versionshantering av filer som innehåller innehållsdata. Funktionsdata är data som leverantören tillfälligt måste bearbeta för att låta användare ansluta till internet och använda onlinetjänster är konfigurationsdata för IT-stödet.

1.3 Omfattning

För en så pass omfattande analys av O365 som helhet har ett grundligt arbete genomförts sedan 2016 som belyser olika aspekter och olika roller.[1]
Den kommungemensamma interna tjänsten O365 har liksom många andra tjänster med IT-innehåll personuppgifter i flera nivåer av data. Med nivåer av data avses innehållsdata, gemensamma innehållsdata, funktionsdata och diagnosdata. Omfattningen av funktionella data samt diagnosdata varierar mellan olika tjänster och dess IT-stöd.

En riskanalys för komponent eller grupp av komponent i Office 365 består av två delar.

- Den första delen är innehållsdata i dokument, e-post, kalendrar med mera och där omfattningen av personuppgiftsbehandlingar bestäms av förvaltning/bolag som använder tjänsten.
- Den andra delen är gemensamma innehållsdata, diagnosdata samt funktionsdata som genereras vid användningen av komponenter i Office 365 och där omfattningen av personuppgiftsbehandlingar kan inte bestämmas av personuppgiftsansvarig (PUA).

Denna riskanalys omfattar gemensamma innehållsdata, funktionsdata och diagnosdata.

Arbetet med att beskriva och bedöma risker i tjänsteleveransen av O365 omfattar gemensamma innehållsdata, diagnosdata samt funktionsdata. Detta betyder att Intraservice har betraktat:

- Outlook mejl som en tjänst som förmedlar e-post från avsändare till mottagare, utan att betrakta innehållet i breven.
- Outlook kalender som en tjänst som möjliggör bokning och genomförande av möten, utan att betrakta innehåll i möteskallelser.
- Sharepoint och Onedrive som tjänster som erbjuder lagring av dokument och information, utan att betrakta innehållet.
- Word Online, Excel Online, Powerpoint Online och OneNote som tjänster som erbjuder skrivmöjligheter, utan att betrakta innehåll.
- Teams är en tjänst för e-möten, chatt och e-samarbete.

1.3.1 Datatyper i Office 365

I denna riskanalys beskrivs främst risker med olika former av metadata, vilket är metadata, alltså data om data. I analysen förkommer många olika termer för datatyper. För att underlätta förståelsen av datatyper och Microsofts terminologi presenteras en analys av termer nedan[2].

[1] Bedömningar har därför skett i flera steg, där alla delar omfattar separata rapporter och riskbedömningar på olika områden. En sammanfattning av tidigare rapporter, undersökningar och bedömningar finns i Appendix 3
[2] Analysen av termer bygger på en konsekvensbedömning från den nederländska staten av Microsoft Teams, Onedrive och Azure, från den 16 feb 2022: https://www.rijksoverheid.nl/documenten/publicaties/2022/02/21/public-dpia-teams-onedrive-sharepoint-and-azure-ad

Typer av data i Microsoft Office 365				
Innehållsdata	Innehållsdata	Teams videoström		
		Filinnehåll		
	Gemensamma innehållsdata	Supportdata		
		Azure AD (kontodata)		
		Visualisering av strukturen		
Metadata (data om data)	Diagnosdata	Telemetri	Nödvändiga servicedata (Required Service Data)	Säkerhetsdata
				Applikationsfel
				Enhetsdata
				Sessions ID
		Serverloggar	Granskningsloggar (audit logs)	
			Loggar från kontodata	
			Viva	
	Funktionsdata	Dataström för autentisering		
		Dataström för kommunikation		
		Konfigurationsdata		

Tjänsteleveransen av O365 till Göteborgs Stad består av alla delar utom den innehållsdata, som är exkluderat ur riskvärderingar. Innehållsdata i filinnehåll och Teams videoström är var och en av verksamheternas egna ansvar. Emellertid ingår den gemensamma innehållsdata i denna riskanalys. Nedan beskrivs vilka typer av data som innehåller personuppgifter i tjänsten O365 till Göteborgs Stad.

Innehållsdata är innehåll i Word-filer, Powerpoint-filer, Excel-filer, OneNote, Forms-enkäter, e-post innehåll etc. Innehållsdata (Content data) är data som användare skapar med Office 365 komponenter, till exempel text som skrivs in i ett Word-dokument, och används i samband med den anslutna upplevelsen. Annan innehållsdata är (Customer data) Signaturer, kontaktkortsinformation som användaren kompletterar med, personlig information i Delve etc.

Gemensamma innehållsdata som är användarinformation som härrör från HR system och Skatteverkets befolkningsregister. Exempel på gemensamma innehållsdata är kontaktkort från Active Directory (AD), gemensamma metadatastrukturer, visualisering av organisation.

Funktionella data konfigurationsdata för komponenter, metadata som tex. rättigheter, tillgång, ändringar om innehållsdata, (t.ex. filnamn, ägare, event loggar, e-post loggar) samt funktionella data som Microsoft tillfälligt måste bearbeta för att låta användare ansluta till internet och använda Microsofts onlinetjänster. Data som behövs för tex. autentisering och konfiguration av

appar mm.

Diagnostikdata (eller diagnosdata) avser data som samlats in eller erhållits av Microsoft från programvara som installeras lokalt av kunden i samband med användning av Microsofts produkter. Diagnostikdata inkluderar inte kunddata, tjänster som genereras eller data om professionella tjänster.

Microsoft delar upp diagnostikdata i flera kategorier:

- Obligatoriska diagnostikdata (required diagnostic data) – minimumnivå på information som är obligatorisk för att hjälpa säkerställa säkerhet, relevans och förväntad prestanda i Microsoft applikationer installerade på de enheter som dessa applikationer körs på.

- Förbättrade diagnostikdata (endast Windows) - innehåller information om de webbplatser användaren surfar på, hur Windows och applikationer används och hur de fungerar, samt enhetsaktivitet. Denna datakategori hjälper Microsoft att fixa och förbättra produkter och tjänster för alla användare. I O365-leveransen ingår inte klienter, alltså Windows och är exkluderat.

- Valfria diagnostikdata (optional diagnostic data) – tilläggsdata som hjälper Microsoft att förbättra sina Office produkter och ger förbättrad information som hjälper Microsoft att upptäcka, diagnostisera och åtgärda problem. För Windows innehåller valfria diagnostikdata mer detaljerad information om användarens enhet och dess inställningar, funktioner och enhetens hälsa. Valfria diagnostiskdata inkluderar även obligatoriska diagnostikdata

Diagnostiska data för tjänster, som är de data som krävs för att hålla tjänsten säker, uppdaterad och fungera som förväntat. Också Intraservice samlar in loggar etc. som diagnosdata.

För mer detaljerad information om begreppet diagnosdata, se utdrag från konsekvensbedömning (på engelska DPIA Data Protection Impact Assessment) utförd-av Nederländerna där omfattande analys av diagnosdata för O365 genomförts (Privacy Company, 2019).

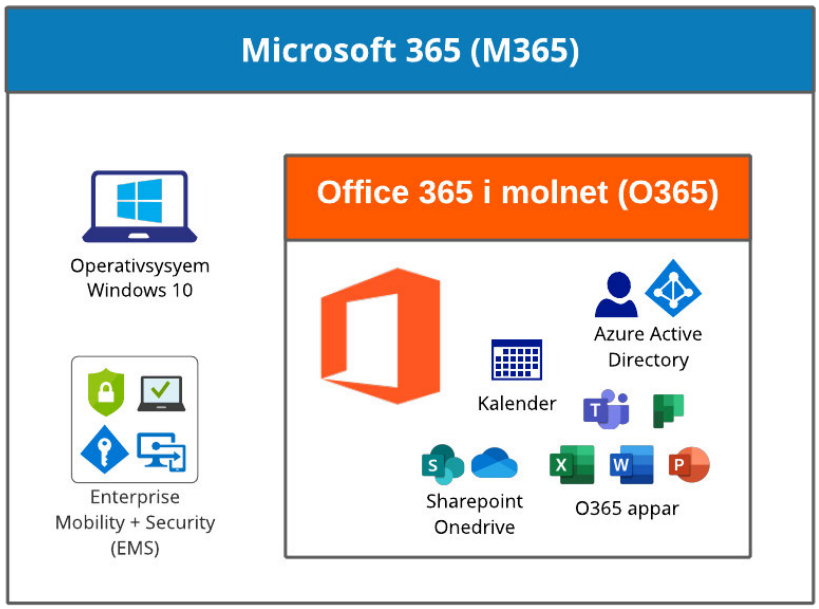
> *The observed telemetry data do not contain any content from documents, emails or conversations, and no directly identifying data such as user names or e-mail addresses. The events related to the use of the processor Connected Experiences such as the spelling checker and Translator also do not contain snippets of content.*
>
> *This finding is in line with Microsofts explanation: "This diagnostic data doesn't include names of users, their email addresses, or the content of their Office files. Our system creates a unique ID that it associates with your user's diagnostic data. When we receive diagnostic data showing that one of our apps crashed 100 times, this unique ID lets us determine if it was a single user who crashed 100 times or if it was 100 different users who each crashed once. We don't use this unique ID to identify a specific user."*

I bilaga 1 finns *Rapport - Analys av Microsofts hantering av diagnostikdata – underlag för konsekvensbedömning* som visar mer detaljerat hur Microsoft använder diagnostikdata samt rekommendationer för hantering av diagnostikdata (Göteborgs Stad Intraservice, 2021a).

1.3.2 M365 och O365

Microsoft 365 (M365) är en samlad benämning på produkter som innehåller Office 365 samt även lokala applikationer, operativsystemet Windows 10 Enterprise, Enterprise Mobility + Security (EMS) och maskininlärning. Office 365 (O365) är en molnbaserad serie med appar och tjänster med bekanta applikationer som Microsoft Outlook, Word, Powerpoint och Excel, vilka görs tillgängliga både via dator, mobila enheter och webbläsare.

M365 betecknas som hela införandet med vad som ingår i licensen och O365 avser de molnbaserade tjänsterna. Riskhanteringen i denna rapport handlar om O365 med ingående tjänster. Operativsystem, EMS och maskininlärning är exkluderat. Lokala applikationer ingår inte i Intraservice tjänst för O365. Denna riskanalys innefattar inte lokala klienter eller servrar.



M365 avser hela licensen, O365 avser de molnbaserade tjänsterna som bedöms i denna rapport.

2 Nulägesbeskrivning av tjänsteleveransen

2.1 Tjänstens namn

Microsoft Office 365 (O365)

2.2 Tjänsteansvarig samt ansvar för riskanalys

Tjänsteansvarig är:

Josephine Andersson, tjänsteansvarig Kommunikation samt Ledning & Styrning

Ansvariga för denna Riskanalys Dataskydd är:
Med ansvariga menas den eller de som ansvarar för arbetet att genomför riskanalysen och därmed säkerställa att alla relevanta perspektiv har tagits i beaktande.

Kontaktpersoner för denna riskanalys för:

Tjänsteleveransen O365: Fredrik Andersson, enhetschef Intern och Extern kommunikation, Intraservice

Informationssäkerhet och dataskydd: Per Gustavsson, CISO, Intraservice

2.3 Vilka regelverk omfattas tjänsteleveransen av?

Ange vilka lagrum och/eller regelverk tjänsteleveransen omfattas av:

Dataskyddsförordningen (även benämnd som DSF eller GDPR) (EU 2016/679)

Offentlighets och Sekretess lag (OSL 2009:400)

Stadens Styrande dokument (Göteborgs Stad, 2021)

Säkerhetspolicy för Göteborgs Stad (Göteborgs kommunfullmäktige, 2019c)

Riktlinje för informationssäkerhet (Göteborgs kommunfullmäktige, 2019a)

Riktlinje för behandling av personuppgifter i Göteborgs Stad (Göteborgs Stad, 2020)

Riktlinjer för styrning av kommungemensamma interna tjänster (vad)
(Göteborgs kommunfullmäktige, 2019b)

Göteborgs Stads generella regler för kommungemensamma interna tjänster (hur)
(Göteborgs Stads kommunstyrelse, 2021a)

Göteborgs Stads regler för kommungemensamma interna tjänster (vilka)
(Göteborgs Stads kommunstyrelse, 2021b)

2.4 Intraservice roll, PUA eller PUB

Beskriv om Intraservice är personuppgiftsansvarig (PUB) eller personuppgiftsbiträde (PUA) i hanteringen av personuppgifter inom tjänsten.

Intraservice betraktar sig som personuppgiftsbiträde (PUB) för all data i O365 plattformen. Med data i O365 avses innehållsdata, gemensamma innehållsdata, funktionella data samt diagnosdata. Se ovan.

Intraservice är personuppgiftsansvarig för data som sker i personuppgiftsbehandlingar för den egna förvaltningen, vilket inte hanteras i detta dokument.

Vad styrker att Intraservice har rollen som beskrivs ovan?

2014-06-15 fattas beslut om nuvarande styrmodell i riktlinjer och regler för Kommungemensamma interna tjänster (Göteborgs kommunfullmäktige, 2019b; Göteborgs Stads kommunstyrelse, 2021a, 2021b). Styrdokument uppdateras årligen och beslutas av kommunfullmäktige.

Senare versioner av regeldokumenten innehåller IT-tjänster och tjänsten e-post. Tjänsten har successivt utvecklats till dagens leverans av O365 plattformen. Det är ett kommungemensamt beslut att tjänsten ska levereras till staden av Intraservice.

Intraservice Nämnd beslutade 2016 augusti att realisera tjänsten med hjälp av O365 plattformen som också utgör ett teknikskifte för befintlig tjänst levererad som SaaS från Microsoft. Bilagt som beslutsunderlag är en beskrivning av tjänstens delar och dess arkitektur samt krav på behov av Risk och Sårbarhetsanalys
(Göteborgs Stad Intraservice, 2016). Beslutet i augusti 2016 innebar också att O365 utgör framtida plattform för Stadens digitala arbetsplats.

I Göteborgs Stads riktlinjer för styrning av kommungemensamma interna tjänster (Göteborgs kommunfullmäktige, 2019b) beskrivs en ansvarsfördelning som är beslutad av kommunfullmäktige. Se också bilaga i Göteborgs *Stads Generella Regler för kommungemensamma interna tjänster* (Göteborgs Stads kommunstyrelse, 2021a) som säger att Intraservice är PUB åt nämnder och styrelser i staden.

Kommunstyrelsen har fastställt att Intraservice ska anses som PUB i sin leverans av Kommungemensamma interna tjänster. Detta resonemang stämmer med synsättet i detta arbete.

Intraservice är alltså leverantör till staden av O365 och därmed PUB för alla personuppgifter som hanteras i tjänsten oavsett typ av data.

2.5 Personuppgiftsansvariga

Skriv in vilken eller vilka organisationer (gemensam personuppgiftsansvarig) som är ansvarig för personuppgiftsbehandling i tjänsten.

Formellt är det är nämnder och styrelser som är personuppgiftsansvariga, men här anges namnet på organisationen (förvaltningar och bolag)

De förvaltningar och bolag som använder tjänsten O365 från Intraservice är:

Arbetsmarknad och vuxenutbildning
Fastighetskontoret
Förskoleförvaltningen
Försäkrings AB Göta Lejon
Förvaltningen för funktionsstöd (FFS)
Got Event AB
Grefab
Grundskoleförvaltningen
Göteborg & Co AB
Göteborgs Stads Leasing AB
Göteborgs Stadshus AB
Göteborgs Stadsteater AB
Idrotts- och Föreningsförvaltningen
Inköp och upphandling
Konsument- och medborgarservice
Kretslopp och vatten
Kulturförvaltningen
Lokalförvaltningen
Miljöförvaltningen
Park- och naturförvaltningen
Revisorskollegiet Regionarkivet
Socialförvaltningen Centrum
Socialförvaltningen Hisingen
Socialförvaltningen Nordost
Socialförvaltningen Sydväst
Stadsbyggnadskontoret
Stadsledningskontoret
Trafikkontoret
Utbildningsförvaltningen
Äldre samt vård- och omsorgsförvaltningen (ÄVO)

Intraservice använder även för Office 365 för den egna förvaltningen, men ändamål i egenskap av PUA inkluderas ej av denna riskanalys.

2.6 Beskriv tjänstens användande i verksamheten (hos PUA)

Beskriv i den omfattning det är känt hur tjänsten används av verksamheterna.

Office 365 är en molnbaserad plattform som omfattar verktyg för att underlätta dagens arbetssätt. Tjänsten innefattar dels den tekniska plattformen, dels stöd till förvaltningar och bolag och deras medarbetare i att använda och få nytta av digitala verktyg i Office 365.

Genom tjänsten kan stadens medarbetare kommunicera, samarbeta och på ett effektivt och säkert sätt få saker gjorda oavsett var man är.

I plattformen ingår:

- Flertalet Out-Of-The-Box (OOTB) program från Microsoft Office 365.
- Gemensamma kommunikationsverktyg som bland annat möjliggör distansmöten med ljud och bild
- Verktyg för kommunikation, samarbete och planering inom grupper
- Programvaror som till exempel Excel, Word, Powerpoint och Outlook i kombination med kraftfulla molntjänster med lagringsmöjligheter såsom Onedrive och Sharepoint.
- Office 365 ger oss möjligheten att skapa och dela filer och information oavsett geografisk plats och enhet; dator, mobiltelefon eller läsplatta.

Plattformen kommer att kunna utvecklas modulärt med olika tjänster och tillämningar. Den är därmed en viktig komponent i framtida digitalisering i staden.

Tjänsten utvecklas utifrån stadens samlade behov. Arbetet med att utveckla tjänsten sker i en utvecklingsorganisation där kundrepresentanter deltar för att fånga in behov kopplade till tjänsten, analysera och prioritera behoven, lansera nya lösningar och förändra arbetssätt.

Tjänstebeskrivning enligt *Regler för kommungemensamma interna tjänster* (Göteborgs Stads kommunstyrelse, 2021b): De tidigare IT-tjänsterna E-post och videokonferens är ersatta av Office 365 och under 2019 sker faktureringen fortfarande under benämningen E-post.

2.7 Tjänstespecifikationer

De deltjänster inom O365 som ingår i denna riskanalys är de funktioner som publicerats till Göteborgs Stad och som omfattas av support från Intraservice.

De vanligaste funktionerna är beskrivna nedan översiktligt, däremot inte alla enskilda appar.

Användning gällande olika datatyper finns även översiktligt beskriven nedan. För en djupare beskrivning av de olika funktionerna, se separata *tjänstespecifikationer.*

2.7.1 Microsoft Teams

Teams är en tjänst för kommunikation likt telefoni för e-möten, chatt och e-samarbete där personal kan genomföra videomöten. Teams samlar ihop och bygger på befintliga Microsoftprodukter. Utöver videokonferenser använder Teams användaridentiteter lagrade i Azure Active Directory (Azure AD) och integreras med de andra tjänsterna inom O365 för att skapa en Sharepoint online-webbplats, en Office 365-grupp och en Exchange-gruppbrevlåda för varje team som skapats.

2.7.2 E-post – Exchange Online och Outlook

Exchange online är en produkt hos Microsoft som tillhandahåller den funktionalitet som används i Outlook. Här har vi funktioner som e-post, kalender, adressbok, att-göra lista. Det är en molnbaserad produkt som användaren kan komma åt via web, lokal applikation eller mobil klient. I första hand är det data som användaren har matat in eller data som har kommit användaren till del via e-post och kalenderfunktionalitet som behandlas. Dessa data innehåller i stor omfattning personuppgifter.

2.7.3 Onedrive online och Sharepoint Online

Onedrive och Sharepoint Online är funktioner för att spara, dela och samarbeta med dokument och data. Den finns som webbaserad funktion så väl som appar för Windows och Mac OS samt för Android och iOS system. Onedrive och Sharepoint används till att behandla och dela på många typer av dokument och filer så som exempelvis Microsoft Office dokument, bilder, video, att-göra listor, bloggar och strukturerade listor.

2.7.4 Microsoft 35 Apps för Enterprise

Microsoft 365 Apps är ett paket av programvaror som för kontorsarbete som installeras lokalt på en Windows eller Mac OS dator. Tidigare kallades detta för Officepaketet och det innehåller bland annat Word, Powerpoint, Excel, Onenote och Publisher. Detta kallas även "feta klienter" som körs på en dator.

2.7.5 Office mobila appar

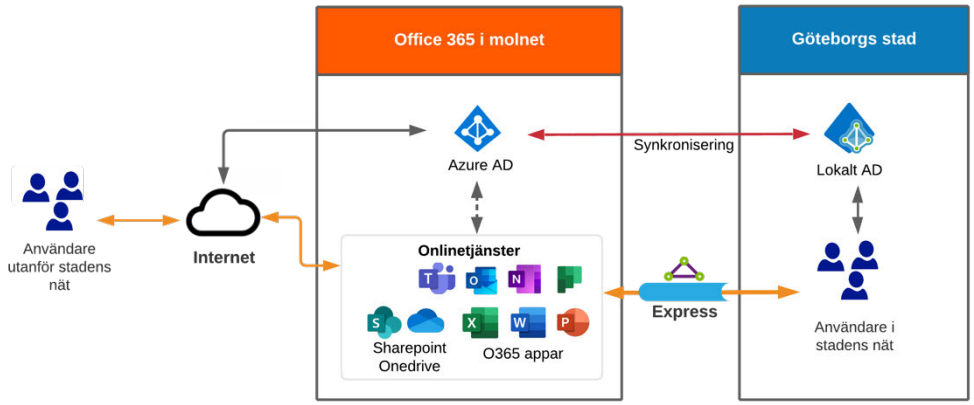
För mobila enheter och operativsystem finns även Word, Excel och Powerpoint samt andra appar där kommunens användare kan skapa, kommunicera och samarbeta. Microsoft Office mobile apps motsvarar Microsoft 365 Apps for enterprise men körs på Android eller iOS mobila enheter.

2.7.6 Office för webben

Office för webben är en webbtjänst som körs i Microsofts Azure miljö. Office för webben hanterar Office-filer var som helst med en internetanslutning.

2.8 Beskriv tjänstens IT-arkitektur

O365 är en SaaS tjänst som tillhandhålls av Microsoft (bild nedan). Göteborgs Stad använder Microsofts molntjänst och har inte en hybrid lösning (där delar av O365 skulle vara i drift lokalt av Intraservice)



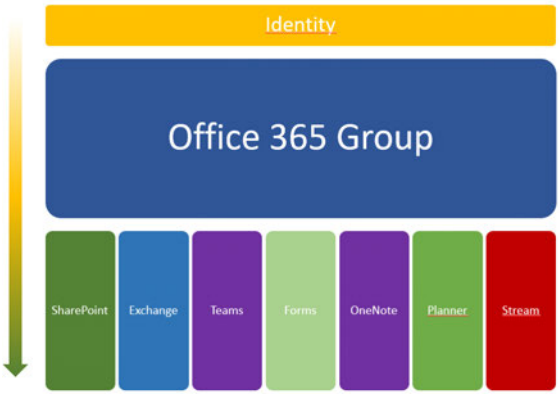
Figur 3- Microsoft molntjänster för att visualisera att O365 är en Saas tjänst hos Microsoft

De flesta funktionerna i Office 365 körs som ”Software as a Service” tjänster i Microsofts Azure moln. Göteborg stad har valt att ha egna redundanta AD servrar i egna datahallar för att säkerställa att användare kan logga in och vara autentiserade även om det skulle bli problem med Azure AD eller problem med kommunikationen. Servrarna synkroniserar den information som behövs för att säkerställa att användare kan arbeta även om det skulle bli störningar i AD funktionen. För att hålla god säkerhet sker synkronisering med jämna mellanrum och autentisering via certifikat av AD och Azure AD. Kommunikationen mot Azure AD sker via en TLS-tunnel.[3]

2.9 Behörigheter inom tjänsten

För att tilldela behörigheter inom tjänsten så använder vi Office 365 grupper. I dessa samlar vi grupper av personer som behöver samarbeta. Gruppen får tillgång till verktyg såsom Sharepoint, Planner, Stream och Teams. Gruppen använd också för att ge medlemmarna behörighet till gemensamma filer.

[3] TLS 1.2 källa: https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-install-prerequisites.



Figur 4 – Principen med Office 365 grupper för behörighetstilldelning

Behörighetstilldelning sker i övrigt enligt andra processer inom staden och beskrivs inte i denna riskanalys närmre.

3 Personuppgifter, känslighet och tjänstens karaktär

Som underlag för att bedöma riskerna för individer, beskrivas de uppgifter som hanteras inom tjänsten nedan. För en rättvisande sammanställning av vilka kategorier av registrerade och uppgifter som finns behövs information från personuppgiftsansvarig. Denna riskanalys förhåller sig på en övergripande nivå och summerar endast översiktliga kategorier.

3.1 Kategorier av registrerade

I den mån vi vet så ange vilka kategorier av registrerade som hanteras i tjänsten. Exempelvis: Anställda, Elever, Leverantörer etcetera

Anställda och konsulter i Göteborg Stad samt deras externa kontakter som hanteras i O365.

3.2 Kategorier av personuppgifter

Vilka kategorier av personuppgifter behandlas?

Beskrivning och kommentarer:

Denna riskanalys sammanfattar inte de förmodade kategorier av personuppgifter som kan vara innehållsdata. Uppgifter som är relevant i sammanhanget är olika kategorier av gemensamma uppgifter som är relaterade till Göteborgs stads verksamheter som myndigheter och kommunala bolag samt funktions och diagnosdata

3.3 Tillgång till personuppgifter

Vilka tjänstemän och andra roller kommer ha tillgång till uppgifterna?

Beskrivning och kommentarer:

Behörigheter är relaterade till respektive användare och grundprincipen är att endast de som behöver tillgång skall ha tillgång till de uppgifter som behövs för att utföra sitt arbete. Generella organisatoriska säkerhetsåtgärder följer Göteborgs stads regelverk. I regel har användare tillgång till sina egna uppgifter och andras uppgifter i det arbete man utför tillsammans.

3.4 Omfattning av personuppgifter i tjänsten

Beskriv i vilken omfattning som de olika kategorierna av personuppgifter behandlas.

Omfattningen varierar utifrån hur aktiv individen är i sitt användande av O365. Omfattningen av antal användare är stor, upp till ca 55 000.

4 Individers rättigheter

4.1 Tillämpliga rättigheter

I artiklarna 12–21 GDPR finns det rättigheter för den enskilde. Vilka artiklar blir aktuella av den aktuella behandlingen?

☒ Art. 12 – Informationspolicy om hur personuppgifter behandlas

☒ Art. 13 – Informationsskyldighet när enskild lämnat uppgiften

☒ Art. 14 - Informationsskyldighet när annan än enskild lämnat uppgiften

☒ Art. 15 – Registerutdrag

☒ Art. 16 – Rättelse

☒ Art. 17 – Radering

☒ Art. 18 – Begränsning av behandling

☒ Art. 19 – Anmälningsskyldighet till mottagare

☐ Art. 20 – Dataportabilitet

☒ Art. 21 – Invändning

Beskrivning och kommentarer:

Alla ovan beskrivna rättigheter faller inom ramen för behandlingar som utförs inom O365 av PUA.

Intraservice som tjänsteleverantör och PUB kan bistå PUA med hantering av registrerades rättigheter på följande sätt för tjänsten O365. Där det nedan står ”Hanteras av PUA” innebär det att rättigheten hanteras av PUA och PUB bistår enligt tjänstebeskrivning och tillhörande styrande dokument.

Art 12 – Hanteras av PUA. Staden har gemensam policy för detta ”Riktlinjer för personuppgiftsbehandling i Göteborgs Stad”

Art 13 – Hanteras av PUA

Art 14 – Användarinformationen (gemensamma innehållsdata) kommer från Skatteverket via HR-system till AD, Detta ska framgå av PUA:s avtal med registrerade.

Art 15 - Registerutdrag: Intraservice beskriver behandling av PU för Gemensamma innehållsdata, Funktionsdata samt diagnosdata.

Art 16 – Hanteras av PUA

Art 17 – Användarinformation följer PUA:s information om anställning i staden.

När kontot avslutas ligger kontoinformationen kvar i 30 dagar och backup finns kvar i 90 dagar. Rutin för återläsning finns.

Art 18 – Vissa del-tjänster kan användaren själv styra begränsningar. PUA kan också styra med rekommendationer till sin organisation.

Obligatoriska tjänster kan inte begränsas. Ej obligatoriska tjänster kan påverkas via inställningar av användaren.

För vissa delar av diagnosdata kan användaren styra omfattningen.

Art 19 – Hanteras av PUA

Art 20 – Tjänsten stödjer inte dataportabilitet.

Art 21 – Hanteras av PUA

5 Säkerhet vid behandling av personuppgifter i tjänsten

5.1 Administrativa åtgärder

Administrativa säkerhetsåtgärder definierar roller, ansvar, policyer, processer, åtgärder och hantering av informationssäkerhet och dataskydds åtgärder. Dessa säkerhetsåtgärder inkluderar alla aspekter av åtgärder som är nödvändig för att övervaka och hantera konfidentialitet, riktighet, tillgänglighet och personlig integritet gällande den skyddsvärda information, och för att hantera de personer som använder den, fastställa användningsprincipen och fastställa standarder för utförande.

Grundläggande säkerhetsnivåer i Office 365 är beskrivna i rapporten *Bedömning av Microsofts grundsäkerhetsnivå gällande Office 365* (Göteborgs Stad Intraservice, 2018b). I rapporten har man tittat på de säkerhetscertifieringar och rapporter som Microsoft presenterar gällande den säkerhet för de tjänster som Göteborg Stad använder.

Rapporten kommer fram till att man inte ser några hinder till att använda Office 365 för information av informationssäkerhetsklasserna 0, 1 och 2. Klass 2 motsvaras i stadens klassningsmodell av känsliga personuppgifter enligt Dataskyddsförordningen samt uppgifter som innefattar sekretess enligt Offentlighets och sekretesslag (OSL 2009:400). Däremot uppfylls inte de krav som ställs för att behandla information som omfattas av säkerhetsskyddslagstiftningen.

Flertalet dokument och ställningstaganden är gjorda gällande användning av klass 2-information.

Om *klass 2 skulle tillåtas* behöver information ske till användarna gällande e-post och samarbetsytor.

För att kunna skicka e-post med känslig information till såväl interna mottagare som externa måste e-posten vara krypterad. Det vill säga e-post med information som klassas i nivå 2 med ett utökat skyddsbehov. Detta sker genom att användaren väljer markeringen känslig då e-posten skrivs. Genom att markera e-posten som känslig kommer informationen att krypteras i Outlook samt märkas och få behörigheter hanterade i Microsoft Azure molntjänst.

För att kunna använda samarbetsytor i Sharepoint för hantering av känslig information av klass 2, ska det tydligt framgå att det är en yta där klass 2 information hanteras.

Det kan även finnas ytterligare administrativa åtgärder som behöver införas innan klass 2-information tillåtas.

5.2 Tekniska åtgärder

Tekniska säkerhetsåtgärder är de mekanismer som används inom IT-infrastrukturen i en organisation som inkluderar åtgärder som är nödvändiga för att tekniskt övervaka och hantera konfidentialitet, riktighet, tillgängligheten och personlig integritet för den skyddsvärda information, och för att hantera de tekniska system och objekt som använder den.

5.2.1 Inbyggt dataskydd

Inbyggt dataskydd och dataskydd som standard (norm) har målet att säkerställa att processer och system är utformade så att inhämtande och behandling (inklusive användning, utlämnande, bevarande, överföring och radering) begränsas till det som är nödvändigt för det identifierade ändamålet. Flertalet tekniska säkerhetsåtgärder finns inbyggda i tjänsten O365 och är delvis del av infrastruktur och andra tjänster, vilka är införda av Intraservice och återges inte i detalj.

5.2.2 Kryptering

Kryptering av data i Microsofts Azure molntjänst fungerar för de flesta funktioner inom Office 365, men dock inte alla. Här ser vi funktioner som Teams och Yammer som inte kan skyddas i dagens molntjänst utan det data lagras alltid okrypterad.

Gällande kryptering av data så kan vi se det i två delar, kryptering av data i vila och kryptering av data i rörelse. Generellt är kryptering av data i rörelse hanterat via TLS (Transport Layer Security). Vid kryptering av data i vila använder sig Microsoft av AES-256. Detta är en standardiserad krypteringsalgoritm som anses vara säker att hantera skyddsvärda personuppgifter.

5.2.3 Customer Lockbox

Customer Lockbox är en funktion från Microsoft för att ge rättigheter till tekniker och annan personal för åtkomst till data som är lagrad i Microsoft Azure molntjänst. Det innebär också att ägaren kan begränsa åtkomsten till data i tid så att det bara är möjligt för Microsofts supportperson att komma åt data under den tid som ägaren har specificerat.

Det är viktigt att veta att det trots Lockbox finns möjlighet för Microsofts IT-personal att komma åt data genom att använda administratörsrättigheter som då kan gå förbi Lockbox genom åtkomst direkt till data i molnet.

Med tanke på utlämnande till tredjeland så ger Customer Lockbox inget ytterligare skydd då Microsoft har full åtkomst till data och det enbart är skyddat genom avtal och inte med en ytterligare teknisk säkerhetslösning. För djupare genomgång se *Bedömning av Customer Lockbox (Göteborgs Stad Intraservice, 2018a).*

Customer Lockbox har inte ansetts skapa en tillräcklig säkerhet och används därför inte längre av staden (Göteborgs Stad Intraservice, 2021b).

6 Tredjelandsöverföring

Det finns strikta regler i dataskyddslagstiftningen för när personuppgifter får lämnas till länder utanför EU/EES, så kallat tredjeland. Detta gäller all överföring, även till personuppgiftsbiträde som inte själva använder personuppgifterna i sin verksamhet utan bara lagrar, driftar, supportar, utvecklar, underhåller eller servar systemet. Observera att ordet överföring även omfattar åtkomst till personuppgifterna i tredjeland, även om de lagras inom EU/EES.

6.1 Förekomst

Överförs personuppgifter till tredjeland eller internationell organisation?

☒ JA. ☐ NEJ

Ange vilket tredjeland och mottagare

Mottagaren kan vara en extern verksamhet som finns utanför EU/EES. Vem mottagaren är kan vara av intresse bland annat för vilka avtal som ska ingås. Exempel: "Biträde X i USA", "Intern verksamhet Y i Japan", "Internationell organisation Z".

O365 är en SaaS-tjänst som levereras av Microsoft Corporation Inc. Lagring sker inom EU men överföring av vissa funktionsdata och diagnosdata sker till tredjeland, dvs Microsoft i USA samt till Microsofts underbiträden.

6.2 Grund för tredjelandsöverföring

På vilka grunder sker överföringen till tredjeland eller internationell organisation?

☒ EU-kommissionens standardavtalsklausuler (SCC)

☐ Bindande företagsbestämmelser (Binding Corporate Rules, BCR)

☐ EU-kommissionen har godkänt mottagandet som har ansetts ha en godkänd skyddsnivå

☐ Godkänd certifieringsmekanism

☐ Godkänd uppförandekod

☐ Eget avtal mellan parterna som godkänts av tillsynsmyndigheten

☐ Viktigt allmänintresse

☐ Avtal med den registrerade

☐ Rättsliga anspråk

☐ Samtycke

☐ Annat

Beskrivning och kommentarer:

Microsoft har i personuppgiftsbiträdesavtalet, Data Protection Addendum (DPA) meddelat att de stödjer tredjelandsöverföringen på EU-kommissionens standardavtalsklausuler. Detta meddelades av Microsoft i deras DPA från den 21 juli 2020 och senare versioner (Microsoft, 2020).

Gällande tredjelandsöverföringen till USA är det inte tillräckligt med att överföringen enbart använder överföringsmekanismen SCC. Kompletterande åtgärder behöver finnas på plats för att hantera Schrems 2 men även till viss del Cloud Act. Sammantaget behövs åtgärder för att minska dessa risker, vilket behöver hanteras i en analys av tredjelandsöverföringen (Transfer Impact Assessment).

Sedan december 2020 har Microsoft en uppdaterad DPA som adderar nya tillägg med kompletterande skyddsåtgärder till standardavtalsklausulerna. Microsoft utlovar en kompensation för registrerade vid ett eventuellt utlämnade till amerikansk underrättelsetjänst samt att de ska med alla lagliga medel försöka förhindra utlämnande.

Tjänsteutlåtandet *Redogörelse för Intraservice arbetssätt och metod för utveckling av Kommungemensamma interna tjänster med stöd av molntjänstleverantörer* daterad 2021-05-25 antogs av nämnden för Intraservice 2021-06-15. Detta dokument är även en bilaga till denna riskanalys. Här konstateras att rättsläget är osäkert gällande amerikanska molntjänst-leverantörer och att det i hög grad påverkar på vilket sätt som nya tjänster kan startas. Vidare konstateras att Intraservice kommer fortsätta med att utreda och bedöma molntjänster i Kommungemensamma interna tjänster. Dokumentet innehåller en grundlig redogörelse för problematiken på området, inkluderar flera juridiska analyser och innehåller även en omfattande omvärldsbevakning.

6.3 Tolkning gällande Schrems II

Intraservice tolkning är för närvarande att EU-domstolen (Court of Justice the European Union eller CJEU) beslut Case C-311/18 Schrems II innebär att Privacy Shield inte är tillämpbart (CJEU, 2020). Standardavtalsklausuler i kontrakt (EU-kommissionen 2010/87) samt Bindning Coperate Rules (BCR) kan fortfarande vara tillämpbara med extra juridiska mekanismer och skyddsåtgärder under vissa förutsättningar i enlighet med dataskyddastyrelsens rekommendationer från EDPB.

EU domstolen har i målet konstaterat att beslut 2010/87 om standardavtalsklausuler innehåller sådana effektiva mekanismer som i praktiken gör det möjligt att säkerställa att den skyddsnivå som krävs enligt unionsrätten iakttas och att överföringar av personuppgifter med stöd av sådana dataskyddsbestämmelser avbryts eller förbjuds om dessa bestämmelser

åsidosätts eller är omöjliga att iaktta. Domstolen konstaterade att beslut 2010/87 om standardavtalsklausuler innehåller sådana mekanismer.

Domstolen framhöll i detta avseende bland annat att beslutet innebär en skyldighet för exportören och importören av personuppgifter att i förväg kontrollera att den skyddsnivå som krävs enligt unionsrätten iakttas i det berörda tredjelandet.

Utöver detta innebär beslutet även en skyldighet för importören (Microsoft) av personuppgifter att informera exportören (PUA i Göteborgs stad) om att importören eventuellt inte kan följa dessa standardavtalsklausuler, åligger exportören att avbryta överföringen av personuppgifter och/eller häva avtalet med den importören.

I DPA (Microsoft, 2022, s. 9) står det under rubriken "Data Transfers and Location" att Microsoft förbehåller sig rätten att överföra innehållsdata och andra personuppgifter. Eftersom direkta personuppgifter ska vara kvar i EU/EES enligt ovan stycke, rör detta indirekta personuppgifter:

> [...] Taking into account such safeguards, Customer appoints Microsoft to transfer Customer Data, Professional Services Data, and Personal Data to the United States or any other country in which Microsoft or its Subprocessors operate and to store and process Customer Data, and Personal Data to provide the Products, except as described elsewhere in the DPA Terms.
>
> All transfers of Customer Data, Professional Services Data, and Personal Data out of the European Union, European Economic Area, United Kingdom, and Switzerland to provide the Products and Services shall be governed by the 2021 Standard Contractual Clauses implemented by Microsoft.

EU-kommissionens antog 2021 nya standardavtalsklausuler (EU-kommissionen 2021/914) för tredjelandsöverföring som ersätter de tidigare (EU-kommissionen 2010/87). De adresserar olika förhållanden såsom PUA>PUA, PUB>PUA, PUB >PUB, PUB>PUA och flerpart. Exportörer i de nya SCC kan alltså även vara en PUB. Intraservice i tjänsteleveransen är ett personuppgiftsbiträde och alltså gäller förhållandet PUB>PUB. Här ställs krav på att exportören (Intraservice i detta fall) ska införa säkerhetsåtgärder som efterlever Dataskyddsförordningen.

> The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter ‘personal data breach’). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subject. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter or the controller. In complying with its obligations under this paragraph, the data importer shall at least

> implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

Enligt tidigare rekommendationer från EDPB, vilka syftar på de äldre standardavtalsklausulerna finns inga tekniska åtgärder, så länge data hanteras okrypterad hos importören (Microsoft). Andra administrativa åtgärder kan säkerställa exportörens skyldigheter, men detta innebär att olika PUA i Göteborgs stad behöver göra en bedömning av själva tredjelandsöverföringen, en så kallad (Transfer Impact Assessment) i enlighet med EDPB:s riktlinjer.

Här skulle det behövas att krav ställs på Microsoft att inte överföra någon data från EU/EES, inte ens funktionsdata eller diagnosdata samt göra innehållsdata helt otillgänglig för utlämning. Om Microsoft inte kan efterleva kraven, återstår endast att avbryta överföringen. Microsoft menar, att de kan följa amerikansk lag och ändå efterleva kraven i SCC, tack vare av nya tillägg gjorts gällande kompensation för registrerade och att de ska försöka förhindra utlämnande, vilka beskrivs under *ytterligare säkerhetsåtgärder*.[4] Se text under "Processor and Controller Roles and Responsibilities" (Microsoft, 2022, s. 7):

> [...] With respect to processing of Personal Data under this paragraph, Microsoft makes the commitments set forth in the Additional Safeguards section; for those purposes, (i) any Microsoft disclosure of Personal Data, as described in the Additional Safeguards section, that has been transferred in connection with business operations is deemed a “Relevant Disclosure” and (ii) the commitments in the Additional Safeguards section apply to such Personal Data.

6.4 Behov av Transfer Impact Assessment (TIA)

Europeiska dataskyddsstyrelsen (EDPB) släppte 2020-11-11 två dokument:

- Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data (EDPB, 2020a). Dessa rekommendationer har uppdaterats och är slutgiltigt färdigställda 2021-06-18 (EDPB, 2021).
- Recommendations 02/2020 on the European Essential Guarantees for surveillance measures (EEG) (EDPB, 2020b)

Dessa dokument vägleder hur en analys av överföring till tredjeland kan ske– en så kallad *Transfer Impact Assessment (TIA).*

Sex steg föreslås i det 01/2020 dokumentet (EDPB, 2021):

1. Skapa en kartläggning av behandlingens laglighet, vilket är samma krav som i artikel 30.
2. Välja mekanism (SCC)
3. Undersöka 3:e landet (lagar, fall, praxis)

[4] Appendix C *ytterligare säkerhetsåtgärder* (Additional Safeguards Addendum)

   a. Rättigheter för registrerade
   b. Redress (juridisk möjlighet för registrerade till att få rättslig prövning och upprättelse, *gottgörelse*)
   c. Myndigheters agerande (och access)
   d. **Bedöm på Makro-nivå** (EEG) och **Mikro-nivå** för PUB och PUA i Göteborg med dess användning av O365 (relevant inom sektorn av den typ av uppgifter som används)
4. Kompletterande åtgärder (avtalsmässiga, organisatoriska och tekniska)
5. Implementera kompletterande åtgärder
6. Bevaka och uppdatera vid förändring av lagar (tredjeland eller EU) eller förändring av data man avser behandla (eller process för detta) samt avbryt överföringen om ingen annan möjlighet kvarstår.

Det andra dokumentet 2/2020 är EDPB:s rekommendationer för att utvärdera andra staters övervakningslagar mot bakgrund av europeiska grundläggande rättigheter (European Essential Guarantees - EEG). Detta innebär ett minsta krav enligt EU-lag och fördrag "så nära som det går" med tanke på vad som är rimligt gällande övervakning i ett demokratiskt samhälle(EDPB, 2020b).

Fyra garantier ska uppfyllas:

A. Behandling bör baseras på tydliga, exakta och tillgängliga regler
B. Nödvändighet och proportionalitet för legitima mål som eftersträvas behöver visas
C. Oberoende tillsynsmekanism
D. Effektiva rättsmedel måste vara tillgängliga för den enskilde

6.4.1 TIA och analys av tredjelandsöverföring i O365

De faktorer som en TIA ska vila på ska vara ”...relevanta, objektiva, pålitliga, verifierbara och allmänt eller på annat sätt tillgängliga”. En riskvärdering ska inte vara baserad på godtycklig sannolikhet. En TIA ska förhålla sig till konkreta fakta som finns tillgänglig. Det finns därmed utrymme för att tolka Microsofts transparens och vad för faktiska förhållanden och avtalsvillkor som finns i DPA och med stöd av objektiva offentliga källor samt information som finns i Microsoft Trust Center.[5]

EDPB (2021):

> 47. You may also take into consideration documented practical experience of the importer with relevant prior instances of requests for access received from public authorities in the third country. […]
> You will be able to consider this information, together with other types of information obtained from other sources, as part of your overall assessment of the laws and practices of the third country in relation to your transfer.

Gällande risker för personuppgiftsbehandlingarna i tjänsteleveransen för O365 som ska överföras, behöver de vara i linje med Artikel 32 om *lämpliga säkerhetsåtgärder i förhållande till risken*. Det finns med en specifik hänvisning till känsliga uppgifter enligt definitionerna i artiklarna 9 och 10 i dataskyddsförordningen om att beakta känsligheten för uppgifterna och

[5] Rapporter om begäranden från amerikanska myndigheter för ändamål med brottsbekämpning samt nationell säkerhet finns på: https://www.microsoft.com/sv-se/trust-center

potentiellt andra kontextuella faktorer i överföringsanalysen, om vilka kompletterande åtgärder som kommer att vara tillräckliga. Ställningstagandet för Göteborgs stad är i nuläget är att det inte går att överföra uppgifter som omfattas av stadens informationssäkerhetsklass 2, vilka omfattar känsliga samt extra skyddsvärda personuppgifter. Därför antas personuppgifter som ska överföras i att vara klass 1 eller lägre. Därtill behöver varje personuppgiftsansvarig göra en subjektiv bedömning om de kategorier av personuppgifter som överföringen omfattar som baseras på objektiva faktorer som presenteras i en TIA.

I de uppdaterade rekommendationerna från Europeiska dataskyddsstyrelsen den 18 juni 2021 för extra skyddsåtgärder ges utrymme för riskanalys med subjektiv bedömning (EDPB, 2021).

Dock måste en subjektiv bedömning baseras på objektiva faktorer. I tjänsteleveransen gäller Intraservice aspekter gällande tredjelandsöverföring främst artikel 32 gällande säkerhet i samband med behandlingen. Med denna utgångspunkt sker alltså riskhanteringen.

En TIA omfattar innehållet i de sex stegen i rekommendationerna från EDPB. Den subjektiva bedömningen baserad på objektiva faktorer sker inte i TIA, utan i en framtida uppdaterad version av detta dokument. En TIA är framtagen, enligt tidigare riskanalys, men det är för närvarande ett arbetsdokument. TIA:n omfattar både begärande av amerikanska myndigheter från brottsbekämpande ändamål, såväl som för nationella säkerhetsändamål. Dock är arbetet avstannat, då DSO ej anser att Intraservice ska göra en TIA-bedömning av landet "[…] då EU-domstolen redan gjort en bedömning av skyddsnivån i USA genom Schrems II-domen" (Intraservice Dataskyddsenheten, 2022a). I stället rekommenderar DSO att fokus ska vara på typ av data och hur denna hanteras/förekommer/behandlas inom de olika delarna av tjänsten och förvaltningens möjligheter samt utreda och vidta tillräckliga skyddsåtgärder för att skydda de registrerades fri- och rättigheter. Vidare rekommenderar Dataskyddsenheten att bara följa stegen i EDPB:s rekommendationer ”Om överföring av personuppgifter sker till ett land utanför EU/EES **som inte är USA** saknar adekvansbeslut […]” (Intraservice Dataskyddsenheten, 2022b).

Riskerna 16 och 17 adderades under avsnitt 7.8 nedan för att utgå från underlaget i en TIA. Dessa risker är inte bedömda, eftersom de förutsätter att en TIA görs. I denna uppdaterade riskanalys tillkommande risker sker indelning på datatyper och riskerna #16–17 är tillfälligt ersatta av riskerna #18–30, som mer precist visar förekomst av risker för tredjelandsöverföring. Flertalet av dessa risker gäller specifikt innehållsdata och det sker ingen värdering i denna riskanalys, men riskidentifieringen kan användas som underlag för andras bedömningar.

6.5 Hemtagning

En ytterligare slutsats blir även att Göteborgs stad behöver förbereda en realistisk strategi för hemtagning, även om den kanske inte realiseras. I ett kort perspektiv är det inte realistiskt att flytta från Microsoft Office 365, men det kan

finnas hybridvarianter att köra vissa tjänster lokalt installerade (on prem). Det kan också innebära minskad säkerhet, och eventuellt högre kostnader för Intraservice än via Microsoft Office 365, vilket var en av anledningarna att tjänsten infördes. Ett konkret förslag behöver emellertid finnas och därefter behöver bevakning efter lämpliga alternativ eller hybrid-alternativ utvärderas löpande.

Detta är i linje med sista steget, punkt 63 i det första dokumentet (EDPB, 2020a) :

> 63. You should put sufficiently sound mechanisms in place to ensure that you promptly suspend or end transfers where:
> - the importer has breached or is unable to honour the commitments it has taken in the Article 46 GDPR transfer tool; or
> - the supplementary measures are no longer effective in that third country.

Vidare analys av alternativ för riskhantering gällande tredjelandsöverföringar i Office 365 avseende Schrems II finns i. bilaga *3, TU – Redogörelse för Intraservice arbetssätt och metod för utveckling av Kommungemensamma interna tjänster med stöd av molntjänstleverantörer.*

7 Risker och åtgärder

Riskanalys är utförd enligt Intraservice strukturerade riskhanteringsprocess med medverkande från verksamheten, projektet, systemförvaltning och dataskyddsombud (se medverkande). Nedan presenteras riskvärdering före riskbehandling och resthantering med riskvärdering efter genomförande av åtgärder. Utgångspunkten för riskhanteringen är att grundläggande skydd genom administrativa och tekniska åtgärder är införda.

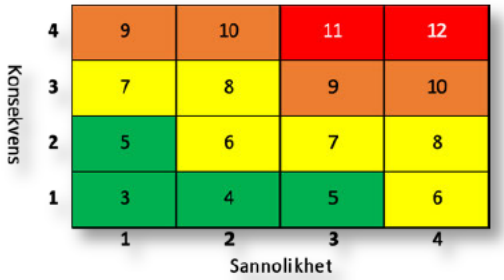
Själva riskvärderingen har dokumenterats i excelformat och återfinns i bilagan *O365 Riskanalys Dataskydd v3.0* och omfattar riskerna R1–R30. Riskerna 16 och 17 har är ej bedömds och ersätts i aktuell riskhantering av riskerna 18–30, som mer precist visar förekomst av risker för tredjelandsöverföring.

7.1 Riskhanteringsmetod

Riskhanteringen sker med utgångspunkt av konsekvenser och sannolikhet för att risker ska inträffa. Den påverkan för individen som kan bli följden av en situation bör bedömas med hänsyn tagen till konsekvenser som förlust av konfidentialitet, riktighet, tillgänglighet eller personlig integritet. Sannolikheten är hur frekventa hoten är och hur enkelt sårbarheterna kan utnyttjas.

- Värdering av konsekvens sker i en skala mellan 1 och 4.
- Värdering av sannolikhet sker i en skala mellan 1 och 4.
- Riskvärdet räknas ut i analysen och sker enligt formeln Sannolikhet + konsekvens x 2.

Illustration av riskvärden finns Figur 6 - Riskvärde och olika grader av allvar av konsekvenser



Figur 5 - Riskvärde och olika grader av allvar av konsekvenser

Olika risker behöver åtgärder som motsvarar riskvärderingen. Nedan illustration i Figur 7 - Riskbehandlingsalternativ för prioritering av risker är en fingervisning om *när* åtgärder behöver sättas in och en hjälp att prioritera olika skyddsåtgärder. För riskerna i analysen är de som PUB själva kan implementera redan införda av riskanalys som utfördes i *O365 Riskanalys Dataskydd v3.0* vilken är bilaga 1.

Röd	Risker som kräver omedelbara åtgärder
Orange	Risker som kräver åtgärder
Gul	Risker som skall bevakas och planeras åtgärder för
Grön	Risker som anses hanterade eller behöver inte hanteras

Figur 6 - Riskbehandlingsalternativ för prioritering av risker

7.1.1 Summering av riskhantering före åtgärder

Riskvärde	Antal	Risker
11–12	0	–
9–10	2	R5 Skyddade identiteter i adressboken R6 Tillgång till information vid byte av tjänst
6–8	13	R1 Intrång av obehöriga R2 Intrång av leverantör R3 E-post kommer inte fram till mottagaren R4 Kalenderinformation kan ses och ändras R8 Röjande av information vid registerutdrag R9 För generösa behörigheter i Sharepoint R14 Chatt i Teams sparas "för evigt" R15 Inspelningar lagras i Teams tills arkivering R21 Bristande transparens och begränsning från Microsoft gällande säkerhetshändelser R22 Bristande transparens i Office för Webben för överföring av diagnosdata R23 Tillfälliga överföringar från Onedrive av användarnamn, e-postadresser och sökvägar R25 Samtal i Teams inkluderar vilka konton/användare som samtalar och när. R26 Diagnosdata kan innehålla uppgifter i klartext trots pseudomymiseing
3–5	7	R7 Krypterade mail kan inte öppnas R10 Nedladdning till privat dator R11 Delve utan klart syfte för Göteborgs Stad R12 MyAnalytics utan klart syfte för Göteborgs Stad R13 Inställningar och tjänster ändras R28 Supportärenden: Kontodata kan inkluderas i kommunikation med MS R29 Supportärenden kan överföras tillfälligt till underleverantörer i tredjeländer
Ej bedömda	9	R16 Uppgifter delas med amerikanska myndigheter (Cloud Act) R17 Uppgifter delas hemligt med amerikanska myndigheter (Schrems 2) R18 Möjlig otillåten övervakning av personuppgifter som lagras och hanteras i Office 365 (innehållsdata) R19 Bristande kontroll över vad som och hanteras i Office 365 (känsliga personuppgifter) R20 Viva behandlas och lagras på Microsofts servrar i USA R24 Bristande kontroll: Data delas med Microsoft och tredjeparter som Bing samt Cloudflare som är egna PUA R27 Oförmåga att utöva den registrerades rätt till tillgång för nödvändiga servicedata i DDV. R30 Samtal i Teams vid flerpartssamtal kan avlyssnas R31 Övervakning av anställda (Teams analytics och Viva Insights)

7.2 Riskbeskrivningar

Nedan är en sammanfattning av de riskerna med högst riskvärde samt nytillkomna risker (18–31) samt ej bedömda risker.

Beskrivning av tabell: **Konsekvenser för hur individers personuppgifter kan påverkas:**

Konfidentialitet (K), Obehörig åtkomst till eller röjande av PU
Riktighet (R), Oönskad ändring av PU
Tillgänglighet (T), Förlust av PU

Sannolikhet (Sa) 1–4, Osannolikt, Möjlig, Sannolik, Mycket Sannolik (se Appendix 8.2 för definitioner)
Konsekvens (Ko) 1–4, Försumbar, Måttlig, Allvarlig, Mycket allvarlig (se Appendix 8.1 för definitioner)
Riskvärde (Rv) är en sammanlagd värdering av sannolikhet och konsekvens och är ett stöd för prioritering av risker

#	Beskrivning	Påverkar	Kommentar och åtgärder för riskhantering	Riskvärde
R1	**Intrång av obehöriga** Risk för … obehörig åtkomst, obehörigt röjande, förlust av uppgifter eller oönskad ändring av uppgifter …på grund av… intrång av obehöriga externa användare. … vilket leder till … Påverkan av större eller mindre art för individen när obehörig får del av information och de personuppgifter som lagras i tjänsterna och kan ändra data. Förlust av konfidentialitet och kontroll.	**K** **R** **T**	**Åtgärder** Tekniska säkerhetsåtgärder är redan införda, varför sannolikhet bedöms låg. Avser olaga intrång med uppsåt från staden-nära individer. Vi avser inte intrång såsom från främmande makt etc. *Acceptabel risknivå, på grund av införda tekniska åtgärder.*	**Sa: 1** **Ko: 3** **Rv: 7**
R2	**Intrång av leverantör** Risk för … obehörig åtkomst, obehörigt röjande, förlust av uppgifter eller oönskad ändring av uppgifter …på grund av… intrång av leverantören eller dess underleverantörer. … vilket leder till … Påverkan av större eller mindre art för individen när obehörig får del av information och de personuppgifter som lagras i tjänsterna och kan ändra data. Förlust av konfidentialitet och kontroll.	**K** **R** **T**	**Åtgärd** Avtalsmässiga åtgärder är införda Uppsåt saknas eller är lågt från leverantörens sida *Acceptabel risknivå på grund av införda avtalsmässiga åtgärder*	**Sa: 2** **Ko: 2** **Rv: 6**

#	Beskrivning	Påverkar	Kommentar och åtgärder för riskhantering	Riskvärde
R3	**E-post kommer inte fram till mottagaren** Risk för … Risk för att e-post försvinner, dvs kommer inte fram till mottagaren …på grund av… inställningar och regler i Spam-filter … vilket leder till … information viktig för mottagaren kommer inte fram utan ”försvinner”.	**T**	Post mellan myndigheter eller från myndighet till individ har fastnat i spam-filter. Spam-filter är en underliggande funktion utanför O365 plattformen **Åtgärder:** A1: Införande av process för förbättrad hantering av spam-filter och dess resultat. Ansvarig Fredrik Hjort. A2: Informera att e-posttjänsten inte ska användas för myndighetspost. *Efter åtgärder påverkas sannolikhet. Risken acceptabel efter föreslagna åtgärder.*	**Sa: 1** **Ko: 3** **Rv: 7**
R4	**Kalenderinformation kan ses och ändras** Risk för … obehörig åtkomst, obehörigt röjande, förlust av uppgifter eller oönskad ändring av uppgifter …på grund av… intrång av obehöriga externa användare. … vilket leder till … Obehörig får del av information och de personuppgifter som lagras i tjänsterna och kan ändra data. Förlust av konfidentialitet och kontroll.	**K** **R** **T**	**Åtgärd** A3: Informera om denna inställning i kalendern som individen kan göra själv. Dessutom informera om allmänna tips om hur rubriker på möten bör sättas för att undvika personuppgifter i dessa. *Efter åtgärder påverkas både sannolikhet och konsekvens. Risken acceptabel efter föreslagna åtgärder.*	**Sa: 1** **Ko: 3** **Rv: 7**

#	Beskrivning	Påverkar	Kommentar och åtgärder för riskhantering	Riskvärde
R5	**Skyddade identiteter i adressboken** Risk för … att personer med skyddad identitet visas i adressboken. Kontaktpersoner i adressboken visas på flera ställen i O365. …på grund av… information om personer är publik i staden. Det finns olika nivåer av skydd. I vissa fall finns personen inte med i adressboken alls. … vilket leder till … svårighet att göra riktig sekretessbedömning av uppgifter. Samt om information om personer med skyddad identitet sprids får detta mycket allvarliga konsekvenser för individen.	**K**	**Åtgärder** A4: Åtgärder för att minimera sannolikhet för att skyddade identiteter röjs är redan införda. Det är sedan tidigare säkerställt att AD-information inte innehåller någon märkning eller liknande som skulle indikera om individen har skyddad identitet. O365 har ingen egen information om skyddade identiteter. Underliggande teknik såsom Active Directory (AD) hanterar detta.	**Sa: 1** **Ko: 4** **Rv: 9**

#	Beskrivning	Påverkar	Kommentar och åtgärder för riskhantering	Riskvärde
R6	**Tillgång till information vid byte av tjänst** Risk för … att individen får tillgång till information från tidigare arbetsgivare om man bytt tjänst mellan förvaltningar inom Göteborgs Stad. …på grund av… att AD-kontot behålls … vilket leder till … är kvar i mailgrupper, har tillgång till filer etc från sin tidigare arbetsgivare, dvs information som individen ej längre är behörig till.	**K** **R**	**Åtgärder** A5: Diskussion pågår om att ändra process och hantering för ”flytt av konto” som istället ska vara ”ta bort konto” och ”skapa nytt konto”. A6: En fråga med konsekvenser för användaren då principiellt beslut behöver fattas om kontohantering i staden. Sannolikhet minskar avsevärt om ny rutin för kontohantering efterföljs vid byte av tjänst till annan förvaltning. Användarkontot finns kvar i mailgrupper, behörigheter till Sharepoint och Onedrive. O365 använder kontoinformation från Active Directory (AD).	**Sa: 3** **Ko: 3** **Rv: 9**

#	Beskrivning	Påverkar	Kommentar och åtgärder för riskhantering	Riskvärde
R7	**Krypterade mail kan inte öppnas** Risk för … att mail som skickas krypterat inte kan öppnas av mottagaren …på grund av… användaren vet inte hur man gör eller tekniska problem med kryptering. … vilket leder till … mottagaren kan inte ta emot viktig information. Om det krånglar kanske sändaren väljer att skicka känslig information okrypterat.	**K** **T**	**Åtgärder** A7: Informera om när kryptering ska göras. Det finns en missuppfattning om att det behövs kryptering mellan interna användare. T1: Granska tekniken för kryptering så att det är enkelt att göra rätt.	**Sa: 2** **Ko: 2** **Rv: 6**
R8	**Röjande av information vid registerutdrag** Risk för … att information röjs om individer då vi söker information för registerutdrag på uppdrag av PUA …på grund av… att instruktioner saknas från PUA om vad som vi som PUB får hantera och lämna ut. … vilket leder till … till information om andra individer än den som begärt registerutdrag kan komma att röjas. Alternativt omfattande arbete att ta bort denna information i underlagen.	**K**	**Åtgärder** A8: Process och rutin ska tas fram med roller och ansvar för hantering av begäran av information från PUA. Intraservice har en restriktiv syn på vilken information som utlämnas för att inte information om andra ska röjas. Intraservice har och kommer ha en mycket restriktiv syn på vad som kan lämnas ut, vilket medför att sannolikheten minskar.	**Sa: 4** **Ko: 2** **Rv: 8**

#	Beskrivning	Påverkar	Kommentar och åtgärder för riskhantering	Riskvärde
R9	**För generösa behörigheter i Sharepoint** Risk för … att behörigheter i Sharepoint tilldelas så att alla kan läsa. O365 ”Rekommenderade filer” visar filer från dessa ytor för individer utan uppenbar anledning. …på grund av… På grund av att informationsägaren tilldelar behörigheter i Sharepoint så att fler än avsett kan läsa. Risken finns på grund av funktioner i O365 som föreslår filer som hanteras av personer i individens närhet. … vilket leder till … att individer kommer åt information som inte är direkt avsett för dom samt att via Rekommenderade filer lockas öppna filer.	**K**	**Åtgärder** A9: Informera om behörighetshantering i Sharepoint och OneDrive. Sharepoint i allmänhet ska inte innehålla känslig information (klass 2). Endast efter att ha beställt och fått separat yta avsedd för klass 2-information kan sådan information hanteras där.	**Sa: 3** **Ko: 2** **Rv: 7**
R14	**Chatt i Teams sparas “för evigt”** Risk för … att chattar som sparats länge innehåller felaktig/gammal information …på grund av… att chatt i Teams sparas till dess att teamets yta ska arkiveras. … vilket leder till … möjlig osäkerhet hos individen om vilken information som finns lagrad.	**R**	**Åtgärd** A13: Informera om hur chatt fungerar i Teams och att inlägg sparas tills teams-ytan arkiveras. Individen kan själv gå in i Teams och redigera och ta bort chatt-inlägg.	**Sa: 2** **Ko: 2** **Rv: 6**

#	Beskrivning	Påverkar	Kommentar och åtgärder för riskhantering	Riskvärde
R21	**Bristande transparens och begränsning från Microsoft gällande säkerhetshändelser** Risk för… Möjlighet för amerikanska myndigheter att begära ut innehållsdata från Microsoft för nationella säkerhetsändamål utan kännedom eller skydd för individens fri- och rättigheter … på grund av… Bristande transparens gällande vilka data som inkluderas i 'säkerhetshändelser' då ingen begränsande beskrivning finns. Säkerhetshändelser skickas till Microsofts centrala säkerhetsloggar i USA. … vilket leder till… Övervakning: Microsoft och amerikanska myndigheter kan ta del av information om användare. Uteslutning: Personuppgifter behandlas utan individens vetskap eller delaktighet	K	**Åtgärder** A14: Hantera i Efterlevnadskontrollen (ELK) och riskhantering i samband med detta. A15: Användare kan informeras genom beskrivning av tjänsten vilken information som samlas in som diagnosdata. A16: Informera om att filnamn och sökvägar aldrig ska innehålla personuppgifter. Detta skulle kunna adresseras till SLK för att få en vidare spridning i staden. T4: Stickprov med MS verktyg kan jämföras data med loggar för nätverkstrafik. Omfattning behöver beskrivas. Detta kan ske inom ramen för ELK.	**Sa: 2** **Ko:4** **Rv: 8**

#	Beskrivning	Påverkar	Kommentar och åtgärder för riskhantering	Riskvärde
R22	**Bristande transparens i Office för Webben för överföring av diagnosdata till USA** Risk för… Möjlighet för amerikanska myndigheter att begära ut innehållsdata från Microsoft för nationella säkerhetsändamål utan kännedom eller skydd för individens fri- och rättigheter …på grund av… Diagnosdata skickas systematiskt till Microsoft i USA om användningen av Office för Webben. …vilket leder till… Övervakning: Amerikanska myndigheter kan ta del av information om användare.	K	**Åtgärder** A14: Hantera i Efterlevnadskontrollen (ELK) och riskhantering i samband med detta. A15: Användare kan informeras genom beskrivning av tjänsten vilken information som samlas in som diagnosdata.	**Sa: 3** **Ko: 2** **Rv: 7**

#	Beskrivning	Påverkar	Kommentar och åtgärder för riskhantering	Riskvärde
R23	**Tillfälliga överföringar från Onedrive av användarnamn, e-postadresser och sökvägar till USA** Risk för… Möjlighet för amerikanska myndigheter att begära ut funktionsdata/diagnosdata från Microsoft för nationella säkerhetsändamål utan kännedom eller skydd för individens fri- och rättigheter. …på grund av… trots inställningen 'neither' i insamlingen av telemetri avidentifieras inte samtliga data., som till exempel när flera redigerar ett dokument …vilket leder till… Övervakning: Amerikanska myndigheter kan ta del av information om användare.	K	**Åtgärder** A15: Användare kan informeras genom beskrivning av tjänsten vilken information som samlas in som diagnosdata. A16: Informera om att filnamn och sökvägar aldrig ska innehålla personuppgifter. Detta skulle kunna adresseras till SLK för att få en vidare spridning i staden. A17. Personer som har identitet skyddas med pseudonyma konton, som sker innan tjänsten. Detta återfinns i anvisning för skyddade identitet.	**Sa: 4** **Ko: 2** **Rv: 8**

#	Beskrivning	Påverkar	Kommentar och åtgärder för riskhantering	Riskvärde
R25	**Samtal i Teams inkluderar vilka konton/användare som samtalar och när** Risk för… Möjlighet för amerikanska myndigheter att begära ut gemensamma innehållsdata från Microsoft för nationella säkerhetsändamål utan kännedom eller skydd för individens fri- och rättigheter …på grund av… Microsoft har tillgång till mediaströmmen vid två- samt flerpartskommunikation i Teams …vilket leder till… Övervakning: Microsoft och amerikanska myndigheter kan ta del av information om användare.	K	**Åtgärder** A18: Förtydliga informationen i kunskapsportalen gällande hur man ska hantera samtal i Teams.	**Sa: 2** **Ko: 2** **Rv: 6**

#	Beskrivning	Påverkar	Kommentar och åtgärder för riskhantering	Riskvärde
R26	**Diagnosdata kan innehålla uppgifter i klartext trots pseudonymisering** Risk för… Möjlighet för amerikanska myndigheter att begära ut diagnosdata från Microsoft för nationella säkerhetsändamål utan kännedom eller skydd för individens fri- och rättigheter …på grund av… Diagnosdata kan innehålla identifierande uppgifter. …vilket leder till… Övervakning: Möjlighet för amerikanska myndigheter att begära ut data från Microsoft för nationella säkerhetsändamål utan kännedom eller skydd för individens fri- och rättigheter	K	**Åtgärder** A16. Personer som har skyddad identitet skyddas med pseudonyma konton, som sker innan tjänsten. Detta återfinns i anvisning för skyddade identitet.	**Sa: 2** **Ko: 2** **Rv: 6**

#	Beskrivning	Påverkar	Kommentar och åtgärder för riskhantering	Riskvärde
R28	**Supportärenden: Kontodata kan inkluderas i kommunikation med MS** Risk för… Möjlighet för amerikanska myndigheter att begära ut diagnosdata från Microsoft för nationella säkerhetsändamål utan kännedom eller skydd för individens fri- och rättigheter …på grund av… Supportärenden hanteras i tredjeländer. Kontodata kan inkluderas i kommunikationen med Microsoft …vilket leder till... Övervakning: Amerikanska myndigheter kan ta del av information om användare.	K	**Åtgärder** A19: Uppgiftsminimering genom att användares personuppgifter aldrig inkluderas. Fel replikeras på en servicedator och endast uppgifter från servicedatorn som förs över.	**Sa: 1** **Ko: 2** **Rv: 5**

#	Beskrivning	Påverkar	Kommentar och åtgärder för riskhantering	Riskvärde
R29	**Supportärenden kan överföras tillfälligt till underleverantörer i tredjeländer** Risk för… Möjlighet för amerikanska myndigheter att begära ut diagnos- och övriga innehållsdata från Microsoft för nationella säkerhetsändamål utan kännedom eller skydd för individens fri- och rättigheter …på grund av… Supportdata kan överföras tillfälligt till underleverantörer i Kina, Serbien och Indien som tillhandahåller support. …vilket leder till… Övervakning: Myndigheter i tredjeland kan ta del av information om användare. Uteslutning: Personuppgifter behandlas utan individens vetskap eller delaktighet (och utan laglig grund).	K	**Åtgärder** A19: Uppgiftsminimering genom att användares personuppgifter aldrig inkluderas. Fel replikeras på en servicedator och endast uppgifter från servicedatorn som förs över.	**Sa: 1** **Ko: 1** **Rv: 3**

#	Beskrivning	Påverkar	Kommentar och åtgärder för riskhantering	Riskvärde
R16	**Uppgifter kan delas med amerikanska myndigheter (Cloud Act)** Risk för … Uppgifter kan delas till amerikanska myndigheter som begär ut kommunens data från Microsoft i strid mot GDPR. …på grund av… Diagnostiska data flyttas till en leverantör som har sin juridiska hemvist utanför EES kan medföra utlämnande till annan stats rättsordning i strid med Cloud Act. … vilket leder till … Förlust av kontroll, konfidentialitet, återidentifiering av pseudonymiserad data och annan sekundär användning av individens personuppgifter utan laglig grund.	K	**Separat tredjelandsanalys enligt europeiska dataskyddsstyrelsens (EDPB:s) rekommendationer *(Transfer Impact Assessment).*** Kompletterande tekniska åtgärder är ej relevant i nuläget. Olika avtalsmässiga och interna administrativa kompletterande åtgärder efter bedömning i utredning samt hänvisning till tjänsteutlåtande 2021-05-25 som är bilaga 3. Risk har ej värderats.	Sa: 4 Ko: Y Rv: Z

#	Beskrivning	Påverkar	Kommentar och åtgärder för riskhantering	Riskvärde
R17	**Uppgifter kan delas hemligt med amerikanska myndigheter (Schrems 2)** Risk för … Uppgifter kan lämnas till amerikanska myndigheter (signalspaning) utan kännedom eller skydd för individens fri- och rättigheter. …på grund av… Överföring av personuppgifter till en leverantör som har sin juridiska hemvist utanför EES kan medföra utlämnande till annan stats rättsordning i strid med GDPR (Schrems 2). … vilket leder till … Förlust av kontroll, konfidentialitet, återidentifiering av pseudonymiserad data och annan sekundäranvändning av individens personuppgifter utan laglig grund.	K	**Separat tredjelandsanalys enligt europeiska dataskyddsstyrelsens (EDPB:s) rekommendationer *(Transfer Impact Assessment).*** Kompletterande tekniska åtgärder är ej relevant i nuläget. Olika avtalsmässiga och interna administrativa kompletterande åtgärder efter bedömning i utredning samt hänvisning till tjänsteutlåtande 2021-05-25 som är bilaga 3. Risk har ej värderats.	Sa: 4 Ko: Y Rv: Z

#	Beskrivning	Påverkar	Kommentar och åtgärder för riskhantering	Riskvärde
R18	**Möjlig otillåten övervakning av personuppgifter som lagras och hanteras i Office 365 (innehållsdata)** Risk för… Möjlighet för amerikanska myndigheter att begära ut innehållsdata från Microsoft för nationella säkerhetsändamål utan kännedom eller skydd för individens fri- och rättigheter …på grund av… Innehållsdata (klass 1) lagras och hanteras i Office 365, som ägs av Microsoft som är ett företag som lyder under amerikansk lagstiftning. …vilket leder till… Övervakning: Amerikanska myndigheter kan ta del av information och individer förlorar kontrollen över sina egna personuppgifter.	K	Risken lämnas öppen och bedöms inte i tjänsteleveransen, utan det är upp till personuppgiftsansvariga att ta med i en konsekvensbedömning	

#	Beskrivning	Påverkar	Kommentar och åtgärder för riskhantering	Riskvärde
R19	**Bristande kontroll över vad som hanteras i Office 365** Risk för… Möjlighet för amerikanska myndigheter att begära och få tillgång till känsliga innehållsdata från Microsoft för nationella säkerhetsändamål utan kännedom eller skydd för individens fri- och rättigheter …på grund av… att användare bryter mot regler om att känsliga data (klass 2) inte skall l hanteras i Office 365, …vilket leder till… Övervakning: Amerikanska myndigheter kan ta del potentiellt känslig information om individer som därmed förlorar kontrollen över sina egna personuppgifter.	K	Risken lämnas öppen och bedöms inte i tjänsteleveransen, utan det är upp till personuppgiftsansvariga att ta med i en konsekvensbedömning	

#	Beskrivning	Påverkar	Kommentar och åtgärder för riskhantering	Riskvärde
R24	**Bristande kontroll: Data delas med Microsoft och tredjeparter som Bing samt Cloudflare som är egna PUA** Risk för… Möjlighet för amerikanska myndigheter att begära ut innehållsdata från Microsoft för nationella säkerhetsändamål utan kännedom eller skydd för individens fri- och rättigheter. …på grund av… Bing och Cloudflare, amerikanska företag, är inte bundna till PUB-avtalet (MS online DPA) …vilket leder till… Övervakning: Amerikanska myndigheter skulle kunna se, lyssna eller spela in innehållsdata. Sekundär användning: Personuppgifter används för ett annat ändamål än vad som var avsett vid insamling.	K	Risken lämnas öppen och bedöms inte i tjänsteleveransen, utan det är upp till personuppgiftsansvariga att ta med i en konsekvensbedömning	

#	Beskrivning	Påverkar	Kommentar och åtgärder för riskhantering	Riskvärde
R30	**Samtal i Teams vid flerpartssamtal kan avlyssnas av MS** Risk för… Möjlighet för amerikanska myndigheter att begära ut innehållsdata från Microsoft för nationella säkerhetsändamål utan kännedom eller skydd för individens fri- och rättigheter …på grund av… Microsoft har tillgång till mediaströmmen vid två- samt flerpartskommunikation i Teams …vilket leder till… Övervakning: Microsoft och amerikanska myndigheter kan ta del av information om användare.		Risken lämnas öppen och bedöms inte i tjänsteleveransen, utan det är upp till personuppgiftsansvariga att ta med i en konsekvensbedömning **Möjliga åtgärder** A20: Förtydliga informationen i kunskapsportalen gällande hur man ska hantera samtal i Teams. A21: Möjlig åtgärd: Beskriva för verksamheten att E2EE kan tillämpas, men att det finns begräsningar med att det endast gäller två-parts spontanspontansamtal. I nuläget avstängd, men kan slås på.	

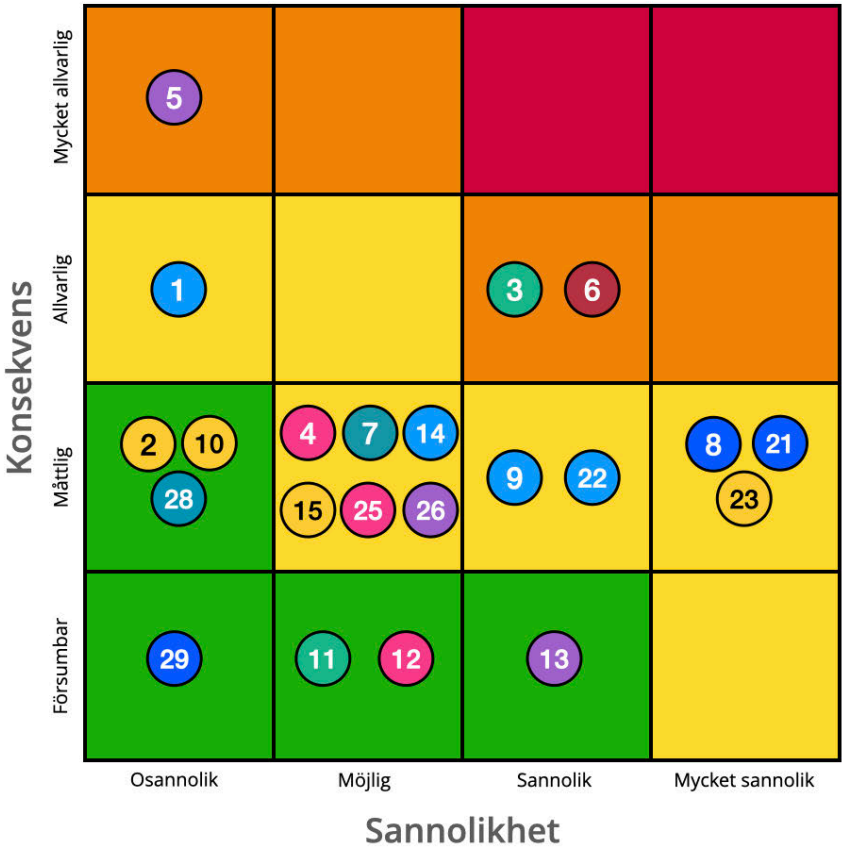
#	Beskrivning	Påverkar	Kommentar och åtgärder för riskhantering	Riskvärde
R31	**Övervakning av anställda (Teams analytics och Viva Insights)** Risk för… Möjlighet för kommunen få tillgång till medarbetares arbetsmönster genom Microsofts tjänster Teams Analytics och Viva Insights På grund av… Diagnosdata används inom ramen för analytiska tjänster som tillhandahålls av Microsoft. Administratörer kan få tillgång till analyserna. Vilket leder till… Övervakning: Kommunen kan se och analysera medarbetares aktiviteter.		Risken lämnas öppen och bedöms inte i tjänsteleveransen, utan det är upp till personuppgiftsansvariga att ta med i en konsekvensbedömning	

7.3 Riskmatriser

Nedan presenteras visualiseringar av risker före och efter åtgärder.

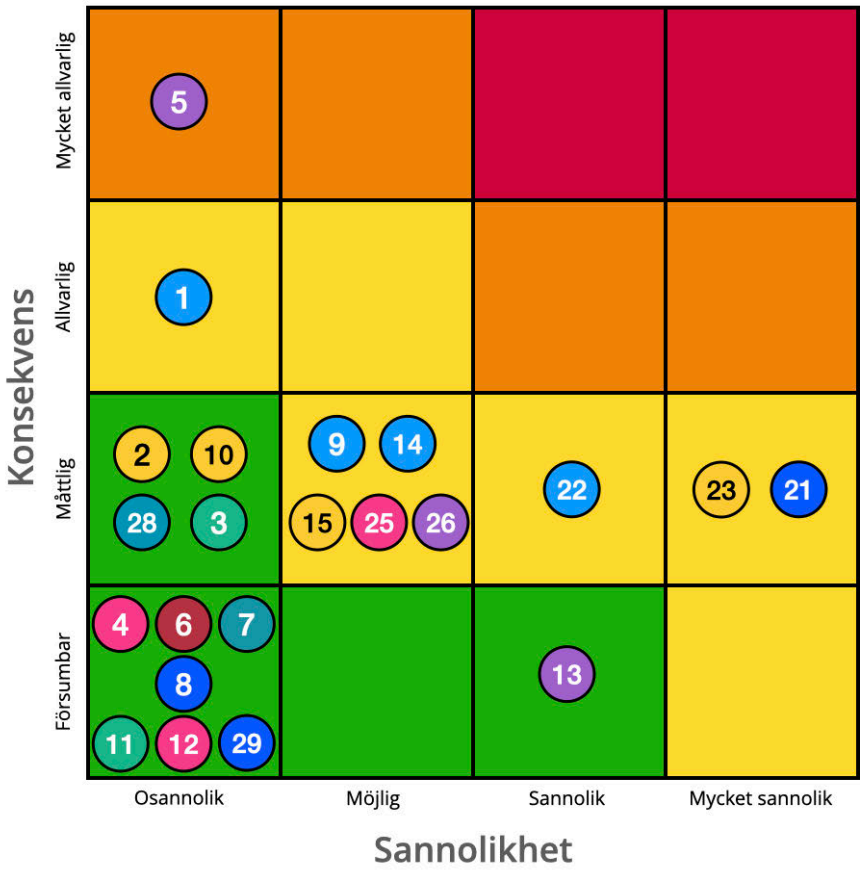
1. Värderade risker före åtgärder
2. Värderade risker efter åtgärder
3. Riskvärdering före och efter åtgärder (jämförelse)
4. Öppna risker

1. Värderade risker före åtgärder



1 Intrång av obehöriga
2 Intrång av leverantör
3 E-post kommer inte fram till mottagaren
4 Kalenderinformation kan ses och ändras
5 Skyddade identiteter i adressboken
6 Tillgång till information vid byte av tjänst
7 Krypterade mail kan inte öppnas
8 Röjande av information vid registerutdrag
9 För generösa behörigheter i Sharepoint
10 Nedladdning till privat dator
11 Delve utan klart syfte för Göteborgs Stad
12 Viva Insights (MyAnalytics) utan klart syfte för Göteborgs Stad
13 Inställningar och tjänster ändras
14 Chatt i Teams sparas "för evigt"
15 Inspelningar lagras i Teams tills arkivering
21 Bristande transparens och begränsning från MS gällande säkerhetshändelser
22 Bristande transparens i Office för Webben för överföring av diagnosdata
23 Tillfälliga överföringar från Onedrive av användarnamn, e-postadresser och sökvägar
25 Samtal i Teams inkluderar vilka konton/ användare som samtalar och när.
26 Diagnosdata kan innehålla uppgifter i klartext trots pseudomymiseing
28 Supportärenden: Kontodata kan inkluderas i kommunikation med MS
29 Supportärenden kan överföras tillfälligt till underleverantörer i tredjeländer

2. Värderade risker efter åtgärder

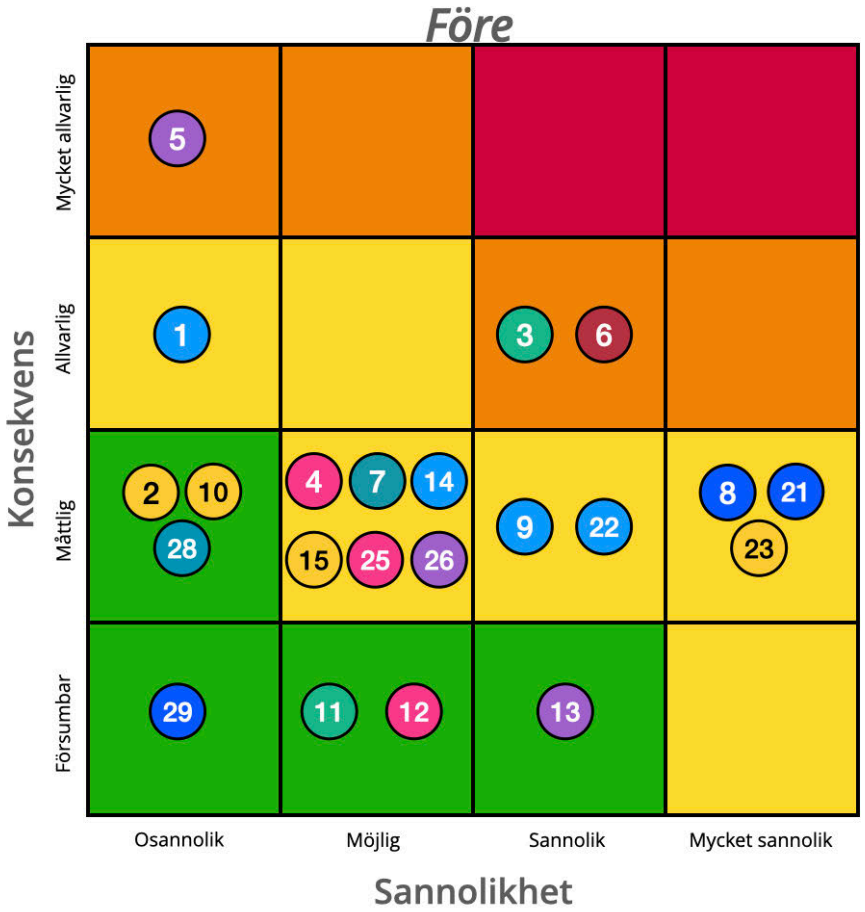


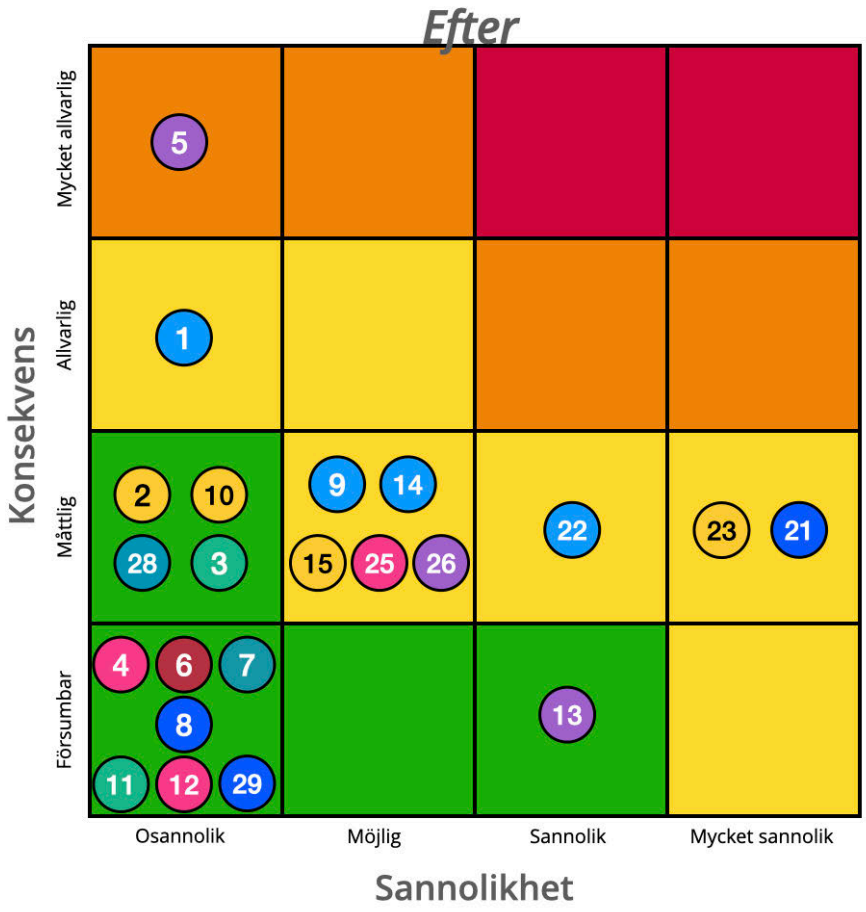
1. Intrång av obehöriga
2. Intrång av leverantör
3. E-post kommer inte fram till mottagaren
4. Kalenderinformation kan ses och ändras
5. Skyddade identiteter i adressboken
6. Tillgång till information vid byte av tjänst
7. Krypterade mail kan inte öppnas
8. Röjande av information vid registerutdrag
9. För generösa behörigheter i Sharepoint
10. Nedladdning till privat dator
11. Delve utan klart syfte för Göteborgs Stad
12. Viva Insights (MyAnalytics) utan klart syfte för Göteborgs Stad
13. Inställningar och tjänster ändras
14. Chatt i Teams sparas "för evigt"
15. Inspelningar lagras i Teams tills arkivering

Risker ej värderade efter åtgärder

21. Bristande transparens och begränsning från MS gällande säkerhetshändelser
22. Bristande transparens i Office för Webben för överföring av diagnosdata
23. Tillfälliga överföringar från Onedrive av användarnamn, e-postadresser och sökvägar
25. Samtal i Teams inkluderar vilka konton/ användare som samtalar och när.
26. Diagnosdata kan innehålla uppgifter i klartext trots pseudomymiseing
28. Supportärenden: Kontodata kan inkluderas i kommunikation med MS
29. Supportärenden kan överföras tillfälligt till underleverantörer i tredjeländer

3. Riskvärdering före och efter åtgärder (brutto)





4. Öppna risker

Förutsätter en tredjelandsanalys (TIA)

- 16 Uppgifter kan delas med amerikanska myndigheter (Cloud Act)
- 17 Uppgifter kan delas hemligt med amerikanska myndigheter (Schrems 2)

Värderas ej i tjänsten O365, skickas till PUA

- 18 Möjlig otillåten övervakning av personuppgifter som lagras och hanteras i Office 365
- 19 Bristande kontroll över vad som och hanteras i O365 (känsliga personuppgifter)
- 30 Samtal i Teams vid flerpartssamtal kan avlyssnas
- 24 Bristande kontroll: Data delas med Microsoft och tredjeparter som Bing samt Cloudflare som är egna PUA
- 31 Övervakning av anställda (Teams analytics och Viva Insights)

Förutsätter vidare utredning

- 20 Viva behandlas och lagras på Microsofts servrar i USA
- 27 Oförmåga att utöva den registrerades rätt till tillgång för nödvändiga servicedata i DDV

7.4 Kvarvarande risk

En *Riskanalys Dataskydd* är en process avsedd att beskriva tjänsten eller det som omfattas av riskanalysen för att bedöma kvalitet och risker för fysiska personers rättigheter och friheter som kan tänkas uppkomma genom användande av tjänsten samt komma fram till vilka åtgärder som ska vidtas för att hantera riskerna.

Värderingar baseras på de säkerhetsåtgärder och skydd av personuppgiftsbehandling i diagnosdata och funktionsdata samt skydd av gemensamma innehållsdata (inte vad innehållsdata innehåller för personuppgifter). De ovanstående identifierade riskerna och planerade och införda åtgärder följer de för stadens styrande dokument avseende informationssäkerhet. Arbetssätt och metoder beskrivs för att säkerställa att kommungemensamma interna tjänster uppfyller verksamhetens krav på informationssäkerhet och att de implementerade skyddsåtgärderna lever upp till dessa.

Efter åtgärder av risker identifierade i kapitel 7 redovisar Intraservice de risker som är hanterade och kvarvarande i tjänsteleveransen av O365.

Acceptans för kvarvarande risker är vidare avsedda att värderas av personuppgiftsansvariga.

7.5 Rekommendation till PUA ang. användning av tjänsten

Rekommendationen är att respektive förvaltning och bolag riskbedömer personuppgiftsbehandlingar i Microsoft Office 365 genom egna konsekvensbedömningar. Det är även lämpligt att varje förvaltning identifierar och klassar informationstillgångar för den information som används i respektive verksamhet, eftersom varje förvaltning bäst kan bedöma känsligheten för de personuppgifter som man hanterar.

Innehållsdata i dokument, e-post, kalendrar med mera bestäms av omfattningen av personuppgiftsbehandlingen av den förvaltning som använder tjänsten. Gemensamma innehållsdata, diagnosdata samt funktionsdata riskhanteras av Intraservice i egenskap av PUB, men varje förvaltning behöver vara medveten om risker, riskbedöma och eventuellt införa egna skyddsåtgärder.

Ett antal risker finns tillgängliga för att överföras och bedömas av PUA, men som inte finns med i denna riskanalys. Det finns även flertalet risker som bedömts i denna riskanalys dataskydd, men som även kan behöva hanteras av PUA, där varje bedömning behöver analysera om de åtgärder som genomförs centralt hos Intraservice är tillräckliga, vem som äger riskerna och när åtgärderna ska vara genomförda i varje förvaltning.

8 Bilagor

Här finns utöver denna rapport finns ytterligare handlingar som har legat till grund för riskanalysen av tjänsten. Längst bak i Appendix 3 – tidigare dokument finns även hänvisningar till tidigare PM, TU, rapporter riskbedömningar och andra dokument som relaterar till O365 i Göteborgs stad.

Bilaga	Datum	Titel
1	2020-04-20	*O365 Riskanalys Dataskydd v3.0*
2	2021-05-17	*Rapport – Analys av Microsofts hantering av diagnostikdata.pdf*
3	2021-05-25	*TU – Redogörelse för Intraservice arbetssätt och metod för utveckling av Kommungemensamma interna tjänster med stöd av molntjänstleverantörer.pdf*
4	2016-06-29	*Införande av Office 365*
5	2018-10-10	*Bedömning av Microsofts grundsäkerhetsnivå gällande Office 365.*
6	2018-05-17	*Bedömning av Customer Lockbox*
7	2019-06-19	*Lösningsspecifikation: Hantering av klass 2 information Office 365*
8	2022-03-14	*PM Microsoft - all lagring inom EU slutet 2022*
9	2022-04-05	*Dataskyddsenhetens rekommendationer och kommentarer TIA M365*
10	2022-05-09	*Uppdaterad rekommendation om tredjelandsöverföringar från dataskyddsenheten*

9 Referenser

CJEU. (2020). *EU-domstolens dom i mål C-311/18 – Data Protection Commissioner mot Facebook Ireland och Maximillian Schrems* Hämtad, från http://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=11549805.

EDPB. (2020a). *Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data* Version 1.0 .Adopted on 10 November 2020 Hämtad, från https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/recommendations-012020-measures-supplement-transfer_en.

EDPB. (2020b). *Recommendations 02/2020 on the European Essential Guarantees for surveillance measures (EEG)*. Hämtad, från https://edpb.europa.eu/our-work-tools/our-documents/recommendations/edpb-recommendations-022020-european-essential_en.

EDPB. (2021). *Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data* Version 2.0 .Adopted on 18 June 2021. Hämtad, från https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/recommendations-012020-measures-supplement-transfer_en.

EU 2016/679. *Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning)*. Hämtad från https://eur-lex.europa.eu/legal-content/SV/TXT/HTML/?uri=OJ:L:2016:119:FULL&from=SV.

EU-kommissionen 2010/87. *2010/87/: Kommissionens beslut av den 5 februari 2010 om standardavtalsklausuler för överföring av personuppgifter till registerförare etablerade i tredjeland i enlighet med Europaparlamentets och rådets direktiv 95/46/EG [delgivet med nr K(2010) 593] (Text av betydelse för EES)*. Hämtad från https://eur-lex.europa.eu/legal-content/SV/TXT/?uri=CELEX:32010D0087.

EU-kommissionen 2021/914. *Kommissionens genomförandebeslut (EU) 2021/914 av den 4 juni 2021 om standardavtalsklausuler för överföring av personuppgifter till tredjeländer i enlighet med Europaparlamentets och rådets förordning (EU) 2016/679.*: Hämtad från https://eur-lex.europa.eu/legal-content/SV/TXT/?uri=CELEX:32021D0914.

Göteborgs kommunfullmäktige. (2019a). *Riktlinje för informationssäkerhet* (H 2013:131, P 2013-09-05, § 21, Dnr 0540/14, 2019-12-19 Dnr 0019/19). Hämtad 2021-07-07, från https://intranat.goteborg.se/wps/portal/int?uri=gbglnk:Intranat.styrandedokument&dominoURL=https://www5.goteborg.se/prod/Stadsledningskontoret/LIS/Verksamhetshandbok/Forfattn.nsf/0/2A8DE6AB694CF7BFC1257C230027B5CF?OpenDocument.

Göteborgs kommunfullmäktige. (2019b). *Riktlinjer för styrning av kommungemensamma interna tjänster*. Version: 8, Gällande from 2019-10-31. Hämtad 2021-07-07, från

https://intranat.goteborg.se/wps/portal/int?uri=gbglnk:Intranat.styrandedokument&dominoURL=https://www5.goteborg.se/prod/Stadsledningskontoret/LIS/Verksamhetshandbok/Forfattn.nsf/0/DC85A7D50DEB1DDAC12580730028A637?OpenDocument.

Göteborgs kommunfullmäktige. (2019c). *Säkerhetspolicy för Göteborgs Stad*. (H 2013:131, P 2013-09-05, § 21, Dnr 0540/14, 2019-12-16 Dnr 0019/19). Hämtad 2021-07-07, från https://intranat.goteborg.se/wps/portal/int?uri=gbglnk:Intranat.styrandedokument&dominoURL=https://www5.goteborg.se/prod/Stadsledningskontoret/LIS/Verksamhetshandbok/Forfattn.nsf/0/EA5AD897046A0B8AC1257BEA0049EFF7?OpenDocument.

Göteborgs Stad. (2020). *Riktlinje för behandling av personuppgifter i Göteborgs Stad* Version: 5 Gällande from 2020-12-16. Hämtad 2021-07-07, från https://intranat.goteborg.se/wps/portal/int?uri=gbglnk:Intranat.styrandedokument&dominoURL=https://www5.goteborg.se/prod/Intraservice/LIS/Verksamhetshandbok/Verkhbok13.nsf/0/9B43B82E7C5D4FCAC1257C08004D7244?OpenDocument.

Göteborgs Stad. (2021). *Styrande dokument*. Hämtad 2021-07-07, från https://intranat.goteborg.se/wps/portal/int?uri=gbglnk:Intranat.styrandedokument.

Göteborgs Stad Intraservice. (2016). *Införande av Office 365*

Göteborgs Stad Intraservice. (2018a). *Bedömning av Customer Lockbox*

Göteborgs Stad Intraservice. (2018b). *Bedömning av Microsofts grundsäkerhetsnivå gällande Office 365*.

Göteborgs Stad Intraservice. (2021a). *Rapport - Analys av Microsofts hantering av diagnostikdata – underlag för konsekvensbedömning*

Göteborgs Stad Intraservice. (2021b). *Rapport avseende informationssäkerhet i Microsoft Office 365* 2021-02-01 Dnr: 0107/21. Hämtad 2021-07-07, från https://www4.goteborg.se/prod/intraservice/namndhandlingar/SamrumPortal.nsf/4412106EF8A797B3C12586700052EE18/$File/Rapport_avseende_informationssakerhet_MicrosoftOffice365.pdf?OpenElement.

Göteborgs Stads kommunstyrelse. (2021a). *Göteborgs Stads generella regler för kommungemensamma interna tjänster* (KS, 2015-03-11, § 142, Stadsdirektörens beslut (på delegation av kommunstyrelsen) 2018-02-14, Dnr 0014/18, Redaktionellt på delegation 2021-02-18, dnr 0110/20). Version: 6, Gällande from 2021-04-21. Hämtad 2021-07-07, från https://intranat.goteborg.se/wps/portal/int?uri=gbglnk:Intranat.styrandedokument&dominoURL=https://www5.goteborg.se/prod/Stadsledningskontoret/LIS/Verksamhetshandbok/Forfattn.nsf/0/DC85A7D50DEB1DDAC12580730028A637?OpenDocument.

Göteborgs Stads kommunstyrelse. (2021b). *Göteborgs Stads regler för kommungemensamma interna tjänster*. (KS, 2015-03-11, § 142, Stadsdirektörens beslut (på delegation av kommunstyrelsen) 2017-05-08 dnr 0014/17, KS P 2017-08-23 § 561, Dnr 0854/17, Stadsdirektörens beslut (på delegation av kommunstyrelsen) 2018-02-14, Dnr 0014/18, Stadsdirektörens beslut (på delegation av kommunstyrelsen) 2018-10-15, Dnr 0014/18), Stadsdirektörens beslut (på delegation av kommunstyrelsen) 2019-05-14, Dnr 0014/19, Stadsdirektörens beslut (på delegation av kommunstyrelsen) 2020-06-25, Dnr 0014/20,

Redaktionellt på delegation 2021-02-18, dnr 0110/20, Stadsdirektörens beslut (på delegation av kommunstyrelsen 2021-06-02, dnr 0014/21). Version: 14, Gällande from 2021-06-11. Hämtad 2021-07-07, från https://intranat.goteborg.se/wps/portal/int?uri=gbglnk:Intranat.styrandedokument&dominoURL=https://www5.goteborg.se/prod/Stadsledningskontoret/LIS/Verksamhetshandbok/Forfattn.nsf/0/DC85A7D50DEB1DDAC12580730028A637?OpenDocument.

Intraservice Dataskyddsenheten (2022a)Dataskyddsenhetens rekommendationer och kommentarer TIA M365 (2022-04-05 uppl.).

Intraservice Dataskyddsenheten (2022b)Uppdaterad rekommendation om tredjelandsöverföringar från dataskyddsenheten (2021-05-09 uppl.).

Microsoft. (2020). *Data Protection Addendum (DPA) - December 2020 (English)* Hämtad, från https://www.microsoftvolumelicensing.com/DocumentSearch.aspx?Mode=3&DocumentTypeId=67.

Microsoft. (2022). *Microsoft Products and Services Data Protection Addendum (DPA) September (English)* Hämtad, från https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA?year=2022.

OSL 2009:400. *Offentlighets- och sekretesslag*. Hämtad, från https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/offentlighets--och-sekretesslag-2009400_sfs-2009-400.

Privacy Company. (2019, 23 July 2019). *DPIA Office 365 ProPlus version 1905 (June 2019) - Data protection impact assessment on the processing of diagnostic data*. Hämtad, från https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/rapporten/2019/06/11/data-protection-impact-assessment-windows-10-enterprise/%28Dutch%29+Summary+DPIA+Office+365+ProPlus+23+juli+2019.pdf.

10 Appendix 1 – Exempel konsekvenser och sannolikheter

10.1 Konsekvenser [6]

Konsekvens-nivå	Generisk beskrivning	Exempel på skada		
		Fysisk	**Materiell**	**Moralisk**
1. Försumbar	Registrerade är inte påverkade eller har små besvär, som de kan komma över utan problem. T.ex personuppgifter som är allmänt tillgänglig (t.ex. i telefonböcker, adressböcker eller listor)	• Bristande omvårdnad (barn, en person beroende av hjälp) • Huvudvärk	• Tidsförlust på grund av formaliteter • Spam • Direktmarknadsföring • Riktad annonsering som konsument	• Ren skär irritation • Rädsla att tappa data • Känsla av obehag av närgångenhet • Smärre tidsförlust • Bristande respekt • Missade erbjudanden
2. Måttlig	Registrerade kan påverkas med tydliga besvär, som de kan komma över, trots vissa svårigheter. T.ex personuppgifter som kräver ett legitimt intresse för åtkomst (t.ex. begränsade offentliga filer eller medlemmarna i en distributionslista)	• Mindre fysisk påverkan (illamående, ångest) • Bristande omvårdnad som orsakar skada • Förtal som resulterar i psykisk eller fysiska symptom.	• Oväntade kostnader (böter, avgifter) • Ej access till tjänster • Missade möjligheter (karriär, semester) • Oönskad post som orsakar skada • Kostnadsökningar • Inkorrekt profilering • Exponering av hemliga uppgifter (graviditet, rehabilitering)	• Avstängning från en tjänst • Ärekränkning och försämrat rykte • Problem med professionella eller personliga relationer (bilder, skamfilning) • Känsla av intrång i privatlivet • Förolämpning på sociala medier
3. Allvarlig	Registrerade påverkas med betydande besvär, som de bör kunna komma över med mycket svårigheter och hjälp. T.ex personuppgifter vars obehöriga avslöjande kan påverka den registrerades rykte (t.ex. information om inkomst, socialförsäkringsförmåner, fastighetsskatt eller påföljder)	• Allvarlig fysisk påverkan som orsakar långsiktiga problem. • Handikapp och fysisk förändring som ett resultat av våld, olycka hemma eller på arbetet	• Bestående ekonomiska problem (måste låna) • Ej möjlighet att låna • Förlust av bostad, arbete, egendom • Separation • Finansiell förlust på grund av bedrägeri • Frysning av tillgångar • Nekad att studera, examen, utvisning	• Allvarliga psykiska problem (depression, fobier) • Känsla av intrång med bestående skada • Kränkning av grundläggande rättigheter (diskriminering, åsiktsfrihet) • Utpressning • Nätmobbning & trakasserier • Maktlöshet av att förlorat en process
4 Mycket allvarlig	Registrerade påverkas med allvarliga besvär, eller oöverstigliga konsekvenser, som kanske inte kan komma över. T.ex personuppgifter vars obehöriga avslöjande, modifiering, förlust eller förstörelse kan påverka den registrerades existens eller hälsa, frihet och liv.	• Långsiktig påverkan med permanenta eller kronisk fysiska besvär • Död (mord, självmord, olycka) • Permanent funktionsnedsättning	• Förlust av bevis (rättsprocess) • Oförmåga att arbeta • Ej möjligt att flytta • Förlust av vital infrastruktur (vatten, el)	• Långsiktig eller permanent psykisk påverkan • Kriminell bestraffning • Förlust av familjeband • Förlust av myndighet eller förmyndarskap • Ej möjlighet att föra process

[6] Enligt CNIL (Franska Tillsynsmyndigheten) Privacy Impact Assessment (PIA) samt ISO 29134 råd för konsekvensbedömning (Privacy impact assessment)

10.2 Sannolikhet

Sannolikheten för att varje hot utnyttjas bör uppskattas med hänsyn till sårbarheterna för behandlingar och deras stödsystem och kapaciteten hos riskkällor för att utnyttja dem (färdigheter, tillgänglig tid, ekonomiska resurser, närhet till informationssystem, motivation, känsla av straffrihet, etc.). Med andra ord, i vilken utsträckning kan egenskaperna för underlättande tillgångar utnyttjas för att utföra ett hot?

Osannolikt: Att utföra ett hot genom att utnyttja sårbarheterna för behandlingar och deras stödsystem verkar inte möjligt för de valda riskkällorna (t.ex. stöld av pappersdokument lagrade i ett rum som skyddas av en kortläsare och åtkomstkod).

Möjlig: Att utföra ett hot genom att utnyttja sårbarheterna för behandlingar och deras stödsystem verkar vara svårt för de valda riskkällorna (t.ex. stöld av pappersdokument som är lagrade i ett rum skyddat av en kortläsare).

Sannolikt: Att utföra ett hot genom att utnyttja sårbarheterna för behandlingar och deras stödsystem verkar vara möjligt för de valda riskkällorna (t.ex. stöld av pappersdokument lagrade på kontor som inte kan nås utan att först kontrollera i receptionen).

Mycket Sannolikt: Att utföra ett hot genom att utnyttja sårbarheterna för behandlingar och deras stödsystem verkar vara extremt lätt för de valda riskkällorna (t.ex. stöld av pappersdokument lagrade i en lobby).

11 Appendix 2 – Tidigare dokument

11.1 Förteckning av tidigare dokument gällande O365

Nedan lista inkluderar dokument med direkt relation till Microsoft Office 365 ur ett personuppgiftsbiträdesperspektiv, som skrivits av eller på uppdrag av olika aktörer i Göteborgs stad.

Datum	Titel och organisation	Beskrivning
2016-06-29	*Införande av Office 365* av Intraservice	Tjänsteutlåtande med beskrivning över nyttor och licensaspekter vid införandet. Tar upp behovet av laglighetskontroll och aspekter på var personuppgifterna lagras geografiskt liksom vilka säkerhetsåtgärder som måste vidtas för att skydda dessa uppgifter.
2017-10-20	*Promemoria avseende Office 365* av Stadsledningskontoret	Bedömning av säkerhetsanalys, röjandebegrepp samt tilläggsavtal med Microsoft angående Customer Lockbox, som förutsättning för fortsatt användning av Office 365.
2018-05-17	*Bedömning av Customer Lockbox* av Intraservice	Intraservice bedömer att Customer Lockbox inte löser den problematik kring röjande av information som beskrivs i Stadsledningskontorets PM daterad 2017-10-20
2018-10-10	*Bedömning av Microsofts grundsäkerhetsnivå gällande Office 365* av Intraservice	Verifiering för att säkerställa efterlevnad av stadens styrande dokument inom informationssäkerhetsområdet.
2019-11-14	*Office 365 – bedömning om röjande enligt OSL* av Stadsledningskontoret	Bedömning ang. Cloud Act att uppgifter som omfattas av sekretess som överförts till O365 inte ska anses som röjda.
2019-06-19	*Lösningsspecifikation: Hantering av klass 2 information Office 365* av Intraservice	En teknisk utredning utifrån behov, möjliga lösningsalternativ, förutsättningar och risker för att tillåta hantering av klass 2 information i Office 365.
2019-12-10	*Intraservice fortsatta utveckling av tjänster baserat på Office 365* av Intraservice	Tjänsteutlåtande om att fortsätta utveckla tjänster baserat på Office 365 inkluderat känsliga personuppgifter och information som omfattas av sekretess.

Datum	Titel och organisation	Beskrivning
2020-06-09	*Riskanalys Dataskydd - Bedömning av Teams* av Intraservice	Riskanalys Dataskydd på videokommunikations- och samarbetsplattformen Teams som ersättare av Skype.
2020-06-29	*Riskanalys Dataskydd - Bedömning av tjänsteleverans O365 version 1.0* av Intraservice	Riskanalys Dataskydd på O365 som helhet som en kommungemensam intern tjänst. Version 1.0
2020-06-29	*Riskanalys Dataskydd - bedömning av e-post till SMS* av Intraservice	Riskanalys Dataskydd gällande en koppling mellan O365 och bedömning av möjligheten att från e-post välja om mottagaren också ska få SMS
2020-11-24	*Riskanalys Dataskydd - bedömning av Bookings (del av O365)* av Intraservice	Riskanalys Dataskydd gällande en O365-produkt som kallas Bookings, vilken används för att tillgängliggöra bokningsbara resurser, även för externa användare
2020-12-11	*Ställningstagande rörande Office 365* av Stadsledningskontoret	Tjänsteutlåtande att fortsatt vidareutveckling och vidmakthållande av O365 inte är av principiell beskaffenhet eller av annars större vikt att kommunfullmäktige ska ta beslut i frågan, utan ärendet skickas till nämnden för Intraservice att besluta.
2021-02-01	*Rapport avseende informationssäkerhet i Microsoft Office 365* av Intraservice	Rapporten avser om en förlängning om avtalet om Customer Lockbox ska ske. Bedömningen är att behovet saknas.
2021-03-18	*Riskanalys tjänsteleverans: Tredjelandsöverföringar enligt Dataskyddsförordningen i anledning av användning av molntjänster* av Intraservice med stöd av Advokatfirman Lindahl	Juridiskt underlag av de aktuella rättsliga förutsättningarna som föreligger enligt Dataskyddsförordningen med analys av analys proportionalitetsprincipen, artiklarna 45, 46 samt 49 vid överföring av personuppgifter till tredjeland.
2021-04-14	*Promemoria Göteborg stads användning av Microsoft Office 365* av Advokatfirman Lindahl	Fördjupad juridisk analys av Stadens användning av O365 om det förändrade rättsläge som domen i Schrems II inneburit vad gäller tillåtligheten av överföringar till tredjeland och hur det påverkar Stadens tidigare slutsatser.
2021-05-03	*Rapport – Analys av Microsofts hantering av diagnostikdata* av Intraservice	Rapport med tekniska analys och konkreta rekommendationer för att minska diagnostikdataflöden O365.

Datum	Titel och organisation	Beskrivning
2021-05-25	*Redogörelse för Intraservice arbetssätt och metod för utveckling av Kommungemensamma interna tjänster med stöd av molntjänstleverantörer* av Intraservice	Tjänsteutlåtande med omfattande beskrivning av historik, omvärldsbevakning samt analyser och ställningstaganden. Konstaterande att fortsatta utredningar behövs på flera områden.
2021-06-07	*Risker och konsekvenser beskrivna i effektkedjor* av Intraservice	Risker och konsekvenser beskrivna i effektkedjor för att avveckla ett ekosystem via leverans i molntjänst som O365.
2021-06-09	*Dataskyddsombudets skrivelse till Nämnden för Intraservice* av Dataskyddsombud för Intraservice	Dataskyddsombudet (DSO) lyfter fram att risker som identifierats i tjänsteutlåtandet daterat 2021-05-25 relaterat till O365 och tredjelandsöverföring behöver utredas vidare. I detta arbete behöver Intraservice kommunicera med berörda PUA och DSO.
2021-07-09	*O365 Riskanalys Dataskydd v2*	Uppdaterad riskanalys som inkluderar aspekter kring tredjelandsöverföring, tekniska aspekter och omarbetat riskkapitel.

Riskanalys dataskydd för intranätet ”Digitala navet”

Underlag framtaget av Intraservice i egenskap av tjänsteleverantör

[Publiceringsdatum]

Versionshantering

Datum	Version	Beskrivning	Ändrat av
2022-09-23	1.0	Första versionen	Ewa Rockmyr
2023-01-20	1.1	Uppdaterad med förtydliganden samt reducerat olika fält.	Marcus Broman

Medverkande

Namn	Roll
Fredrik Andersson	Enhetschef intern extern kommunikation, Intraservice
Anna-Lena Björk	Enhetschef IT-säkerhet (CISO), Intraservice
Sara Herlitz	Kommunikationschef, Intraservice
Per Forsberg	Stöd – Informationssäkerhet, IT säkerhet, Intraservice
Robin Johansson	Informationssäkerhets IT säkerhet, Intraservice
Marcus Broman	Stöd - Informationssäkerhet och dataskydd vid enheten, IT säkerhet, Intraservice

Innehållsförteckning

1 Bakgrund och metod 3
1.1 Bakgrund 4
1.2 Metod 4
1.3 Beskrivning 5

2 Grundläggande uppgifter 6
2.1 Tjänstens namn 6
2.2 Behandlingsnamn 6
2.3 Tjänsteansvarig samt ansvar för riskanalys 6
2.4 Vilka regelverk omfattas tjänsteleveransen av? 6
2.5 Intraservice roll, PUA eller PUB 7
2.6 Intraservice är alltså leverantör till staden av O365 och därmed PUB för alla personuppgifter som hanteras i tjänsten oavsett typ av data.Personuppgiftsansvarig – PUA (organisation) 7
2.7 Beskriv tjänstens användande i verksamheten (hos PUA) 8
2.8 Anlitas underbiträde för hela eller delar, av tjänsten? 8
2.9 Beskriv tjänstens IT-arkitektur 8

3 Personuppgifter, känslighet och tjänstens karaktär 9
3.1 Kategorier av personuppgifter 10
3.2 Vilka kategorier av personuppgifter hanteras i tjänsten. 10
3.3 Tillgång till personuppgifter 11
3.4 Uppgifter om sårbara eller i beroendeställning 11
3.5 Känsliga personuppgifter (art 9) 12
3.6 Automatiskt beslutfattande 12
3.7 Systematisk övervakning 12
3.8 Utvärdering eller poängsättning 12
3.9 Samkörning av uppgifter 12

4 Individers rättigheter 13
4.1 Tillämpliga rättigheter 13

5 Säkerhet vid behandling av personuppgifter i tjänsten 14
5.1 Administrativa åtgärder 14
5.2 Tekniska åtgärder 15

6 Tredjelandsöverföring 16
6.1 Förekomst 16
6.2 Grund för tredjelandsöverföring 17

7 Risker och åtgärder 18
7.1 Sammanfattning av riskbedömning 19

8 Appendix 1 – Exempel konsekvenser och sannolikheter 22
8.1 Konsekvenser 22
8.2 Sannolikhet 24

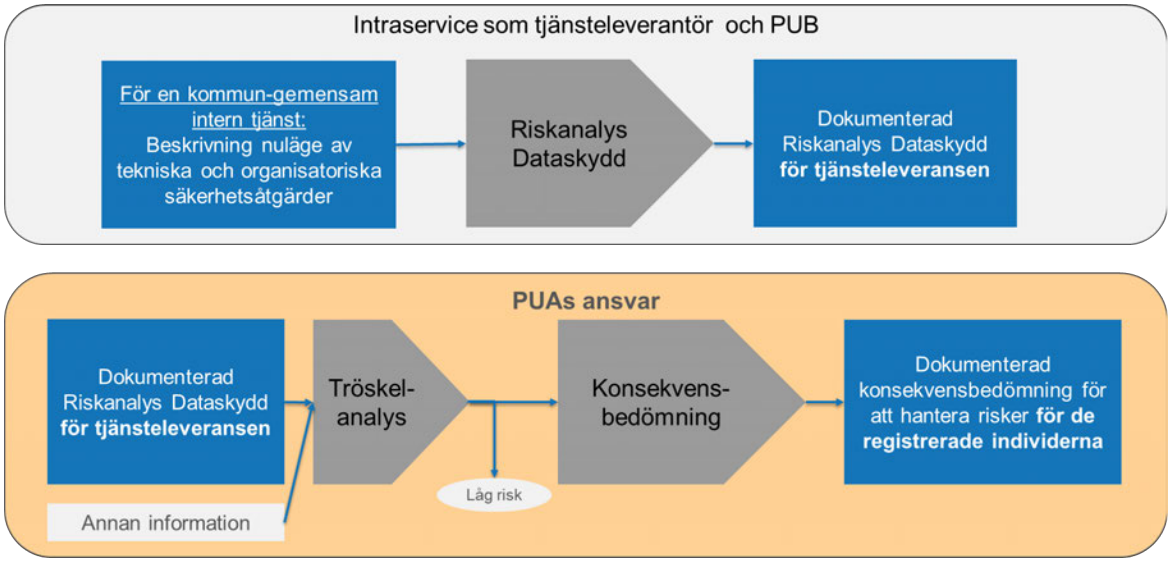
9 Appendix 2 – Lista på personuppgiftskategorier 25

1 Bakgrund och metod

En riskanalys för dataskydd är en systematisk och dokumenterad riskhantering med utgångspunkt i dataskyddsförordningen som utförs på en kommungemensam intern tjänst eller motsvarande.

1.1 Bakgrund

Riskanalys Dataskydd utförs av tjänsteleverantören Intraservice i sitt uppdrag att tillhandahålla kommungemensamma interna tjänster, medan *Tröskelanalys* och *Konsekvensbedömning* görs av personuppgiftsansvarig, PUA.



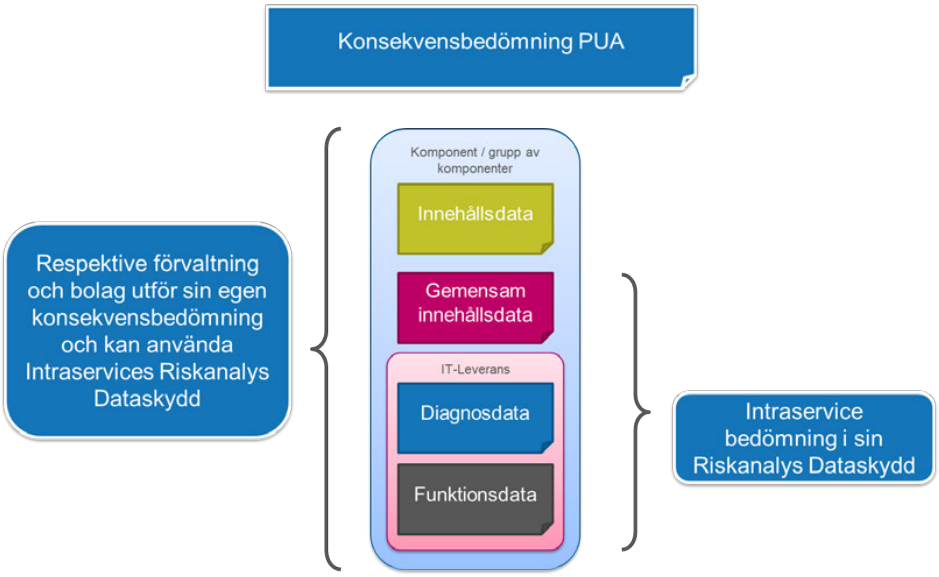
1.2 Metod

Många kommungemensamma interna tjänster har IT-stöd där tjänsteleverantören kan bedöma hantering av vissa data men inte den innehållsdata som användare och personuppgiftsansvarig skapar.

Vi har definierat 4 olika typer av data med personuppgifter och som behandlas i syfte att kunna leverera en tjänst med IT-stöd.

- **Innehållsdata**: Den data som användare hos personuppgiftsansvarig skapar genom att använda tjänsten. *Exempelvis innehåll i e-post, dokument på Sharepoint etc.*
- **Gemensamma innehållsdata**: *exempelvis användarinformation som härrör från HR system, gemensamma metadatastrukturer, visualisering av organisation*
- **Funktionella data**: är konfigurationsdata för IT-stödet, metadata och ev funktionella data som tjänsteleverantören (kan också vara SaaS leverantör) tillfälligt måste bearbeta för att användare ska kunna anslutas till tjänsten.
- **Diagnosdata**: det kan förekomma att Intraservice som tjänsteleverantör och/eller leverantör av SaaS tjänst samlar in och lagrar data om den individuella användningen av tjänstens IT-stöd.

Önskvärt är att beskriva aktuell tjänsts hantering av PU i dessa typer av data samt vad som denna bedömning omfattas av.



1.3 Beskrivning

Det *Digitala navet* är en intranätslösning som är utvecklad inom SharePoint Online. Denna bedömning omfattar inte innehållsdata exempelvis när någon publicerar information. Det Digitala navet skall ses om ett tomt ramverk som man kan publicera något i. SharePoint online har tidigare ingått och ingår i *O365 Riskanalys Dataskydd*.

Nytt i tjänsten är att tjänsten läser in information från Master/metadata om organisatorisk tillhörighet, samt om man är chef eller inte. Användare väljer själv sin roll (taggning) som kan vara exempelvis ekonom eller tekniker. Denna information används för att ta del av en mer relevant och riktad information. Utifrån intresseområde och vald roll kan användare själv välja den information som man ska ta del av. Utöver dessa val kan användare välja andra områden än just det de har i sin direkta yrkesroll.

En användarprofil skapas, där ID-nummer för informationen nedan sparas:

Tilldelad: Organisationstillhörighet
Eget val: Val av intresseområde/roller

ID-nummer pekar på centralt lagrade metadata i SharePoint och denna data speglas också till Azure AD. Information i klartext syns enbart för användaren själv och skulle kunna röjas när man delar skärm.

2 Grundläggande uppgifter

2.1 Tjänstens namn

Interna digitala navet

2.2 Behandlingsnamn

Interna digitala kanaler

2.3 Tjänsteansvarig samt ansvar för riskanalys

Tjänsteansvarig är: Joesphine Andersson, tjänsteansvarig kommunikation och ledning & styrning, intraservice

Ansvariga för denna Riskanalys Dataskydd är:

Med ansvariga menas den eller de som ansvarar för arbetet att genomför riskanalysen och därmed säkerställa att alla relevanta perspektiv har tagits i beaktande.

Kontaktpersoner för denna bedömning för:

Tjänsteleveransen O365: Fredrik Andersson, enhetschef Intern och Extern kommunikation, Intraservice

Informationssäkerhet och dataskydd: Anna-Lena Björk, CISO, Intraservice

2.4 Vilka regelverk omfattas tjänsteleveransen av?

Dataskyddsförordningen (även benämnd som DSF eller GDPR) (EU 2016/679)

Offentlighets och Sekretess lag (OSL 2009:400)

Stadens Styrande dokument (Göteborgs Stad, 2021)

Säkerhetspolicy för Göteborgs Stad (Göteborgs kommunfullmäktige, 2019c)

Riktlinje för informationssäkerhet (Göteborgs kommunfullmäktige, 2019a)

Riktlinje för behandling av personuppgifter i Göteborgs Stad (Göteborgs Stad, 2020)

Riktlinjer för styrning av kommungemensamma interna tjänster (vad) (Göteborgs kommunfullmäktige, 2019b)

Göteborgs Stads generella regler för kommungemensamma interna tjänster (hur) (Göteborgs Stads kommunstyrelse, 2021a)

Göteborgs Stads regler för kommungemensamma interna tjänster (vilka) (Göteborgs Stads kommunstyrelse, 2021b)

Lagen om tillgänglighet till digital offentlig service

2.5 Intraservice roll, PUA eller PUB

Beskriv om Intraservice är personuppgiftsansvarig (PUB) eller personuppgiftsbiträde (PUA) i hanteringen av personuppgifter inom tjänsten.

Intraservice är personuppgiftsbiträde PUB i hanteringen av personuppgifter inom tjänsten.

Intraservice är personuppgiftsansvarig PUA för data som sker i personuppgiftsbehandlingar för den egna förvaltningen, vilket inte hanteras i detta dokument.

Vad styrker att Intraservice har rollen som beskrivs ovan?

Kommunstyrelsen har fastställt att Intraservice ska anses som PUB i sin leverans av Kommungemensamma interna tjänster. Detta resonemang stämmer med synsättet i detta arbete.

2.6 Intraservice är alltså leverantör till staden av O365 och därmed PUB för alla personuppgifter som hanteras i tjänsten oavsett typ av data.Personuppgiftsansvarig – PUA (organisation)

Skriv in vilken eller vilka organisationer (gemensam personuppgiftsansvarig) som är ansvarig för den aktuella personuppgiftsbehandlingen.

De förvaltningar och bolag som använder tjänsten:

- Arbetsmarknad och vuxenutbildning
- Förskoleförvaltningen
- Försäkrings AB Göta Lejon
- Förvaltningen för funktionsstöd (FFS)
- Got Event AB
- Grefab
- Grundskoleförvaltningen
- Göteborg & Co AB
- Göteborgs Stads Leasing AB
- Göteborgs Stadshus AB
- Intraservice
- Idrotts- och Föreningsförvaltningen
- Inköp och upphandling
- Demokrati- och medborgarservice
- Kretslopp och vatten
- Kulturförvaltningen
- Miljöförvaltningen
- Revisionskontoret
- Regionarkivet
- Socialförvaltningen Centrum
- Socialförvaltningen Hisingen
- Socialförvaltningen Nordost

- Socialförvaltningen Sydväst
- Stadsledningskontoret
- Utbildningsförvaltningen
- Äldre samt vård- och omsorgsförvaltningen (ÄVO)

Och de förvaltningar som bildas 2023-01-02

- Exploateringsförvaltningen
- Stadsfastighetsförvaltningen
- Stadsbyggnadsförvaltningen
- Stadsmiljöförvaltningen

2.7 Beskriv tjänstens användande i verksamheten (hos PUA)

Beskriv i den omfattning det är känt hur tjänsten används av verksamheterna.

Information för medarbetare i Göteborgs stad för att kunna utför sitt arbete inom ämnena service, support och stöd i tjänster, ledning och styrning, organisation och min anställning. Kommunikativ aktuell information i form av nyheter, vi delar med oss, nytt från och kommande händelser.

2.8 Anlitas underbiträde för hela eller delar, av tjänsten?

Anlitar Intraservice såsom PUB underleverantörer i sin tur, dvs underbiträden?☐ JA ☒ NEJ

Om Ja i vilka delar av tjänsten? Beskriv och kommentera ditt svar nedan:

För underbiträden kopplat till den underliggande tjänsten Microsoft Office 365 se tjänstespecifikation för Microsoft Office 365

2.9 Beskriv tjänstens IT-arkitektur

Digitala navet bygger på plattformen Sharepoint Online som är en del av M365-plattformen inom Göteborgs Stad. När en användare loggar på sig på sin “staden-dator”, har hen automatisk access till M365 och till det Digitala navet. När användaren besöker det digitala navet hämtas personinformation enligt skisserna nedan.

2.9.1 Sharepoint Online

Sharepoint Online är en funktion för att spara, dela och samarbeta med dokument och data. Den finns som webbaserad funktion så väl som appar för Windows och Mac OS samt för Android och iOS system. Sharepoint används till att behandla och dela på många typer av dokument och filer så som exempelvis Microsoft Office dokument, bilder, video, att-göra listor, bloggar och strukturerade listor. Diagnosdata samlas inte in från de webbaserade funktionerna men det görs vid användning av diagnosdata från applikationer. Ägaren av applikationerna kan ställa in vilka diagnosdata som ska skickas men vissa data anses vara nödvändiga om Microsoft ska kunna hålla applikationerna säkra.

2.9.2 Beskrivning av den tekniska uppsättningen och flödet av persondata för det Digitala navet.

Digitala navet nyttjar användarinformation ifrån tjänsten MMD (Master Meta Data). Användarinformationen från MMD kopplas ihop med motsvarande användare i Azure AD (Active Directory) och relationen sparas i en separat SQL databas (se beskrivning om innehåll längre ner). Informationen som skapas består av unika ID:n (s.k. GUID = Globally Unique Identifier) i form av bokstäver och siffror. Det finns alltså ingen personinformation sparad i varken Digitala navet eller SQL databasen. Personinformationen finns endast i Azure Ad och MMD. Kopplingen till MMD är framtagen för att kunna erbjuda en personifierad inställningsmöjlighet för användaren då fullständig information inte levereras från Azure AD.

Hantering av personuppgifter för personer med skyddad identitet sker i separata databaser och ingen information förs över till det digitala navet. Ingen MMD-information för dessa personer förs över.

3 Personuppgifter, känslighet och tjänstens karaktär

I den mån vi vet så ange vilka kategorier av registrerade som hanteras i tjänsten. Exempelvis: Anställda, Elever, Leverantörer etcetera

Anställda och konsulter i Göteborg Stad samt gästkonton.

3.1 Kategorier av personuppgifter

Vilka kategorier av personuppgifter behandlas?

Se Appendix 2 – Lista på personuppgiftskategorier för detaljerad information om vad de olika kategorierna exempelvis innehåller

☒ Anställningsinformation
☐ Arbetsmiljö
☐ Bakgrundskontroller
☐ Biometriska och genetiska uppgifter
☐ Inloggningsuppgifter
☐ Familjeinformation
☐ Finansiella uppgifter
☒ Kontaktinformation
☐ Myndighetsutfärdad identifikation
☐ Personlig identifikation
☐ Resor och kostnader
☐ Sociala medier
☐ Sociala välfärdsdata
☐ Personliga egenskaper, utbildning och arbete
☒ Tekniska metadata
☐ Annat

3.2 Vilka kategorier av personuppgifter hanteras i tjänsten.

Vilka kategorier av personuppgifter behandlas?

Se ***Appendix 2 – Lista på personuppgiftskategorier*** för detaljerad information om vad de olika kategorierna exempelvis innehåller.

☒ Anställningsinformation
☐ Arbetsmiljö
☐ Bakgrundskontroller
☐ Biometriska och genetiska uppgifter
☐ Inloggningsuppgifter
☐ Familjeinformation
☐ Finansiella uppgifter
☒ Kontaktinformation
☐ Myndighetsutfärdad identifikation
☐ Personlig identifikation
☐ Resor och kostnader
☐ Sociala medier
☐ Sociala välfärdsdata
☐ Personliga egenskaper, utbildning och arbete
☒ Tekniska metadata
☐ Annat

Beskriv och kommentera ditt svar nedan:

Anställningsinformation och kontaktinformation kan visas kopplat till en sida som kontaktkort. Detta ska först verifieras med personen som ska vara kontakt. Så långt det är möjligt används funktionsbrevlådor. Ansvaret för att visa upp kontaktkort är varje enskild personuppgiftsansvarig.

Teknisk metadata – Inom digitala navet kan redaktör i redaktörsgränssnitt se vem som har skapat, ändrat och tagit bort en sida eller inlägg.

3.3 Tillgång till personuppgifter

Vilka tjänstemän och andra roller kommer ha tillgång till uppgifterna?

☐ En person
☐ Ett fåtal handläggare
☐ Personal inom enheten
☐ Personal inom förvaltningen
☒ Personal inom staden
☒ IT-administratörer
☐ Leverantörer
☐ Annat

Beskriv och kommentera ditt svar nedan:

Publicerad information är tillgänglig personal inom staden. Detta filtreras utifrån de val som medarbetare gör i användarinställningar vid första besöket (Detta kan ändras). Utifrån val av roll och organisation filtreras informationen sedan.

Roller, organisationsträd samt ”taggar” (ämnen) kan redigeras av superadmin och kan användas av redaktörerna när innehåll skapas.

3.3.1 Tillgång till personuppgifter (omfattning)

Ange hur många anställda som kommer ha tillgång till hela och de olika delarna av behandlingen om det är relevant.

Tekniska metadata endast ett fåtal medarbetare i staden med en roll som kräver detta. Ca 10 st.

3.4 Uppgifter om sårbara eller i beroendeställning

Inkluderar behandlingen sårbara individer eller personer i beroendeställning?

Innehåller behandlingen personuppgifter om personer som av något skäl befinner sig i ett underläge eller i beroendeställning och därför är sårbara, till exempel barn, anställda, asylsökande, äldre och patienter.

☒ Anställda
☐ Barn
☐ Psykiskt sjuka personer
☐ Asylsökande
☐ Äldre personer
☐ Patienter
☐ Ej tillämpligt
☐ Andra

3.5 Känsliga personuppgifter (art 9)

Behandlas känsliga personuppgifter i tjänsten?

Känsliga uppgifter är sådana uppgifter som kan skada en individs integritet i stor utsträckning om de görs tillgängliga, och som därför behöver extra skydd. Det är inte tillåtet att behandla känsliga uppgifter, förutom i undantagsfall. Känsliga personuppgifter kallas "särskilda kategorier av personuppgifter" i Dataskyddsförordningen.

☐ Ja
☒ Nej

3.6 Automatiskt beslutfattande

Inkluderar behandlingen användning av automatiskt beslutsfattande?

Behandling som har liten eller ingen påverkan på enskilda uppfyller inte detta särskilda kriterium.

☐ Ja
☒ Nej

3.7 Systematisk övervakning

Inkluderar behandlingen användning av systematisk övervakning?

Systematisk övervakning innebär att observera, övervaka eller kontrollera registrerade eller samla in i situationer där de registrerade kanske inte är medvetna om vem som samlar in deras uppgifter eller hur de kommer att användas.

☐ Ja
☒ Nej

3.8 Utvärdering eller poängsättning

Inkluderar behandlingen utvärdering eller poängsättning?

Detta inbegriper att profilera eller förutsäga beteende, särskilt aspekter avseende den registrerades arbetsprestation, ekonomiska situation, hälsa, personliga preferenser eller intressen, pålitlighet eller beteende, vistelseort eller förflyttningar.

☐ Ja
☒ Nej

3.9 Samkörning av uppgifter

Inkluderar behandlingen en samkörning av uppgifter från två eller flera behandlingar?

☐ Ja
☒ Nej

4 Individers rättigheter

4.1 Tillämpliga rättigheter

I artiklarna 12-21 GDPR finns det rättigheter för den enskilde. Vilka artiklar blir aktuella av den aktuella behandlingen?

☒ Art. 12 – Informationspolicy om hur personuppgifter behandlas
☒ Art. 13 – Informationsskyldighet när enskild lämnat uppgiften
☒ Art. 14 - Informationsskyldighet när annan än enskild lämnat uppgiften
☒ Art. 15 – Registerutdrag
☒ Art. 16 – Rättelse
☒ Art. 17 – Radering
☒ Art. 18 – Begränsning av behandling
☒ Art. 19 – Anmälningsskyldighet till mottagare
☐ Art. 20 – Dataportabilitet
☒ Art. 21 – Invändning

Beskrivning och kommentarer:

Alla ovan beskrivna rättigheter faller inom ramen för behandlingar som utförs inom Digitala navet av PUA liksom övriga behandlingar inom O365.

Intraservice som tjänsteleverantör och PUB kan bistå PUA med hantering av registrerades rättigheter på följande sätt för tjänsten O365. Där det nedan står ”Hanteras av PUA” innebär det att rättigheten hanteras av PUA och PUB bistår enligt tjänstebeskrivning och tillhörande styrande dokument.

Art 12 – Hanteras av PUA. Staden har gemensam policy för detta ”Riktlinjer för personuppgiftsbehandling i Göteborgs Stad”

Art 13 – Hanteras av PUA

Art 14 – Användarinformationen (gemensamma innehållsdata) kommer från Skatteverket via HR-system till AD, Detta ska framgå av PUA:s avtal med registrerade.

Art 15 - Registerutdrag: Intraservice beskriver behandling av PU för Gemensamma innehållsdata, Funktionsdata samt diagnosdata.

Art 16 – Hanteras av PUA

Art 17 – Användarinformation följer PUA:s information om anställning i staden.

När kontot avslutas ligger kontoinformationen kvar i 30 dagar och backup finns kvar i 90 dagar. Rutin för återläsning finns.

Art 18 – Vissa del-tjänster kan användaren själv styra begränsningar. PUA kan också styra med rekommendationer till sin organisation.

Obligatoriska tjänster kan inte begränsas. Ej obligatoriska tjänster kan påverkas via inställningar av användaren.

För vissa delar av diagnosdata kan användaren styra omfattningen.

Art 19 – Hanteras av PUA

Art 20 – Tjänsten stödjer inte dataportabilitet.

Art 21 – Hanteras av PUA

5 Säkerhet vid behandling av personuppgifter i tjänsten

5.1 Administrativa åtgärder

Administrativa säkerhetsåtgärder definierar roller, ansvar, policyer, processer, åtgärder och hantering av informationssäkerhet och dataskydds åtgärder. Dessa säkerhetsåtgärder inkluderar alla aspekter av åtgärder som är nödvändig för att övervaka och hantera konfidentialitet, riktighet, tillgänglighet och personlig integritet gällande den skyddsvärda information, och för att hantera de personer som använder den, fastställa användningsprincipen och fastställa standarder för utförande.

Gällande aspekter kring administrativa åtgärder för säkerhet hänvisas till:

- Tjänstespecifikation Digitala Navet
- Tjänstespecifikation - Microsoft Office 365
- Funktionsbeskrivning - Sharepoint Online, OneDrive och Delve
- Funktionsbeskrivning - Azure AD

5.1.1 Inbyggt dataskydd

Beskriv hur tjänsten i sin uppbyggnad har tagit hänsyn till principen om inbyggt dataskydd i art. 25 GDPR.

Digitala navet följer Göteborgs Stads generella rutiner (se intranät).

Digitala navet och O365 använder en begränsad mängd personuppgifter för anställda, konsulter och gästanvändare i Göteborgs Stad utifrån vad som hanteras i HR system (Personec). Detta säkerställer ett inbyggt dataskydd i O365 som följer individers anställning/uppdrag och därmed hanteras uppgiftsminimering med mera.

5.1.2 Lämplig säkerhetsnivå

Beskriv vilka administrativa skyddsåtgärder har bedömts behövas för att säkerställa en lämplig säkerhetsnivå.

Endast information som har säkerhetsklass 1 är rekommenderad för användning av Sharepoint, alltså i Digitala navet.

Grundläggande säkerhetsnivåer i Office 365 är beskrivna i rapporten Bedömning av Microsofts grundsäkerhetsnivå gällande Office 365 från 2018, där juridiska avdelningen vid Stadsledningskontoret tillsammans med Intraservice har dragit slutsatser baserat på då tillgänglig information. Bakgrunden var den amerikanska lagstiftningen CLOUD act (Clarifying Lawful Overseas Use of Data Act) som kom 2018. I rapporten har man tittat på de säkerhetscertifieringar och rapporter som Microsoft presenterar gällande den säkerhet för de tjänster som Göteborg Stad använder. Säkerhetsmässigt erbjuder tjänsten ett svåröverträffat starkt skydd mot såväl interna hot som cyberhot i omvärlden.

Klass 2 motsvaras i stadens aktuella klassningsmodell av känsliga personuppgifter enligt Dataskyddsförordningen samt uppgifter som innefattar olika former av sekretess enligt Offentlighets och sekretesslag (OSL 2009:400). Rapporten kommer fram till att man inte ser några hinder till att använda Office 365 för information av informationssäkerhetsklasserna 0, 1 och 2. Rapporten ser emellertid inte att de krav som ställs för att behandla information som omfattas av säkerhetsskyddslagstiftningen uppfylls.

Med bakgrund i risken för problematisk tredjelandsöverföring – där det finns ett juridiskt dilemma mellan EU-lag och amerikansk lag – finns det anledning att rekommendera att information med säkerhetsklass 2 inte används i O365 och Digitala navet.

5.2 Tekniska åtgärder

Tekniska säkerhetsåtgärder är de mekanismer som används inom IT-infrastrukturen i en organisation som verkställer organisationens säkerhetspolicy. Dessa säkerhetsåtgärder inkluderar alla aspekter av åtgärder som är nödvändig för att tekniskt övervaka och hantera konfidentialitet, riktighet, tillgängligheten och personlig integritet för den skyddsvärda information, och för att hantera de tekniska system och objekt som använder den.

Gällande aspekter kring tekniska åtgärder för säkerhet hänvisas till:

- Tjänstespecifikation Digitala Navet
- Tjänstespecifikation - Microsoft Office 365
- Funktionsbeskrivning - Sharepoint Online, OneDrive och Delve
- Funktionsbeskrivning - Azure AD

5.2.1 Inbyggt dataskydd

Beskriv hur hänsyn tagits till principen om inbyggt dataskydd i art. 25 GDPR.

Inbyggt dataskydd och dataskydd som standard (norm) har målet att säkerställa att processer och system är utformade så att inhämtande och

behandling (inklusive användning, utlämnande, bevarande, överföring och radering) begränsas till det som är nödvändigt för det identifierade ändamålet. Flertalet tekniska säkerhetsåtgärder finns inbyggda i tjänsten O365 och är delvis del av infrastruktur och andra tjänster, vilka är införda av Intraservice och återges inte i detalj.

Användarprofiler använder endast ID-nummer. Förklaringen till dessa ligger i *Managed meta data* och Azure AD, sedan tidigare etablerade rutiner.

6 Tredjelandsöverföring

Det finns strikta regler i dataskyddslagstiftningen för när personuppgifter får lämnas till länder utanför EU/EES, så kallat tredjeland. Detta gäller all överföring, även till personuppgiftsbiträde som inte själva använder personuppgifterna i sin verksamhet utan bara lagrar, driftar, supportar, utvecklar, underhåller eller servar systemet. Observera att ordet överföring även omfattar åtkomst till personuppgifterna i tredjeland, även om de lagras inom EU/EES.

6.1 Förekomst

Överförs personuppgifter till tredjeland eller internationell organisation?

☒ JA. ☐ NEJ

Ange vilket tredjeland och mottagare

Mottagaren kan vara en extern verksamhet som finns utanför EU/EES. Vem mottagaren är kan vara av intresse bland annat för vilka avtal som ska ingås. Exempel: "Biträde X i USA", "Intern verksamhet Y i Japan", "Internationell organisation Z".

O365 är en SaaS-tjänst som levereras av Microsoft Corporation Inc.

Lagring av innehållsdata sker inom EU, men överföring av vissa typer av metadata (funktionsdata och diagnosdata) sker till tredjeland, dvs Microsoft i USA samt till Microsofts underbiträden.

Sedan 1 januari 2023 genomför Microsoft införandet av *EU-data boundry*, vilket innebär att all data processas och lagras inom EU, inklusive metadata. Stora delar av metadatan är redan flyttade till EU, men det finns en backlog, som kommer att lösas under året.[1]

Efter fullbordande av *EU-data boundry* finns ingen bekräftad tredjelandsöverföring, utan återstår är endast vad som kan kallas för *risk* för

[1] Vad som ännu inte är inom EU data boundry kan ni läsa här. Customer data storage and processing for European customers in Azure Active Directory - Microsoft Entra | Microsoft Learn

tredjelandsöverföring, eftersom Microsoft är ett företag med amerikansk hemvist, som lyder under amerikansk lag.

6.2 Grund för tredjelandsöverföring

På vilka grunder sker överföringen till tredjeland eller internationell organisation?

☒ EU-kommissionens standardavtalsklausuler (SCC)
☐ Bindande företagsbestämmelser (Binding Corporate Rules, BCR)
☐ EU-kommissionen har godkänt mottagandet som har ansetts ha en godkänd skyddsnivå
☐ Godkänd certifieringsmekanism
☐ Godkänd uppförandekod
☐ Eget avtal mellan parterna som godkänts av tillsynsmyndigheten
☐ Viktigt allmänintresse
☐ Avtal med den registrerade
☐ Rättsliga anspråk
☐ Samtycke
☐ Annat

Beskriv och kommentera ditt svar nedan:

För redovisning kring tredjelandsöverföring se kapitel 6.2-6.5 Office 365 Riskanalys dataskydd för

7 Risker och åtgärder

Risker beskrivs nedan i en övergripande dokumentation av identifierade risker, samt tekniska och organisatoriska åtgärder.

Risker som identifieras är kopplat till användningen av digitala navet och den innehållstext som skapas av varje respektive verksamhet. Dessa risker måste hanteras av personuppgiftsansvarig och genom redaktörsutbildning.

Två risker finns identifierade, men bedöms inte i tjänsteleveransen. Den ena risken gäller är oklara roller för PUB och PUA. Den andra risken är faktumet att införandet av digitala navet innebär en fortsatt användning av O365 och därmed inkluderar risker för problematisk tredjelandsöverföring.

I övrigt har inga specifika risker kopplat till navet identifierats i tjänsteleveransen. För risker kopplat till Microsoft Office 365 som underliggande tjänst, se *Office 365 Riskanalys dataskydd.*

7.1 Sammanfattning av riskbedömning

Nedan är en sammanfattning av de riskerna med högst riskvärde

Sannolikhet (Sa) 1–4, Osannolikt, Möjlig, Sannolikt, Mycket Sannolikt (se Appendix 7.2 för definitioner)
Konsekvens (Ko) 1–4, Försumbar, Måttlig, Allvarlig, Mycket allvarlig (se Appendix 7.1 för definitioner)
Riskvärde (Rv) är en sammanlagd bedömning av sannolikhet och konsekvens och är ett stöd för prioritering av risker

Kryssrutor för K, R och T avser Konfidentialitet, Riktighet och Tillgänglighet
Åtgärder är angivna med T1, T2 för tekniska åtgärder och A1 osv för administrativa åtgärder.

#	Beskrivning	Kommentar och åtgärder för riskhantering	Riskvärde
R1	**Problematisk tredjelandsöverföring av personuppgifter som visas i Digitala navet.** Risk för… problematisk tredjelandsöverföring av personuppgifter som visas i Digitala navet. …på grund av… lansering av Digitala navet innebär fortsatt användning av O365 och dess underliggande risker …vilket leder till… Risk för tredjelandsöverföring och övervakning: Microsoft och därmed amerikanska myndigheter kan ta del av information om användare.	Digitala navet presenterar information som finns i underliggande tjänster. Digitala navet inte kan påverka hantering av dessa personuppgifter i underliggande tjänster. Risken lämnas öppen och bedöms inte i tjänsteleveransen, utan det är upp till personuppgiftsansvariga att ta med i en konsekvensbedömning	-

#	Beskrivning	Kommentar och åtgärder för riskhantering	Riskvärde
R2	**Oklara roller för PUB och PUA** Risk för… Risk för att PUA/PUB-förhållanden förändras utifrån pågående utredningar, vilket leder till behov av förändringar i riskhanteringen. …på grund av… Risk för att PUA/PUB-förhållanden förändras utifrån pågående utredningar, vilket leder till …vilket leder till… behov av förändringar i riskanalys.	Det behöver redas ut när Microsoft är personuppgiftsansvarig (PUA), när Intraservices nämnd är PUA, samt om stadsledningskontoret är PUA för viss gemensam information.. Risken lämnas öppen och bedöms inte i tjänsteleveransen, utan det är upp till personuppgiftsansvariga att ta med i en konsekvensbedömning	-

8 Appendix 1 – Exempel konsekvenser och sannolikheter

8.1 Konsekvenser [2]

Konsekvens-nivå	Generisk beskrivning	Exempel på skada		
		Fysisk	**Materiell**	**Moralisk**
1. Försumbar	Registrerade är inte påverkade eller har små besvär, som de kan komma över utan problem. T.ex personuppgifter som är allmänt tillgänglig (t.ex. i telefonböcker, adressböcker eller listor)	• Bristande omvårdnad (barn, en person beroende av hjälp) • Huvudvärk	• Tidsförlust på grund av formaliteter • Spam • Direktmarknadsföring • Riktad annonsering som konsument	• Ren skär irritation • Rädsla att tappa data • Känsla av obehag av närgångenhet • Smärre tidsförlust • Bristande respekt • Missade erbjudanden
2. Måttlig	Registrerade kan påverkas med tydliga besvär, som de kan komma över, trots vissa svårigheter. T.ex personuppgifter som kräver ett legitimt intresse för åtkomst (t.ex. begränsade offentliga filer eller medlemmarna i en distributionslista)	• Mindre fysisk påverkan (illamående, ångest) • Bristande omvårdnad som orsakar skada • Förtal som resulterar i psykisk eller fysiska symptom.	• Oväntade kostnader (böter, avgifter) • Ej access till tjänster • Missade möjligheter (karriär, semester) • Oönskad post som orsakar skada • Kostnadsökningar • Inkorrekt profilering • Exponering av hemliga uppgifter (graviditet, rehabilitering)	• Avstängning från en tjänst • Ärekränkning och försämrat rykte • Problem med professionella eller personliga relationer (bilder, skamfilning) • Känsla av intrång i privatlivet • Förolämpning på sociala medier
3. Allvarlig	Registrerade påverkas med betydande besvär, som de bör kunna komma över med mycket svårigheter och hjälp. T.ex personuppgifter vars obehöriga avslöjande kan påverka den registrerades rykte (t.ex. information om inkomst, socialförsäkringsförmåner, fastighetsskatt eller påföljder)	• Allvarlig fysisk påverkan som orsakar långsiktiga problem. • Handikapp och fysisk förändring som ett resultat av våld, olycka hemma eller på arbetet	• Bestående ekonomiska problem (måste låna) • Ej möjlighet att låna • Förlust av bostad, arbete, egendom • Separation • Finansiell förlust på grund av bedrägeri • Frysning av tillgångar • Nekad att studera, examen, utvisning	• Allvarliga psykiska problem (depression, fobier) • Känsla av intrång med bestående skada • Kränkning av grundläggande rättigheter (diskriminering, åsiktsfrihet) • Utpressning • Nätmobbning & trakasserier • Maktlöshet av att förlorat en process

[2] Enligt CNIL (Franska Tillsynsmyndigheten) Privacy Impact Assessment (PIA) samt ISO 29134 råd för konsekvensbedömning (Privacy impact assessment)

4 Mycket allvarlig	Registrerade påverkas med allvarliga besvär, eller oöverstigliga konsekvenser, som kanske inte kan komma över. T.ex personuppgifter vars obehöriga avslöjande, modifiering, förlust eller förstörelse kan påverka den registrerades existens eller hälsa, frihet och liv.	• Långsiktig påverkan med permanenta eller kronisk fysiska besvär • Död (mord, självmord, olycka) • Permanent funktionsnedsättning	• Förlust av bevis (rättsprocess) • Oförmåga att arbeta • Ej möjligt att flytta • Förlust av vital infrastruktur (vatten, el)	• Långsiktig eller permanent psykisk påverkan • Kriminell bestraffning • Förlust av familjeband • Förlust av myndighet eller förmyndarskap • Ej möjlighet att föra process

8.2 Sannolikhet

Sannolikheten för att varje hot utnyttjas bör uppskattas med hänsyn till sårbarheterna för behandlingar och deras stödsystem och kapaciteten hos riskkällor för att utnyttja dem (färdigheter, tillgänglig tid, ekonomiska resurser, närhet till informationssystem, motivation, känsla av straffrihet, etc.). Med andra ord, i vilken utsträckning kan egenskaperna för underlättande tillgångar utnyttjas för att utföra ett hot?

Osannolikt: Att utföra ett hot genom att utnyttja sårbarheterna för behandlingar och deras stödsystem verkar inte möjligt för de valda riskkällorna (t.ex. stöld av pappersdokument lagrade i ett rum som skyddas av en kortläsare och åtkomstkod).

Möjlig: Att utföra ett hot genom att utnyttja sårbarheterna för behandlingar och deras stödsystem verkar vara svårt för de valda riskkällorna (t.ex. stöld av pappersdokument som är lagrade i ett rum skyddat av en kortläsare).

Sannolikt: Att utföra ett hot genom att utnyttja sårbarheterna för behandlingar och deras stödsystem verkar vara möjligt för de valda riskkällorna (t.ex. stöld av pappersdokument lagrade på kontor som inte kan nås utan att först kontrollera i receptionen).

Mycket Sannolikt: Att utföra ett hot genom att utnyttja sårbarheterna för behandlingar och deras stödsystem verkar vara extremt lätt för de valda riskkällorna (t.ex. stöld av pappersdokument lagrade i en lobby).

9 Appendix 2 – Lista på personuppgiftskategorier

Kategori	Exempel på personuppgifter
Anställningsinformation	• Uppgifter om anställningsförmåner • Anställningsnummer • Företagskredit- eller betalkortsnummer • Anspråk om ersättning till anställda • Jobbtitel/roll • Disciplinär åtgärd • Frånvaroregister/tidsspårning/årlig ledighet • Hälso- och säkerhetsrelaterad information och rapportering • Slutdatum och skäl för uppsägning • Tidigare arbetslivserfarenhet • Arbetstimmar • Avtalstyp - bestämd tidsperiod / tillfällig / fast anställning, etc. • Prestationsbedömning • Lön • Startdatum • Avgångsintervju och kommentarer • Detaljer om jobbansökan (t.ex. ansökningsblankett, intervjuanteckningar, referenser) • Överordnad chef • Klagomål • Kontorsadress • Verksamhet/Enhet • Personalnummer
Arbetsmiljö	• Detaljer om mobbning och trakasserier
Bakgrundskontroller	• Drogtestresultat • Referens- eller bakgrundskontroller • Belastningsregister • Trafikböter • Brottshistorik
Biometriska och genetiska uppgifter	• Näthinneskanning • Ansiktsigenkänning • Röstigenkänning • Fingeravtryck • Genetisk sekvens
Inloggningsuppgifter	• Kontonummer • Kontoålder • Kontolösenord
Familjeinformation	• Namn på föräldrar • Namn på barn • Namn på partner • Annan familjestatus & information om närstående
Finansiella uppgifter	• Bankkontoinformation • Kontoutdrag • Bonusutbetalningar • Kreditkortsnummer • Ersättningsuppgifter • Uppgifter om lån, krediter, amorteringar etc

	• Finansiell status (inkomst, egendomar, investeringar)
Kontaktinformation	• Tidigare bostadsadress • Hemadress • Kontaktuppgifter vid nödfall • Telefonnummer • Personlig e-postadress • Kontaktuppgifter
Myndighetsutfärdad identifikation	• Personnummer • Körkortsnummer • Detaljer om nationellt identitetskort • E-tjänstekort • Pass • ID-kort • Skyddad identitet
Personlig identifikation	• Förnamn • Efternamn • Vikt • Födelsedatum • Religion/Religiös övertygelse • Sexuell läggning • Längd • Fullständigt namn • Civilstånd • Signatur • Ras eller etniskt ursprung • Nationalitet • Kön • Hälsa • Ålder • Foto, bild • Alias eller pseudonymer • Kännetecken
Resor och kostnader	• Resehistorik • Resebokningsinformation • Uppgifter om kostnader
Sociala välfärdsdata	• Arbetslöshetsersättning • Förtidspension • Försörjningsstöd eller andra bistånd (utsatthet, arbetslöshet, fattigdom)
Sociala medier	• Sociala medier - konto • Sociala medier - historik • Sociala medier - kontaktuppgifter
Personliga egenskaper, utbildning och arbete	• Examensbevis • Betyg • Utbildningshistorik • Språk • Akademiska meriter • Förbundsmedlemskap • Kvalifikationer/certifieringar • Curriculum vitae • Utvärderingsinformation • Fackligt medlemskap • Beteende och preferenser • Vanor, personliga preferenser & intressen, umgängesliv & kontakter

	• Utvärderingar av personlighet och beteende
Tekniska metadata	• Webbplatshistorik • Lokaliseringsdata (Position) • Cookie-information • IP-adress • Webbsökningstid • Trafikdata • Information om använda telefontjänster (Har ringt 1177 t.ex.) • Loggar (applikationsloggar, säkerhetsloggar etc.)

Beskrivning av använda figurer

- Aktivitet som utförs
- Mejlas, postas, papper

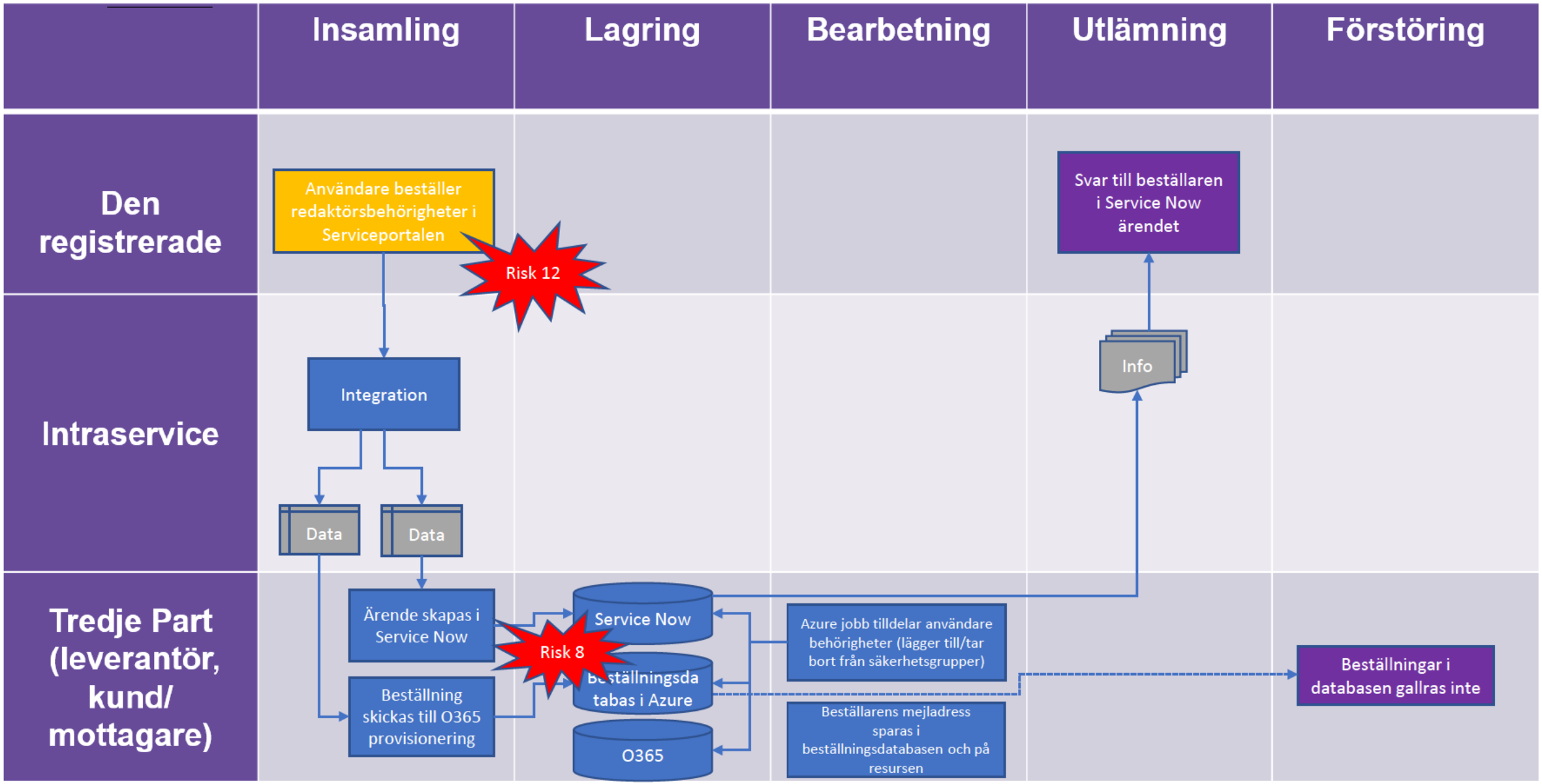
- Uppgifterna är inlagda i ett system och överförs via systemet, eller läggs in i ett system

- Lagring sker i ett skåp eller i ett arkiv
- Lagring sker i ett datasystem
- Möjlig risk

- Orange färg, här börjar processen, orange färg ex.
- Här slutar processen, är inte alltid med, - lila färg ex.

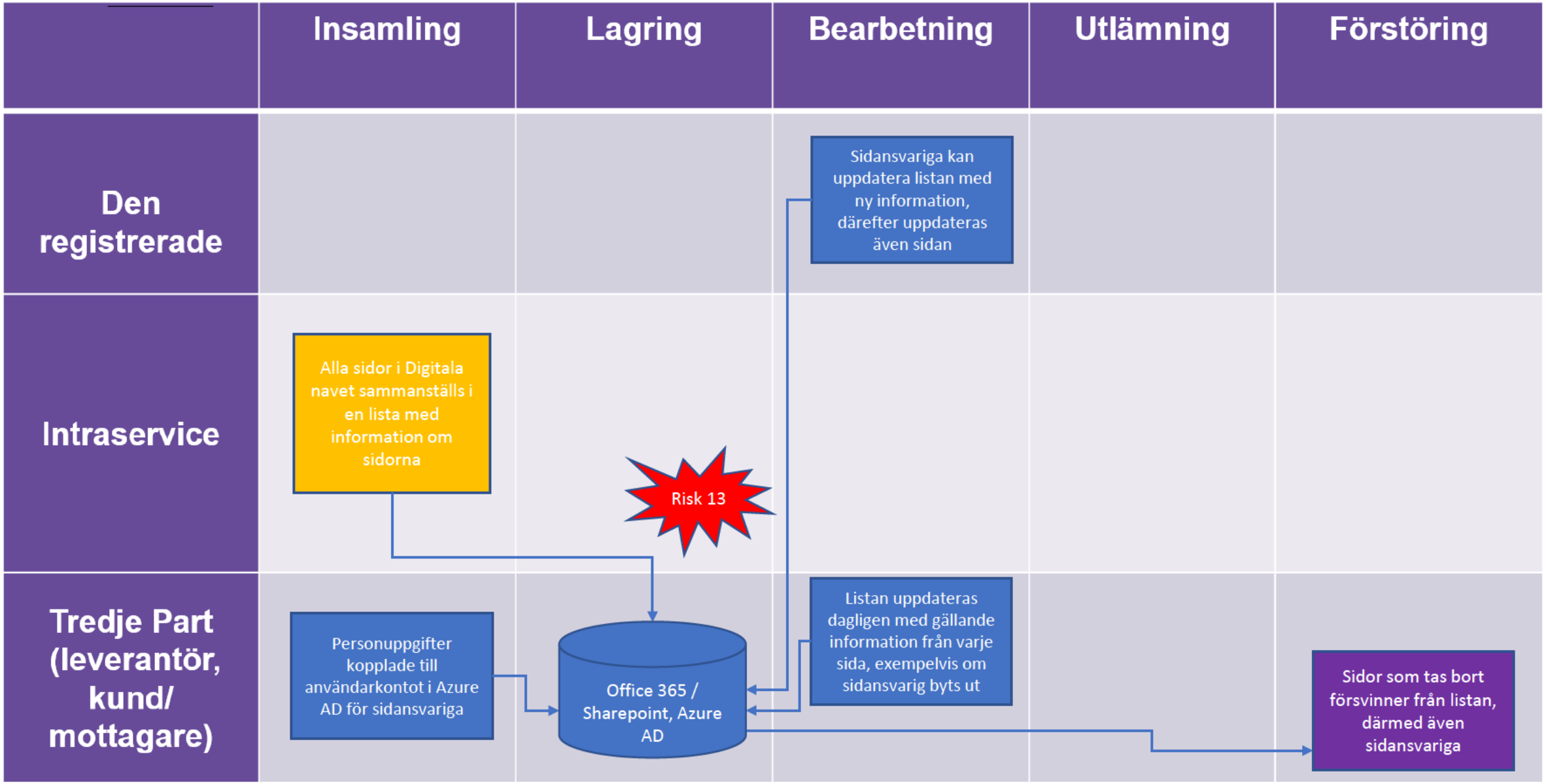
M365/Navet

2- Beställningar av redaktörsbehörigheter i Digitala navet via Serviceportalen



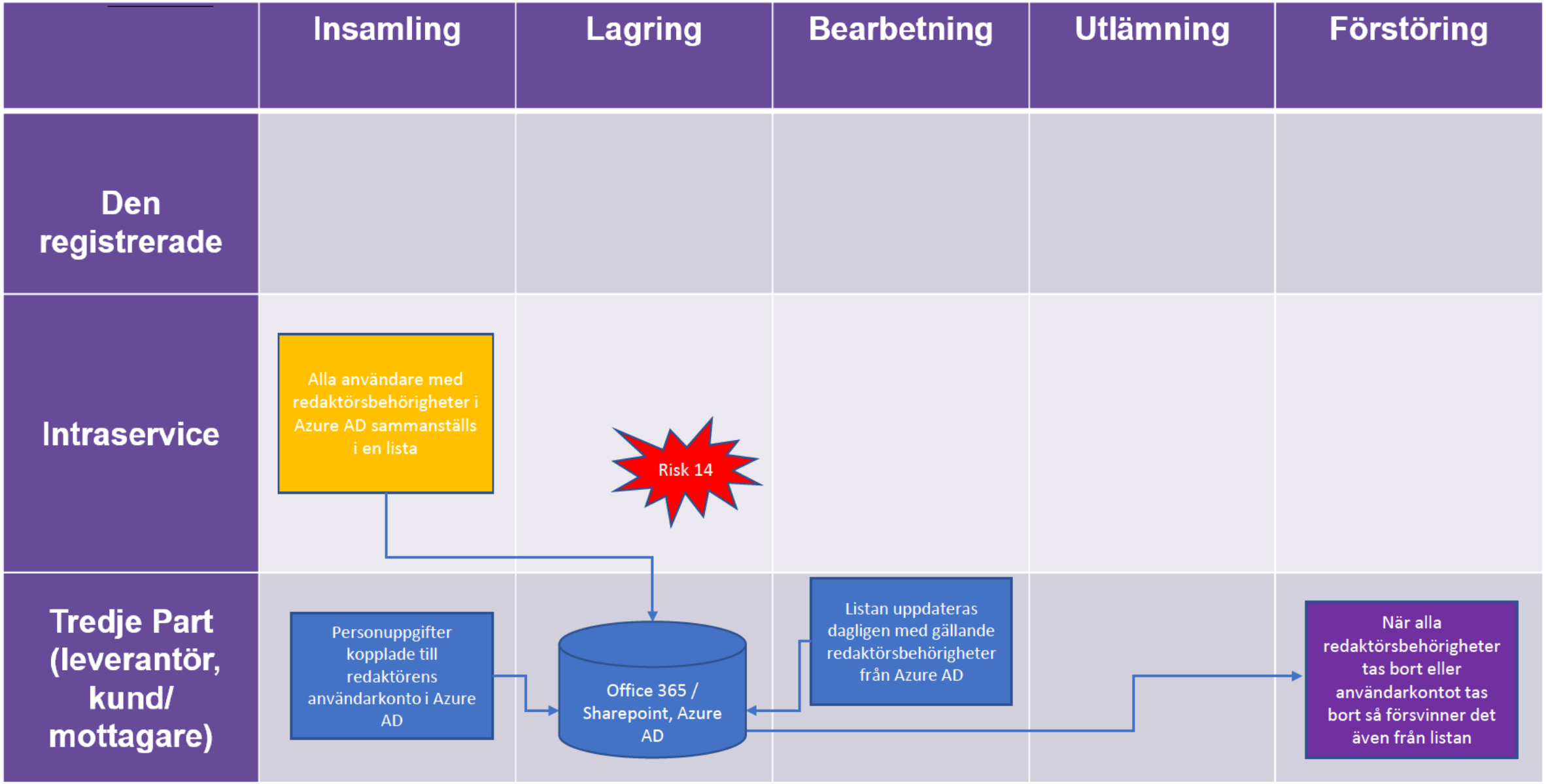
M365/Navet

3- Lista över alla sidor i Digitala navet



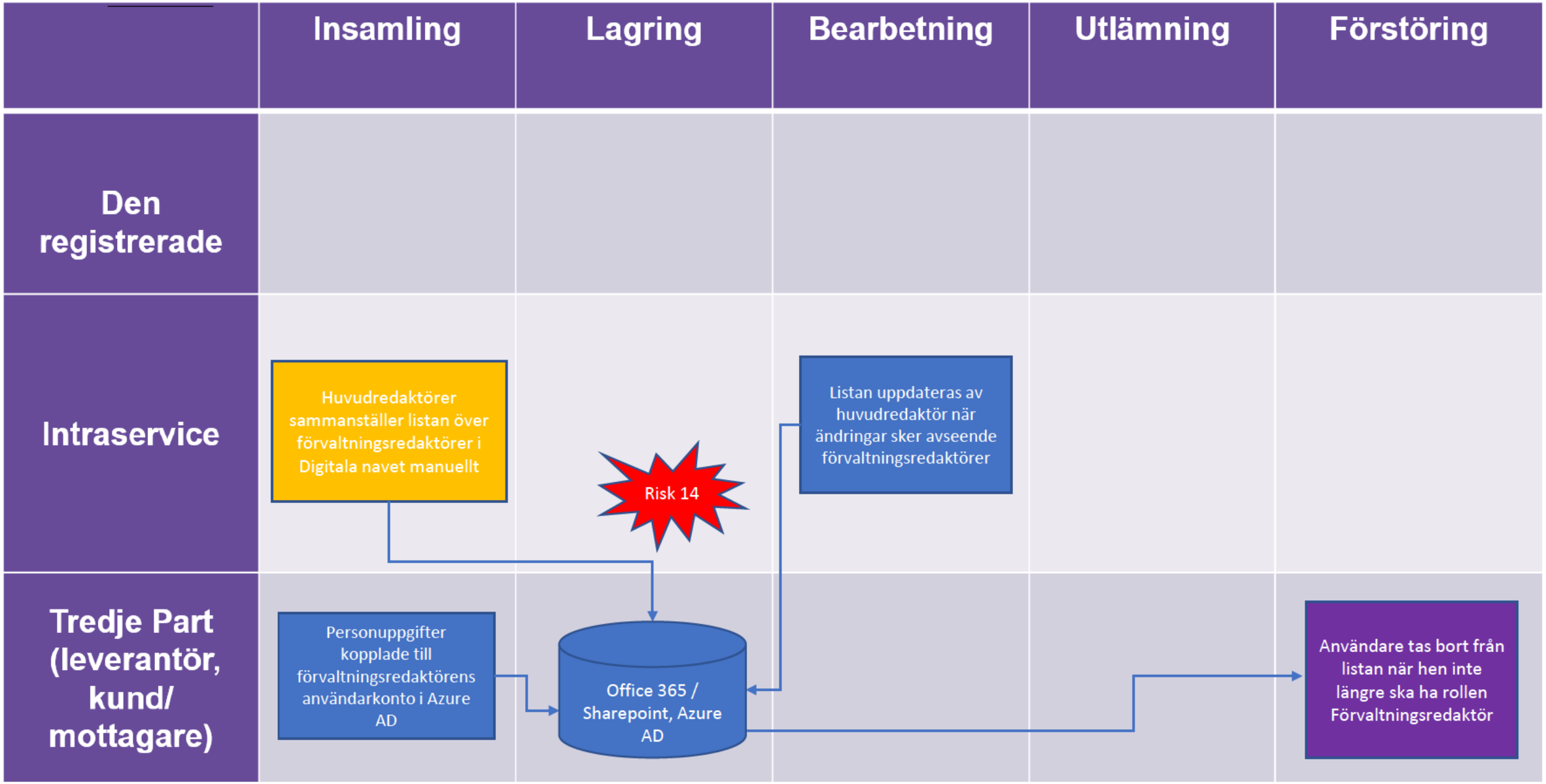
M365/Navet

4 - Lista över redaktörsbehörigheter



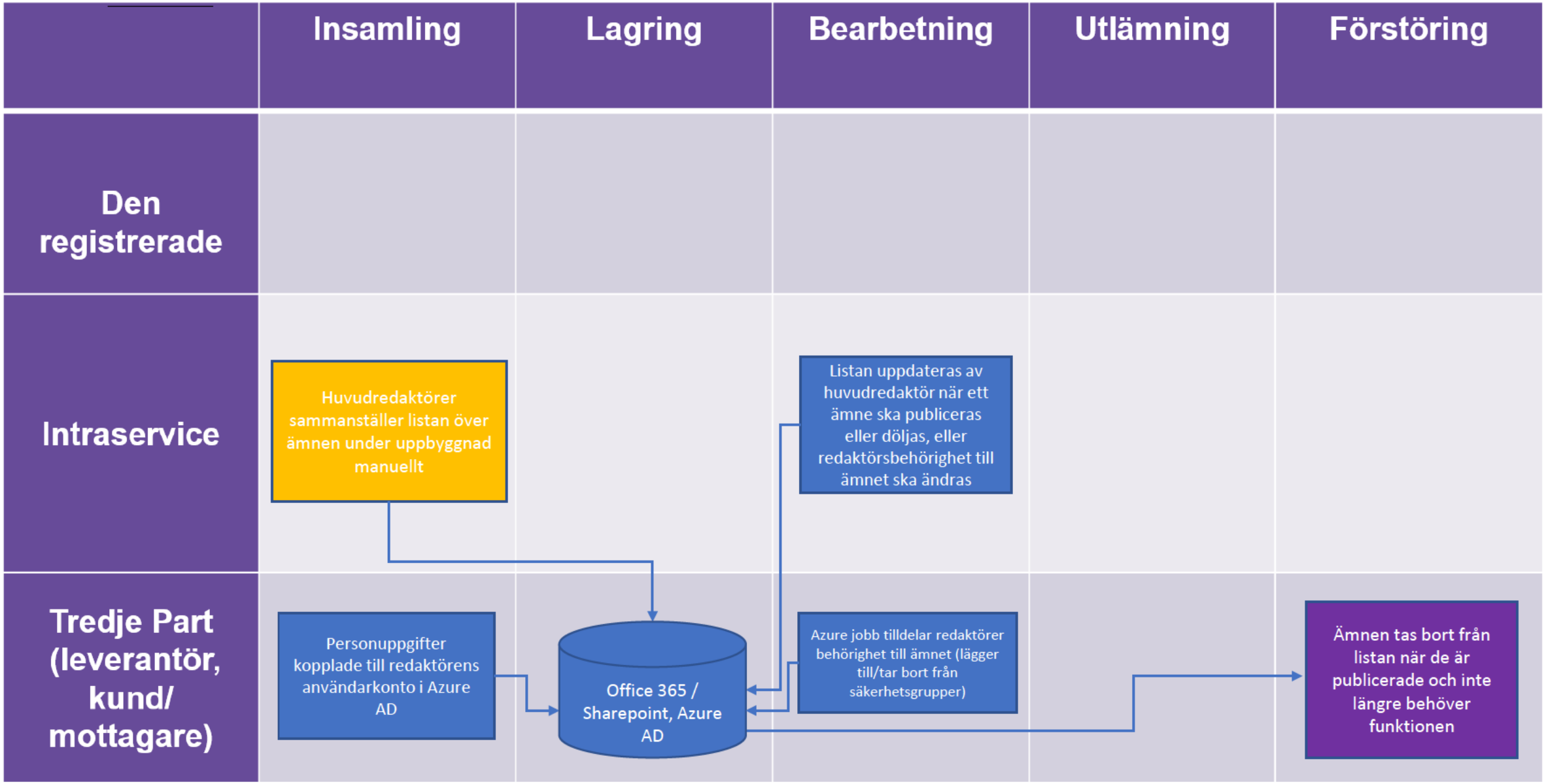
M365/Navet

5- Lista över förvaltningsredaktörer



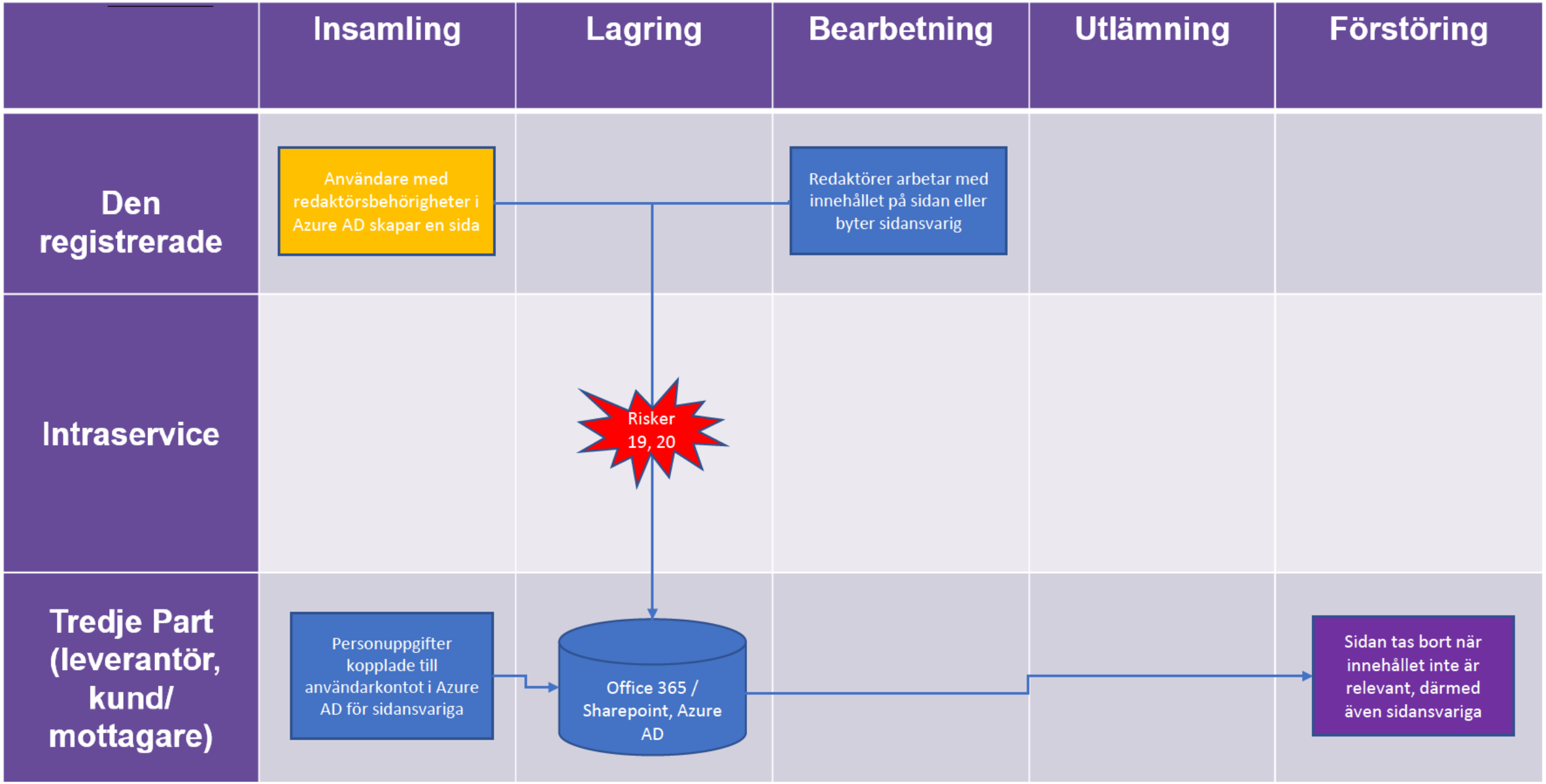
M365/Navet

6 - Lista för ämnen under uppbyggnad



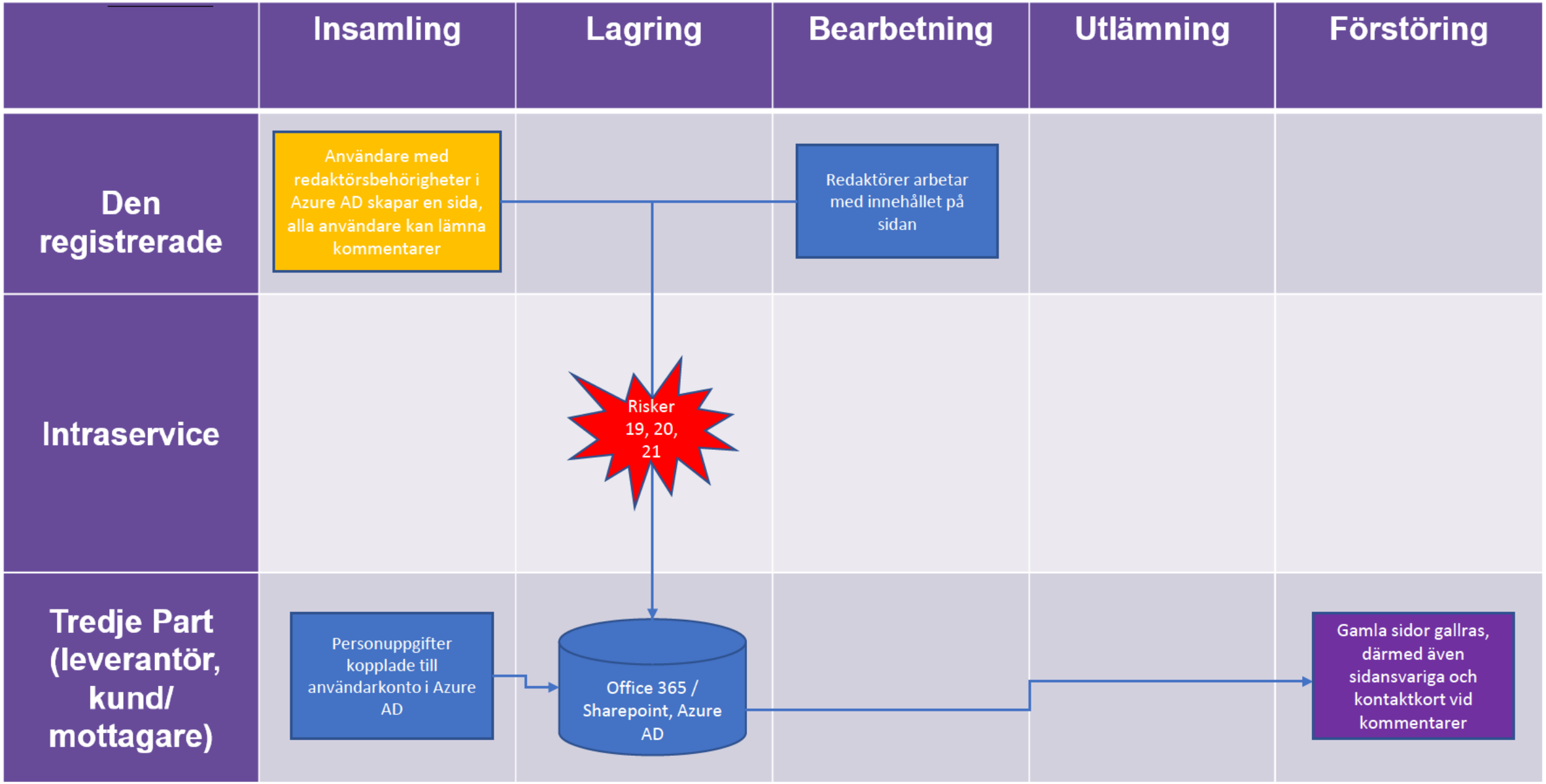
M365/Navet

7 - Artikelsidor och specifika tillägg



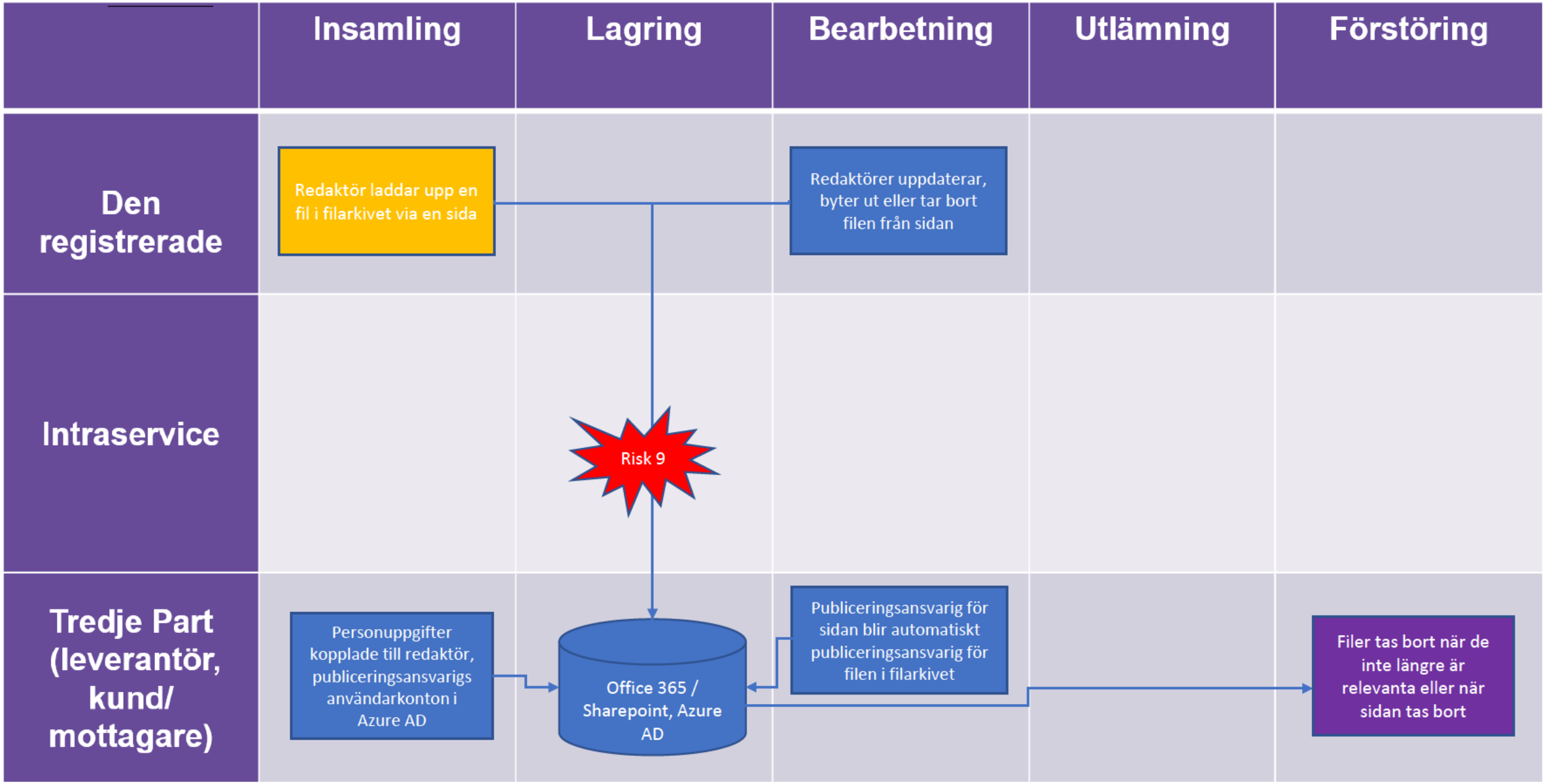
M365/Navet

8 - Inlägg i kommunikativa kanaler



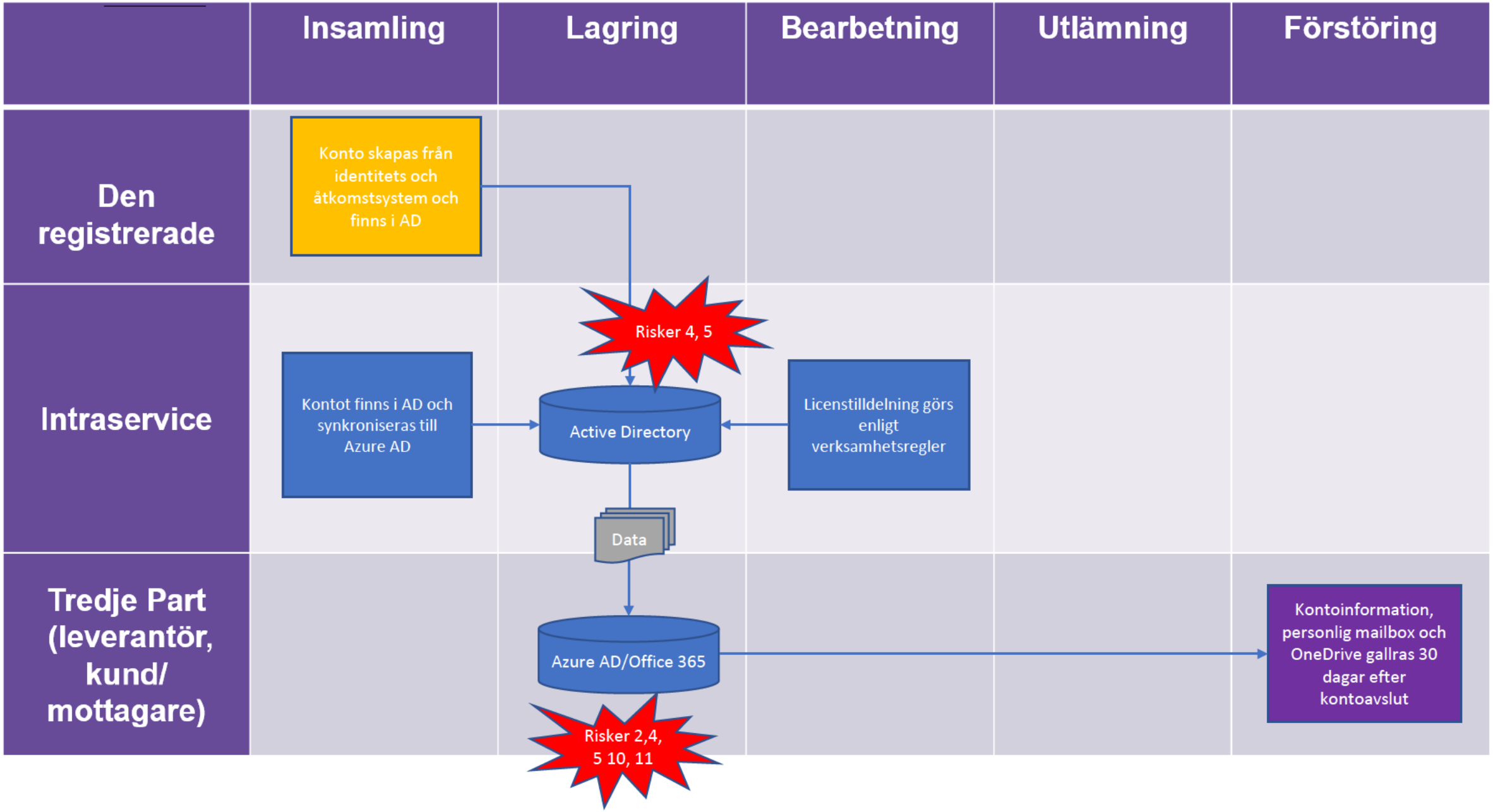
M365/Navet

9 - Filer i Digitala navets filarkiv



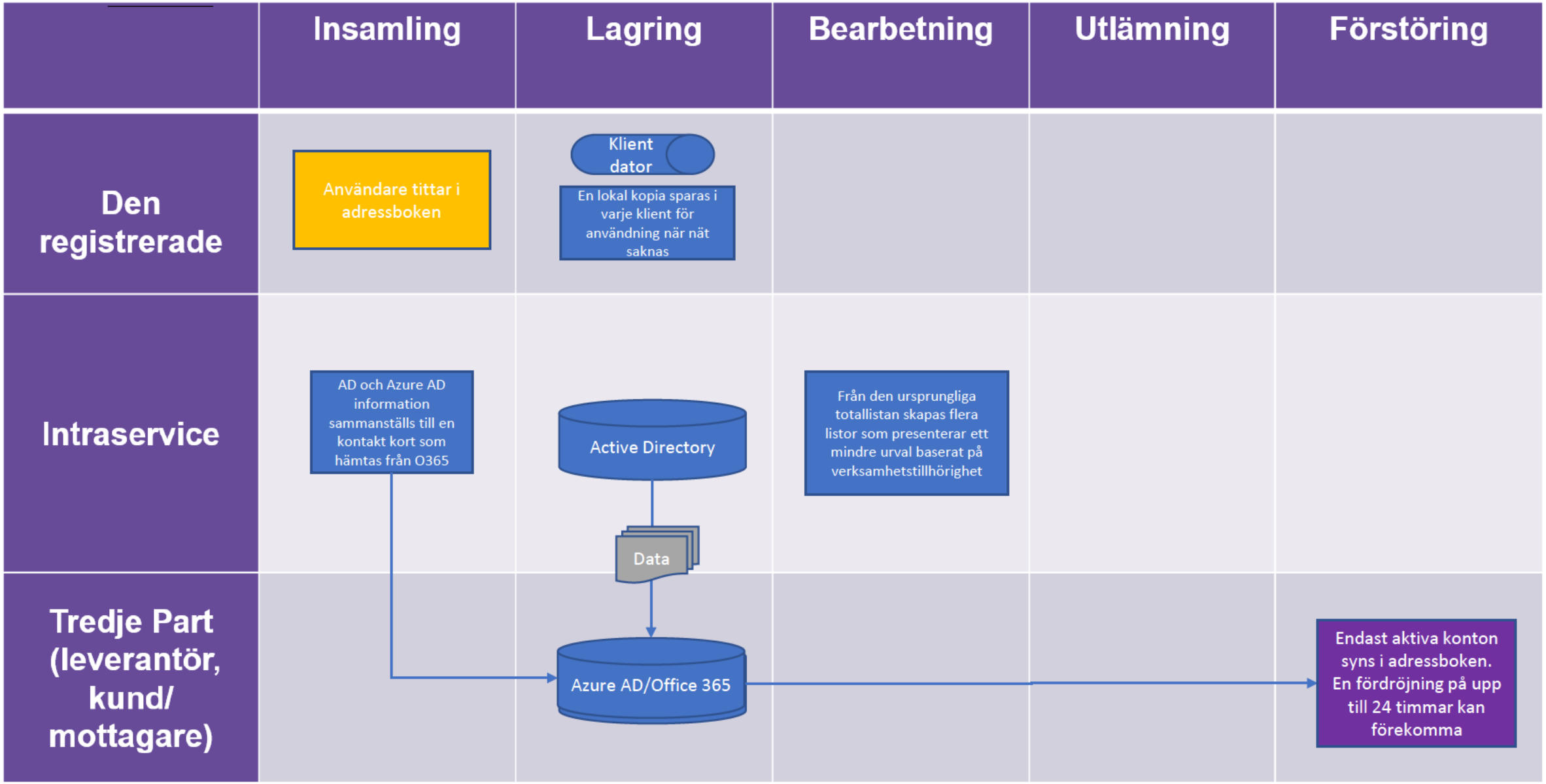
M365/Navet

10 - Kontoskapande



M365/Navet

11- Adressboken i Outlook



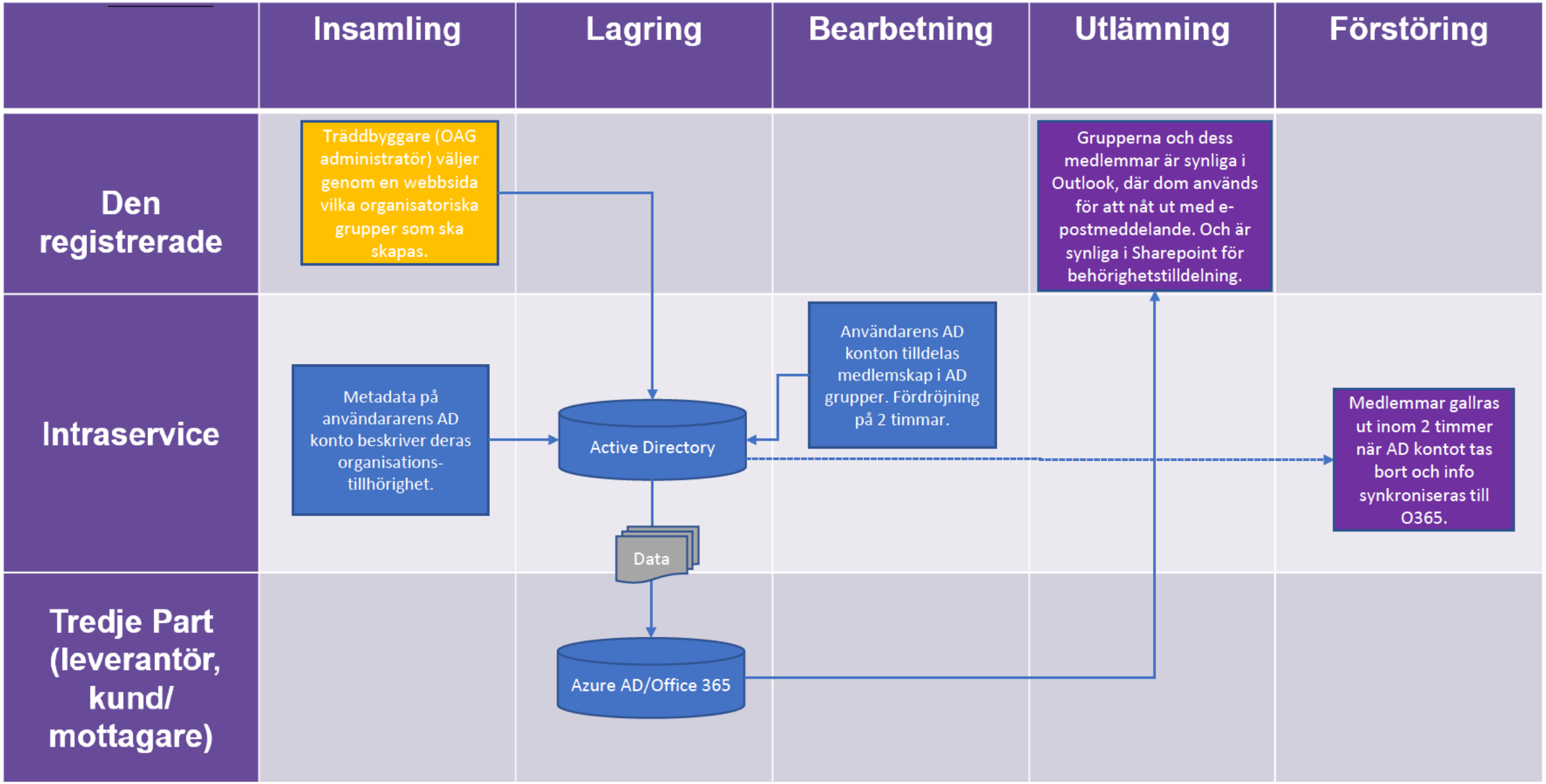
M365/Navet

Kontakt korten

	Insamling	Lagring	Bearbetning	Utlämning	Förstöring
Den registrerade	Användare söker information om en kollega.				
Intraservice	Azure AD information sammanställs till en kontakt kort som hämtas från O365				
Tredje Part (leverantör, kund/ mottagare)		Azure AD/Office 365			Endast aktiva konton har ett kontakt kort. En fördröjning på upp till 24 timmar kan förekomma

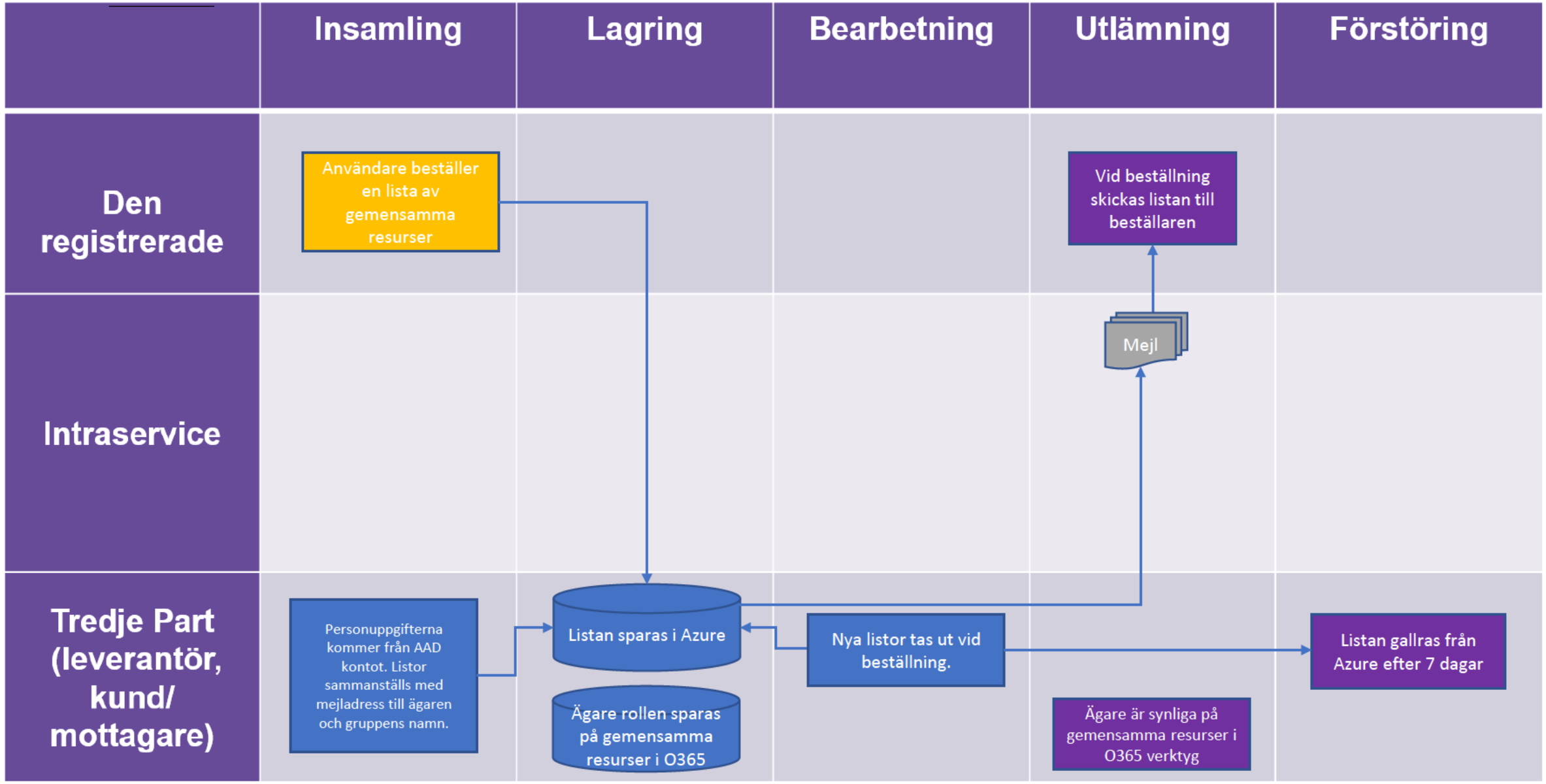
M365/Navet

13 - Skapade av organisatoriska AD grupper (OAG)



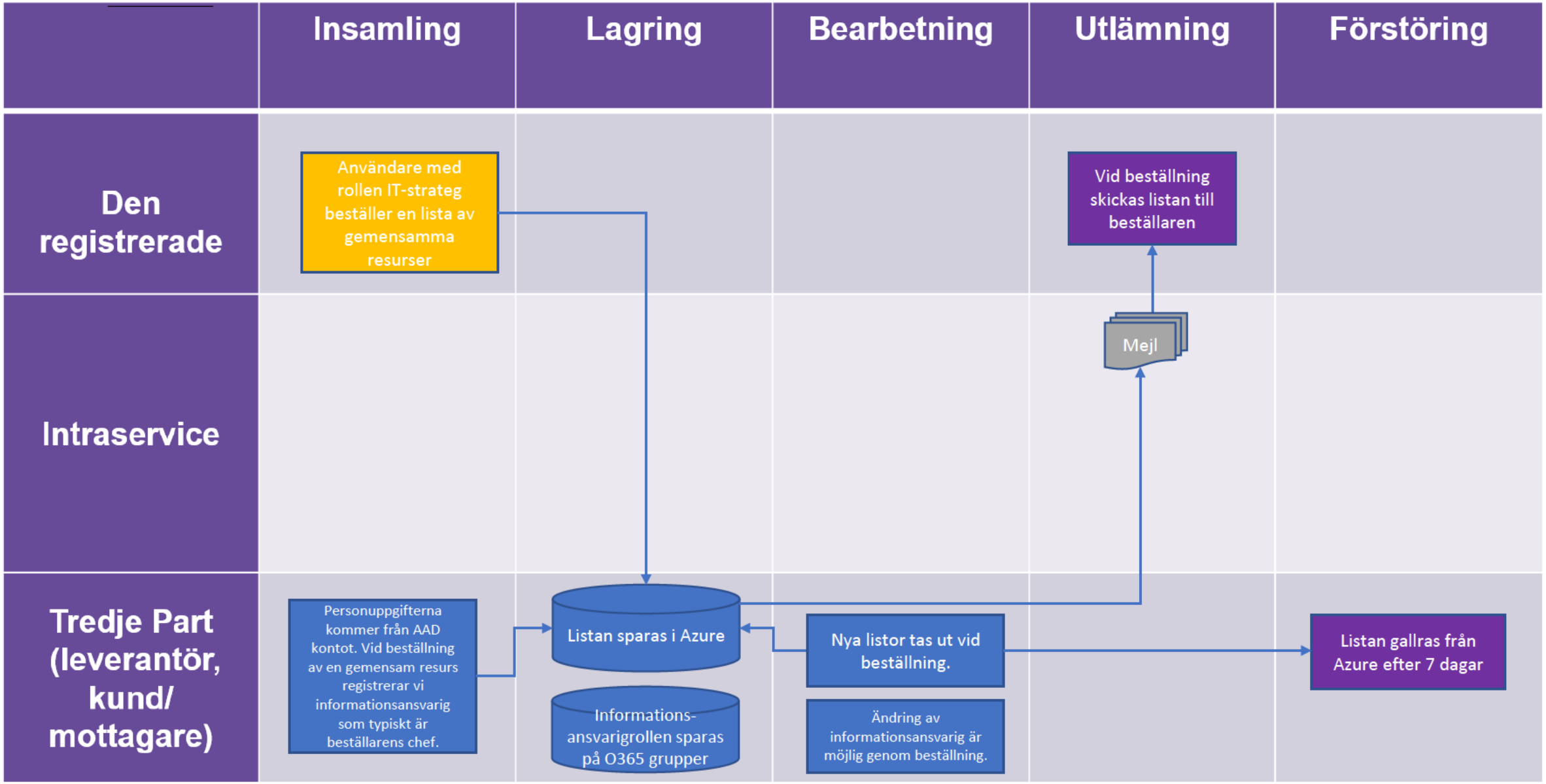
M365/Navet

14 - Ägare rollen



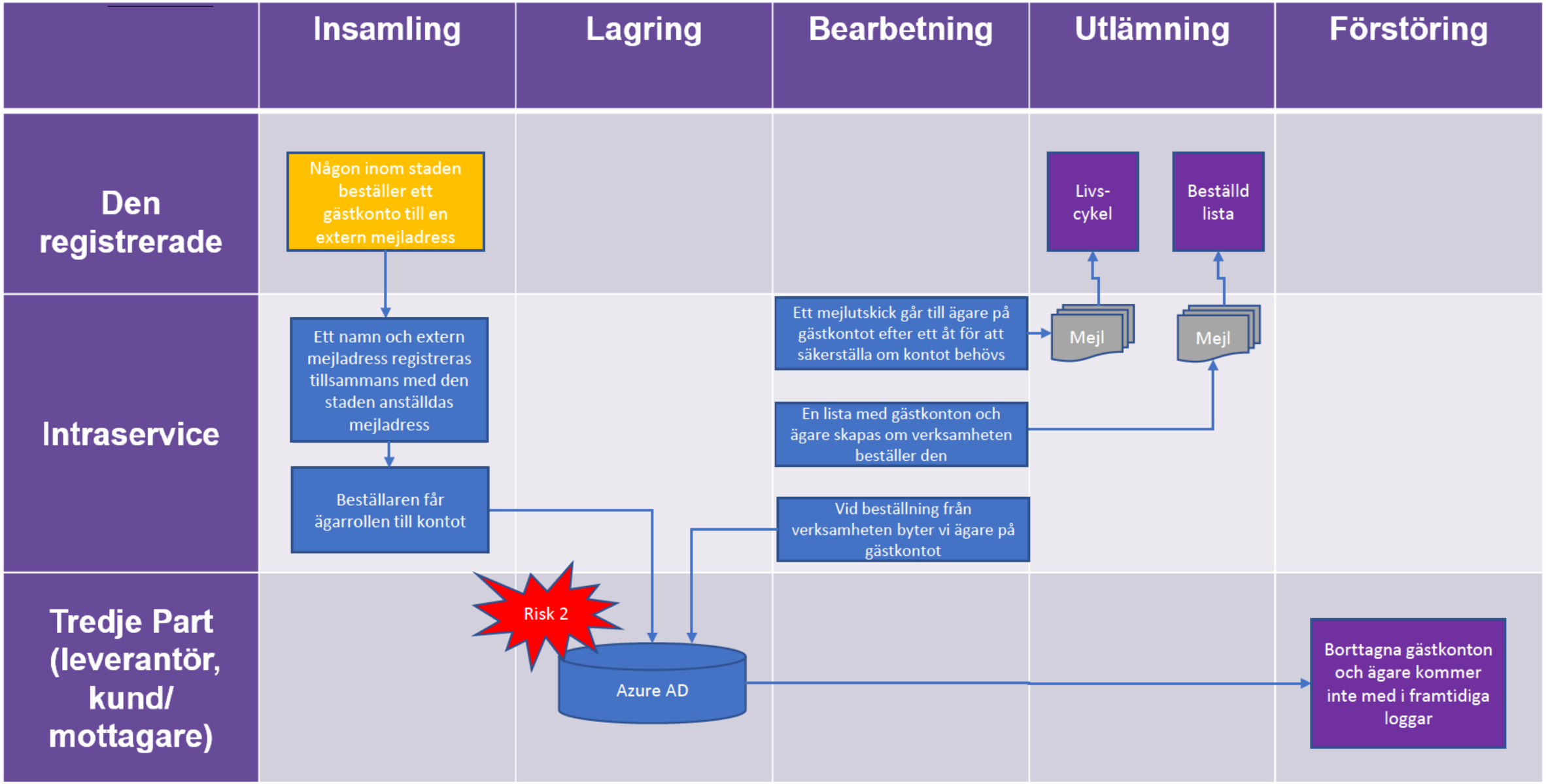
M365/Navet

15- Informationsansvarig rollen



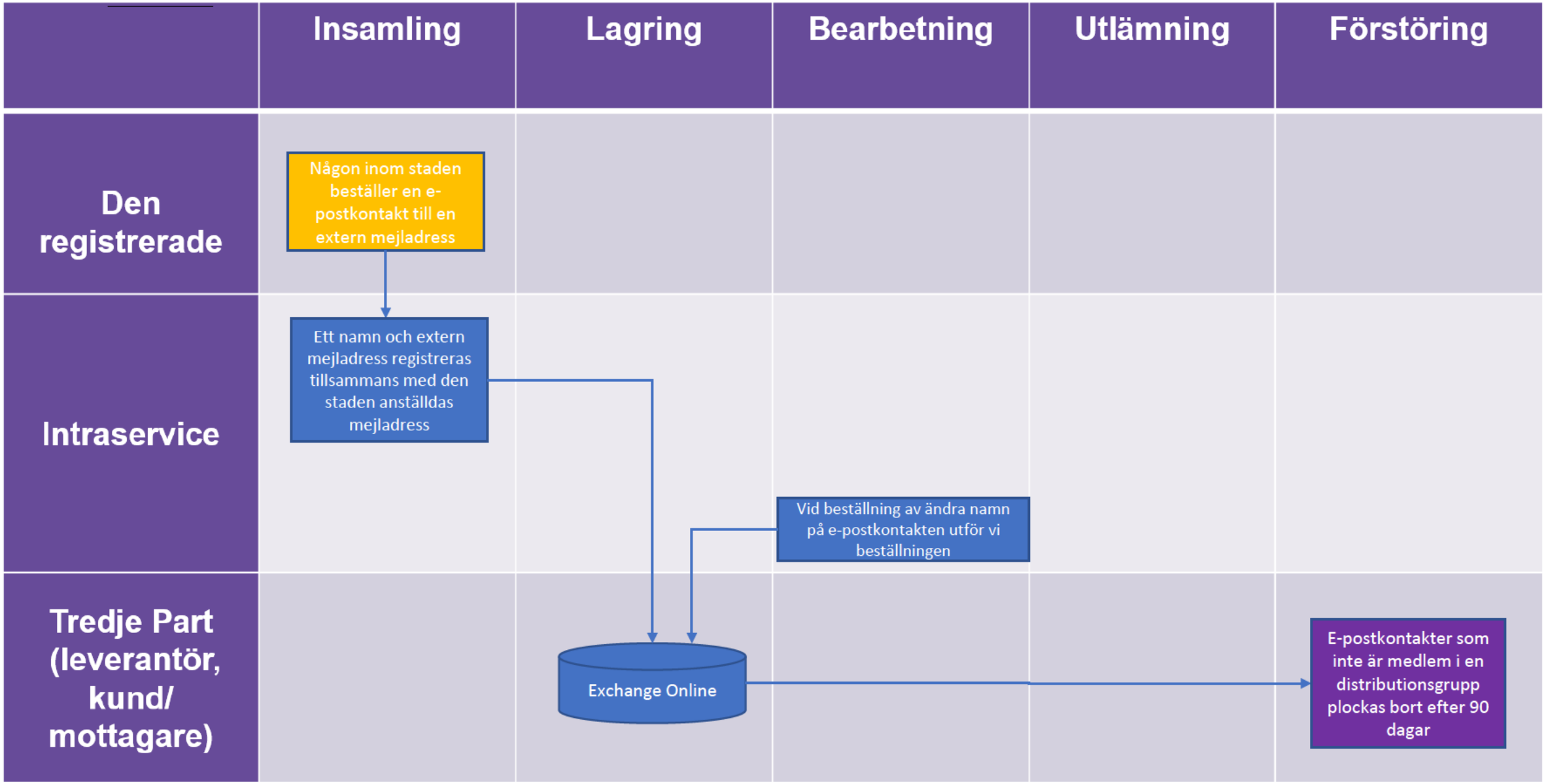
M365/Navet

16 - Gästkonton



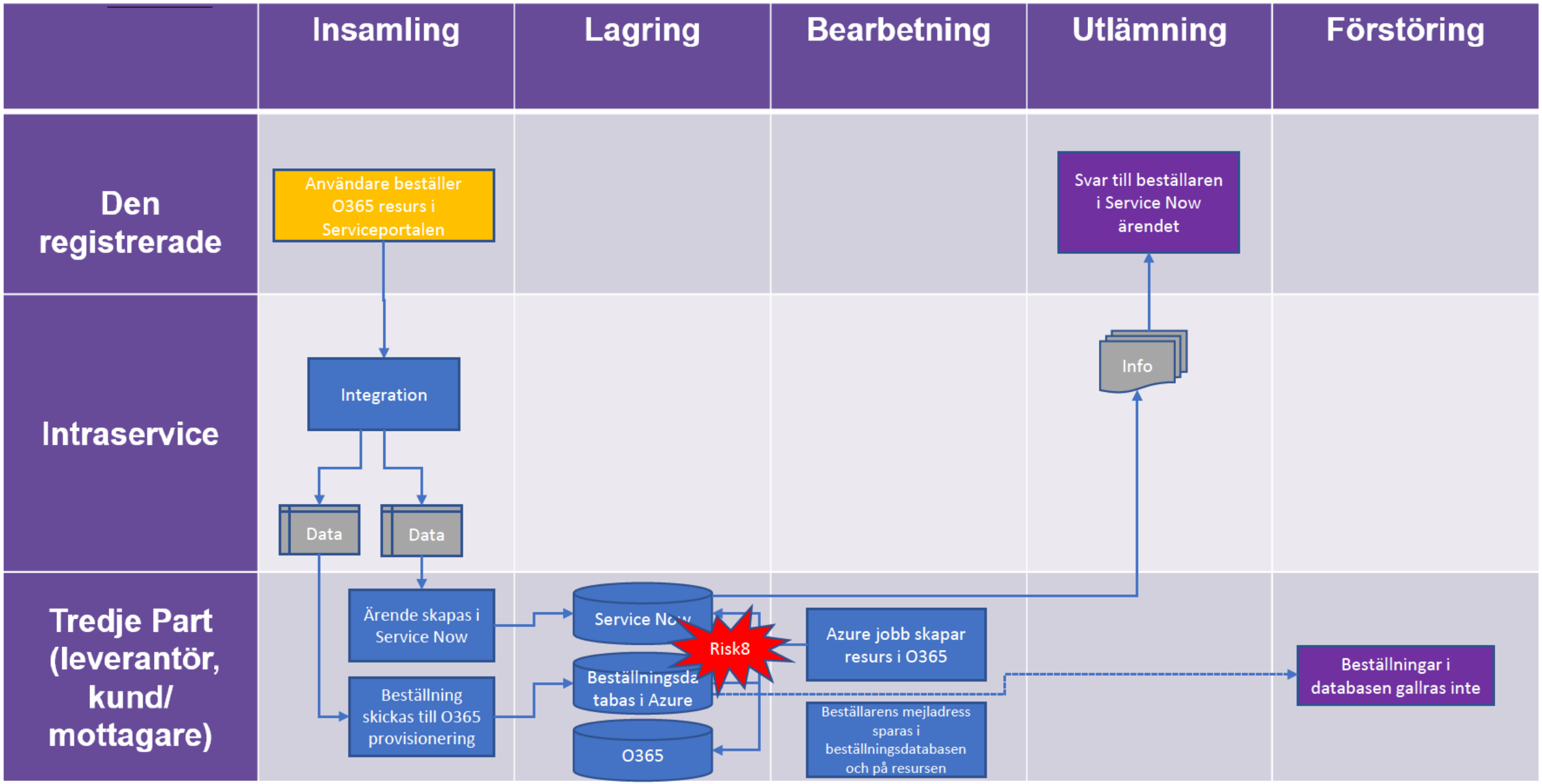
M365/Navet

E-postkontakter



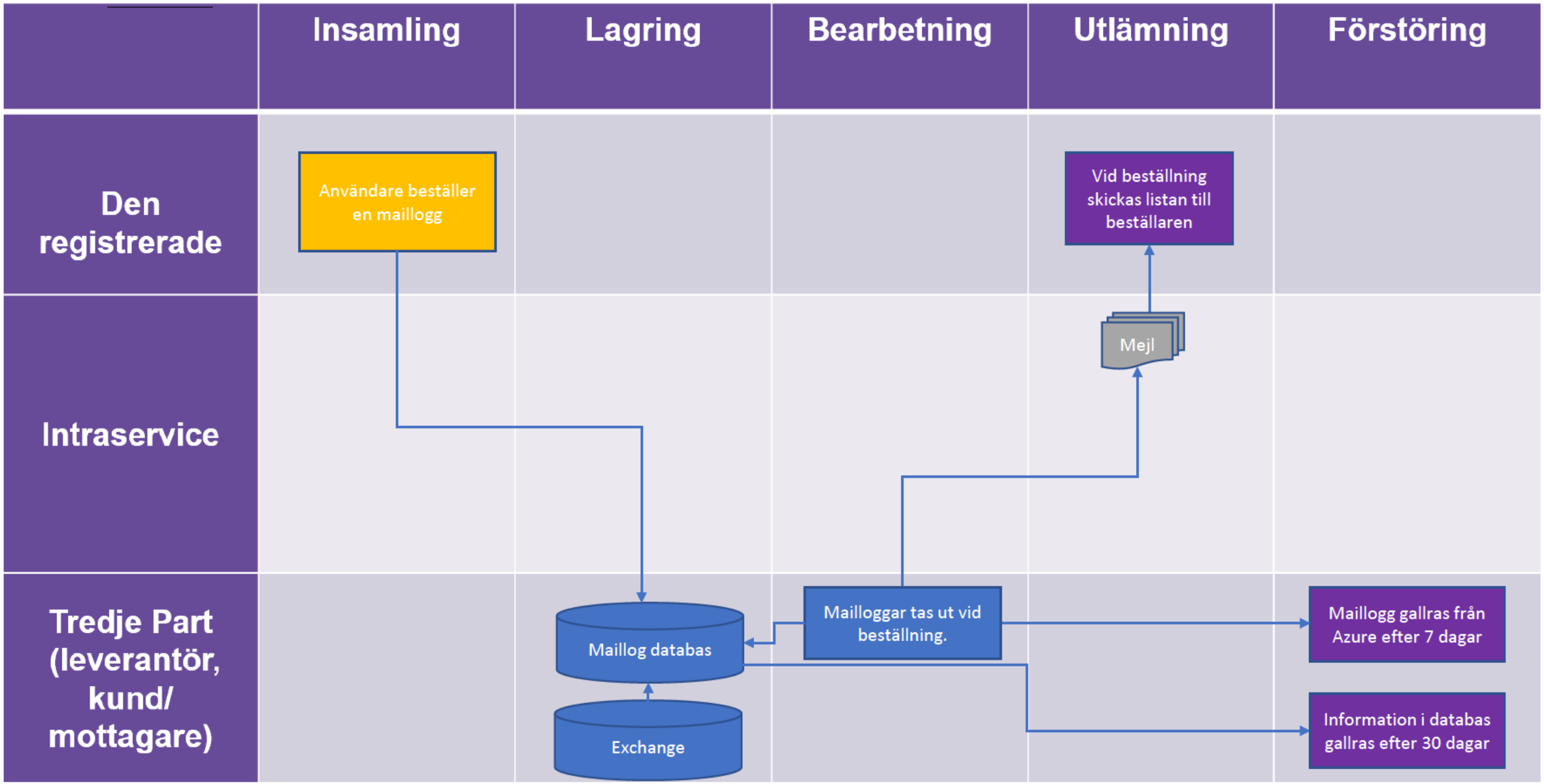
M365/Navet

18 - Beställningar av Office 365 resurser i Serviceportalen



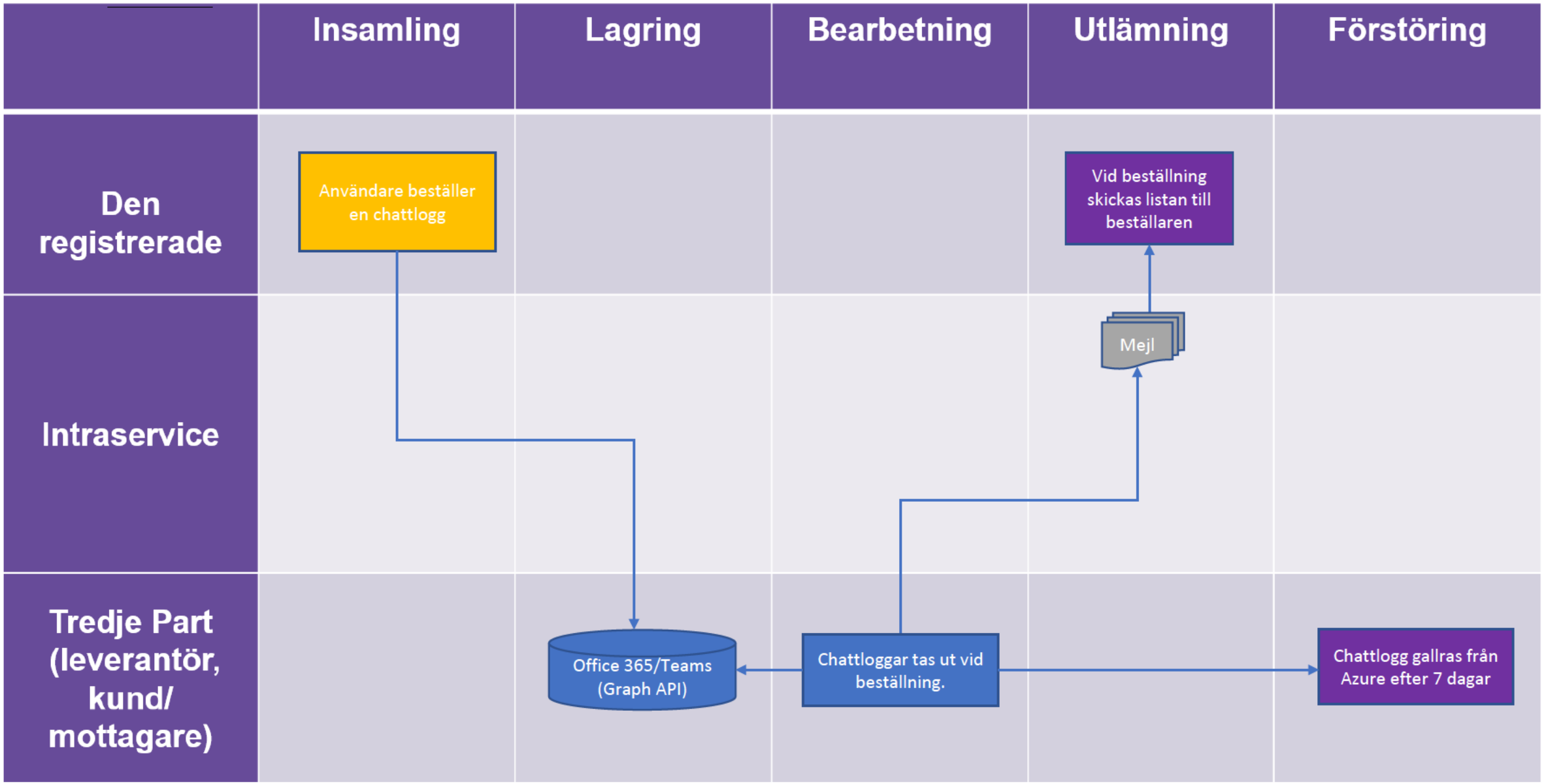
M365/Navet

19 - Mailbox loggning



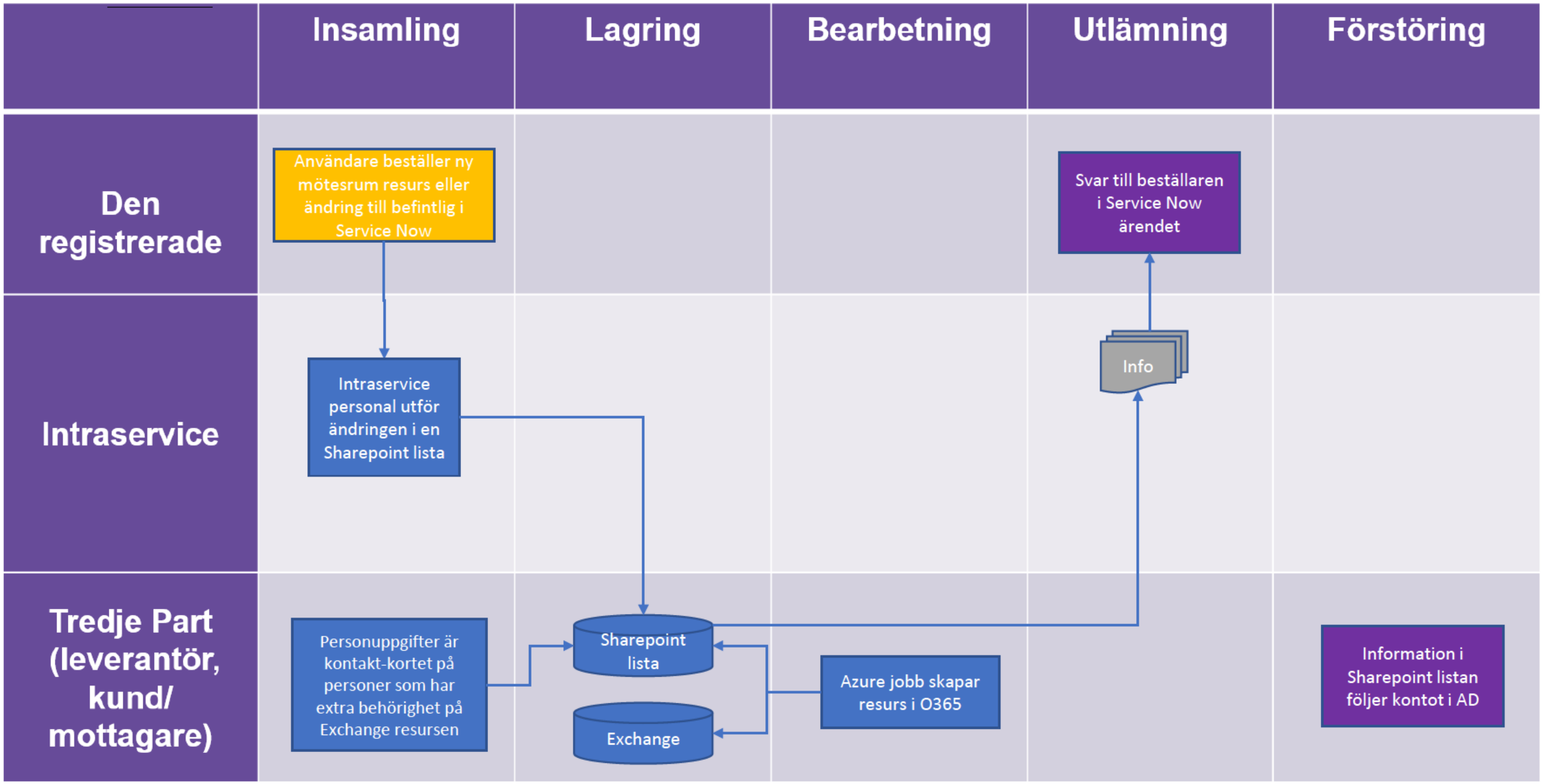
M365/Navet

Chatt loggning



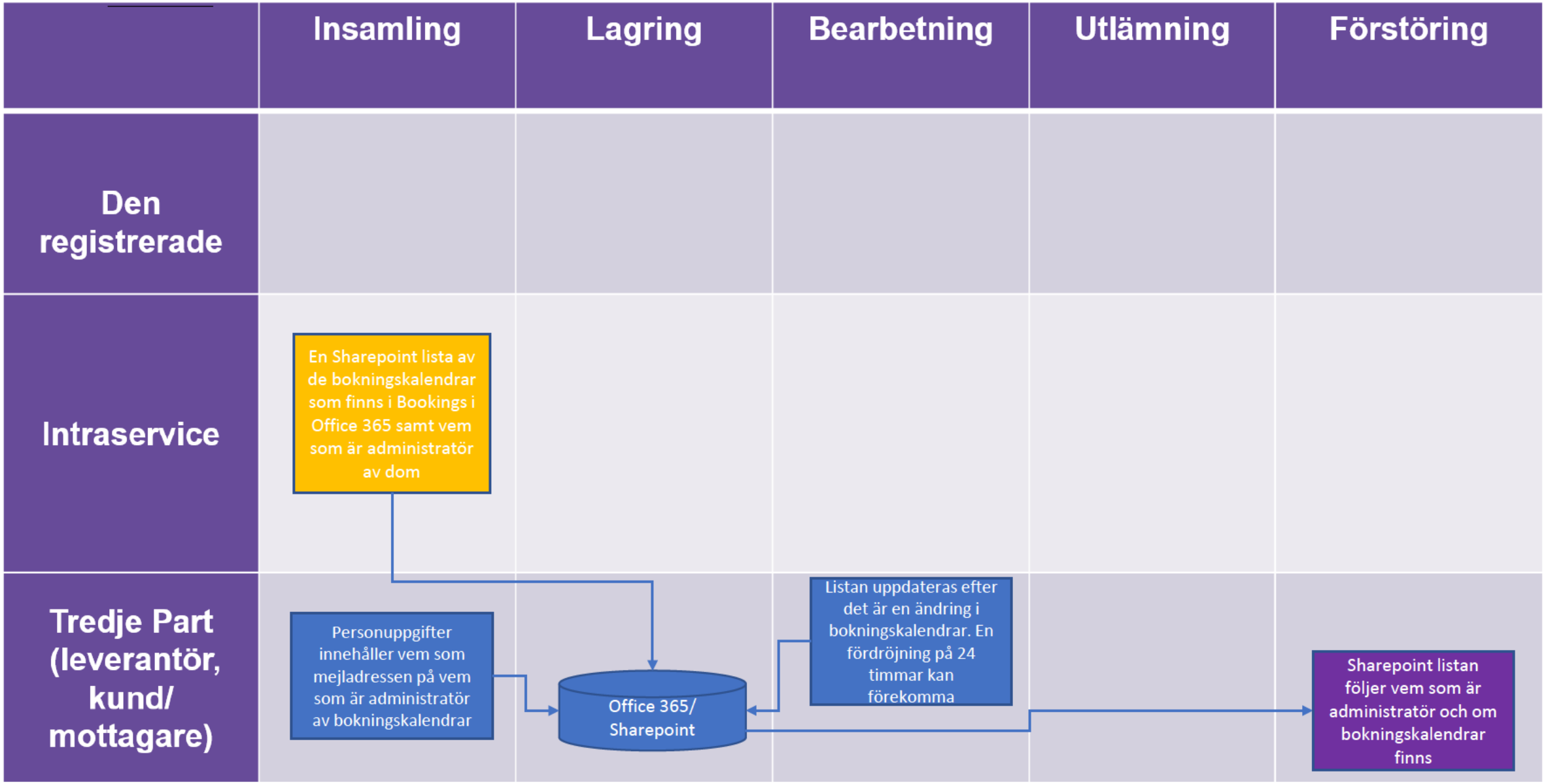
M365/Navet

21 - Exchange resursadministration



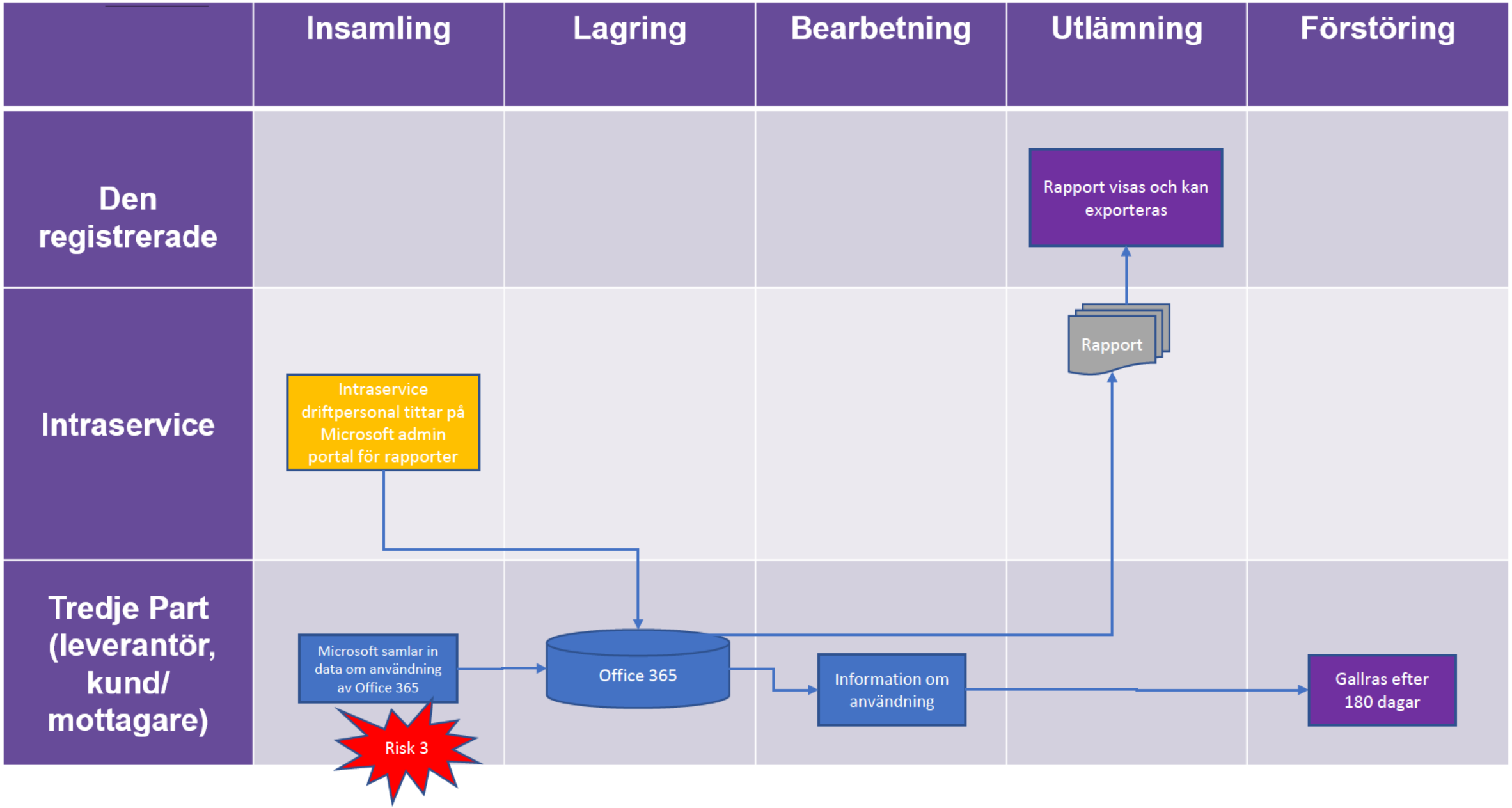
M365/Navet

22 - Microsoft Bookings



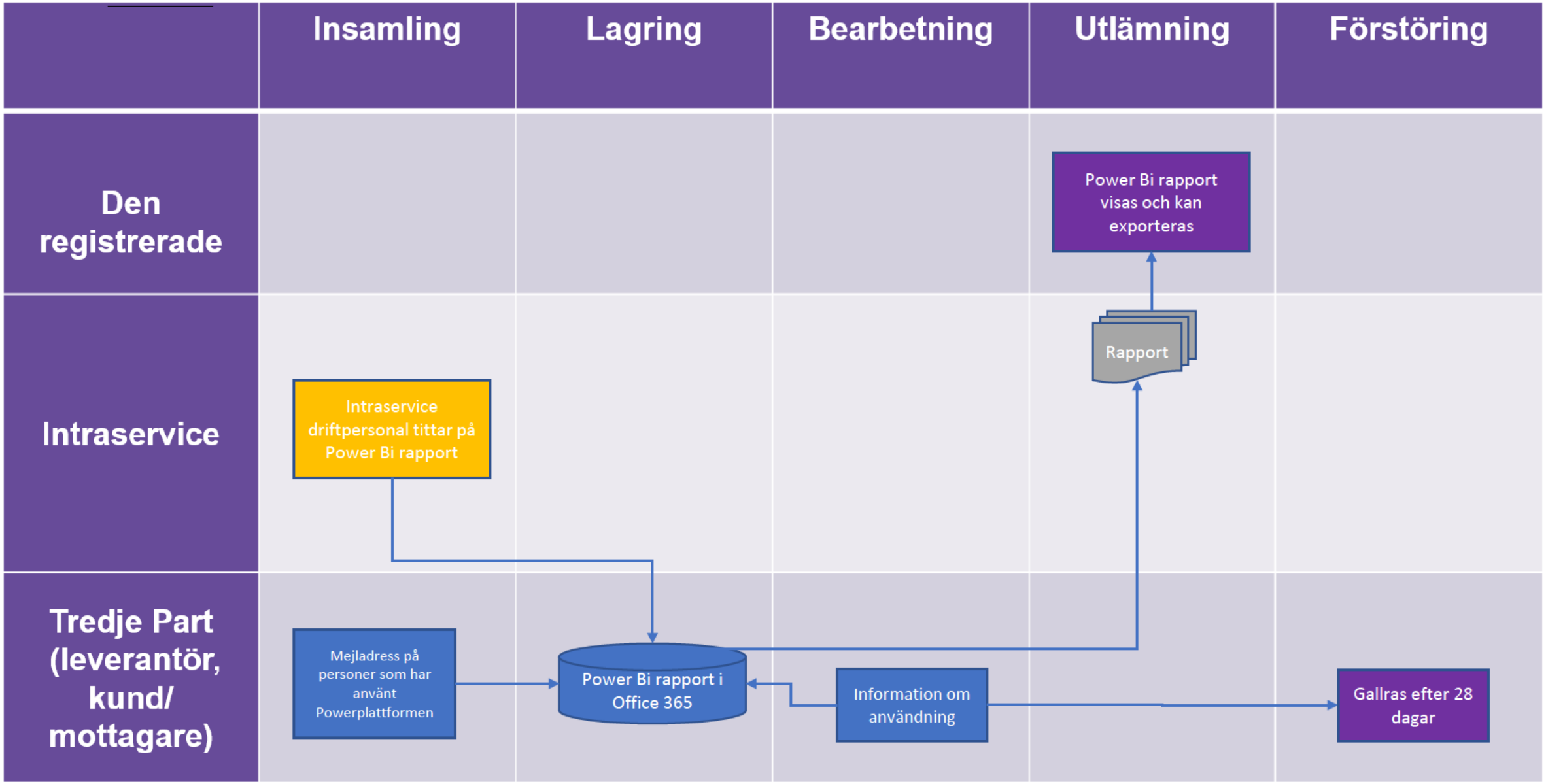
M365/Navet

23 - Rapporter och statistik leveranser



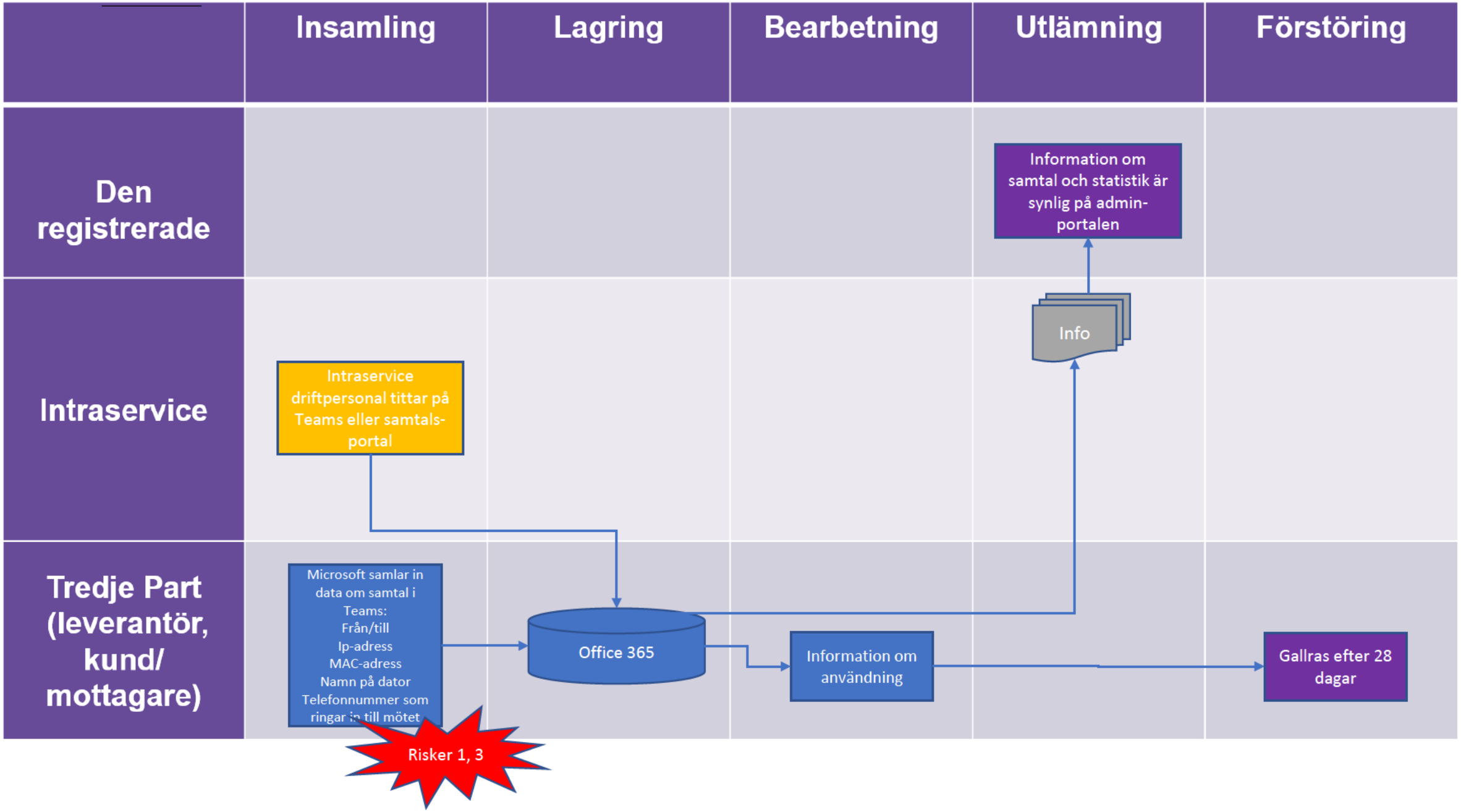
M365/Navet

24 - Center of Excellence (CoE)



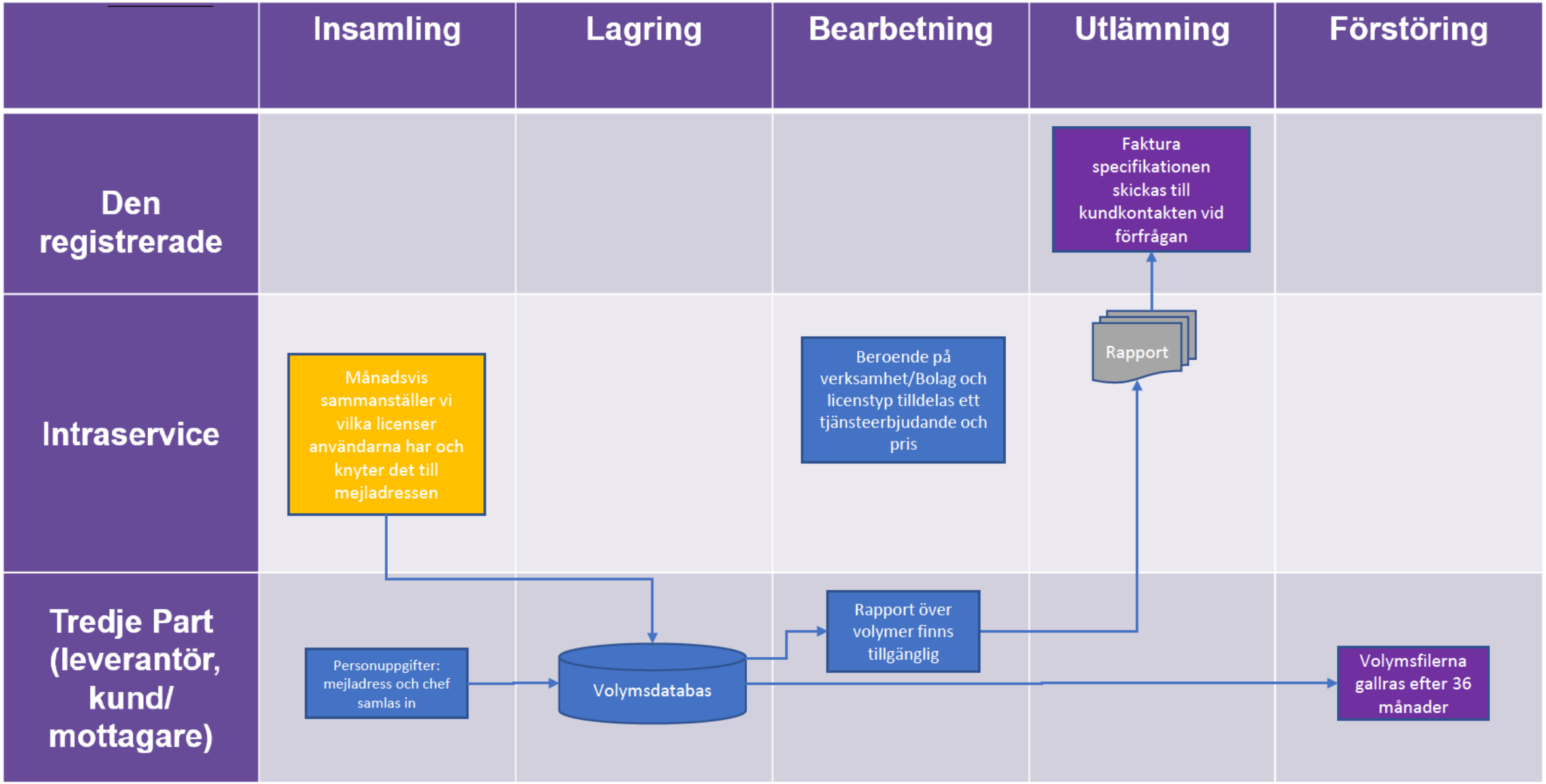
M365/Navet

25 Teams samtalsstatistik/analys



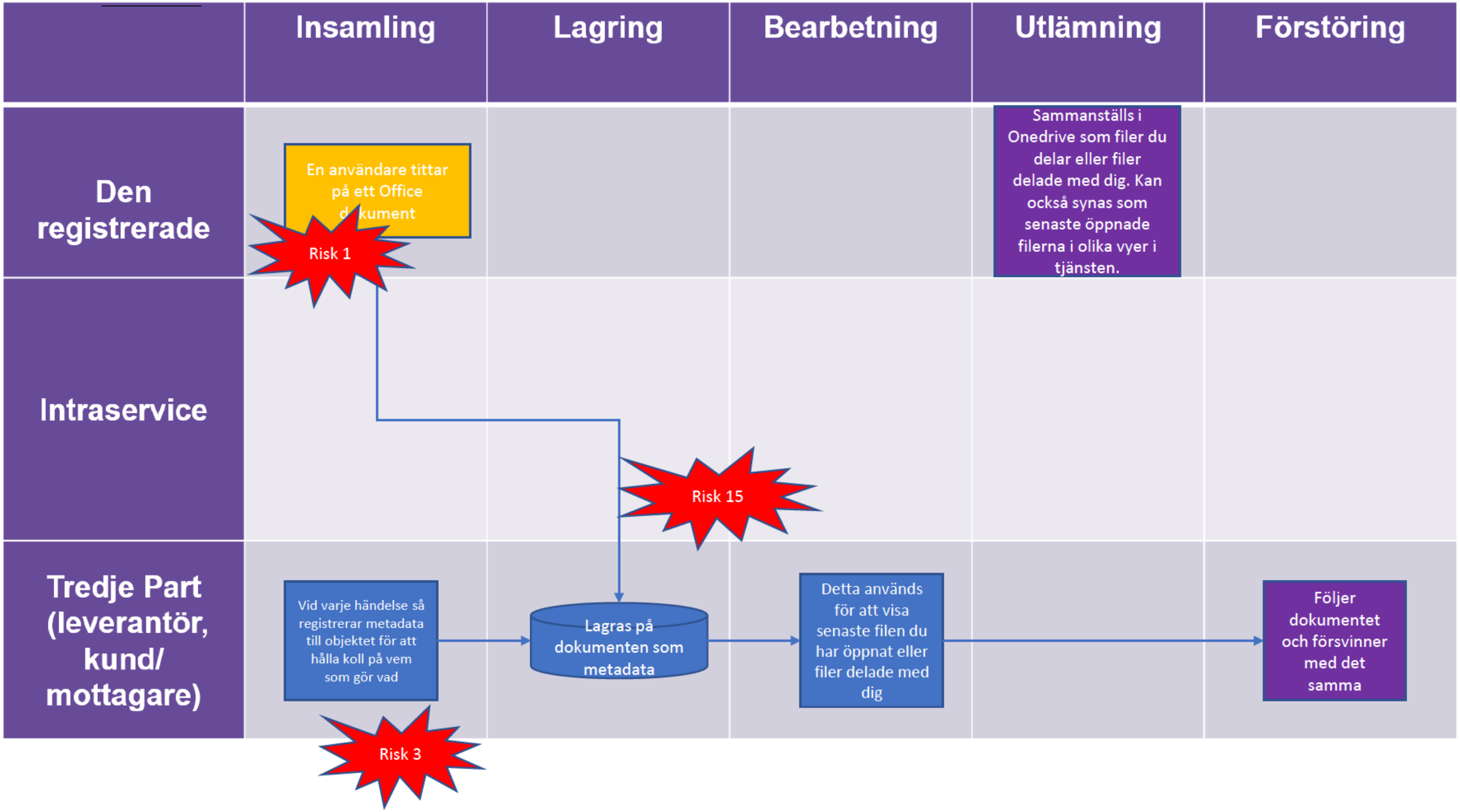
M365/Navet

26 - Volymsrapportering



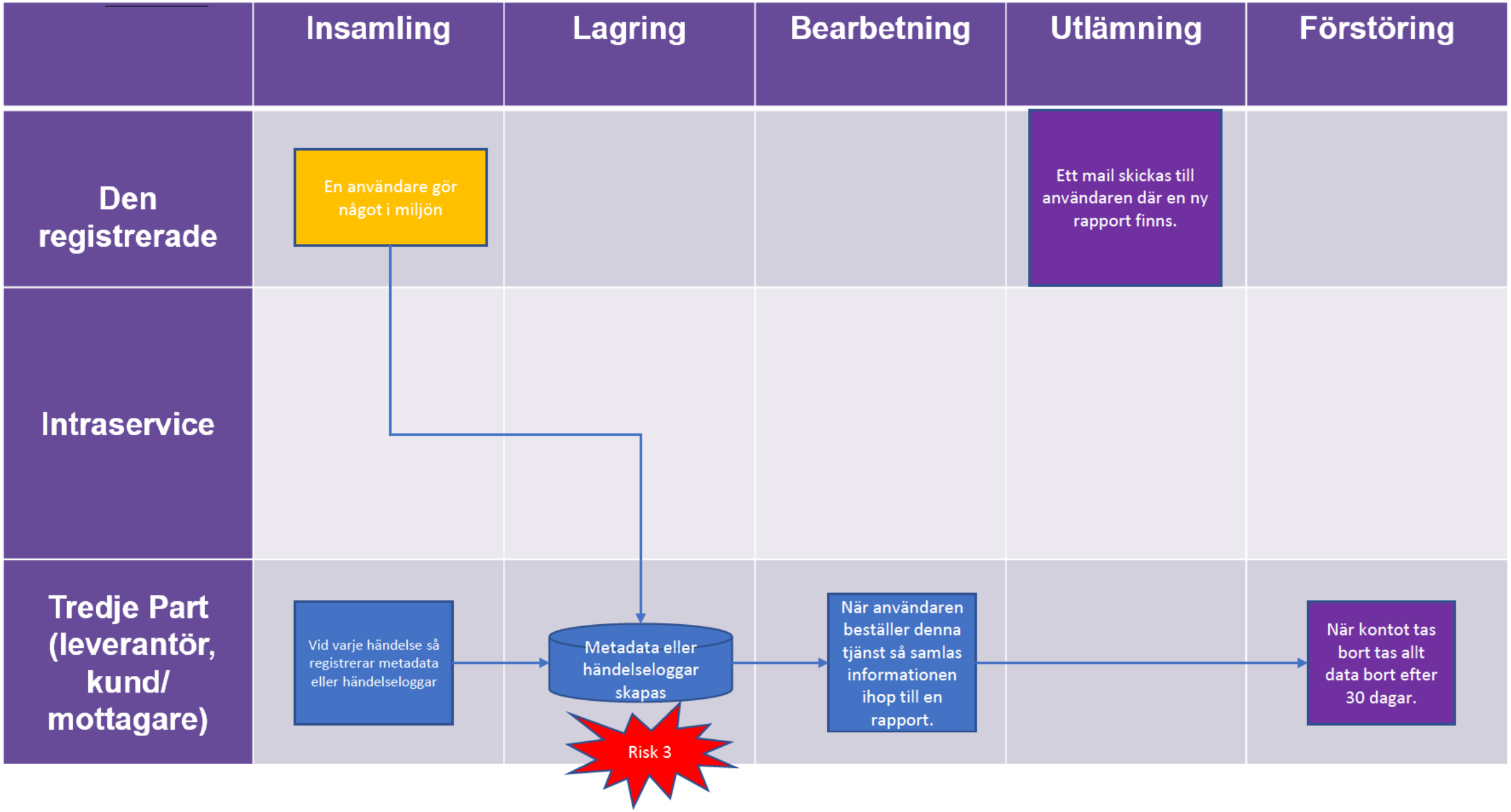
M365/Navet

27 - Vem har gjort vad (metadata)



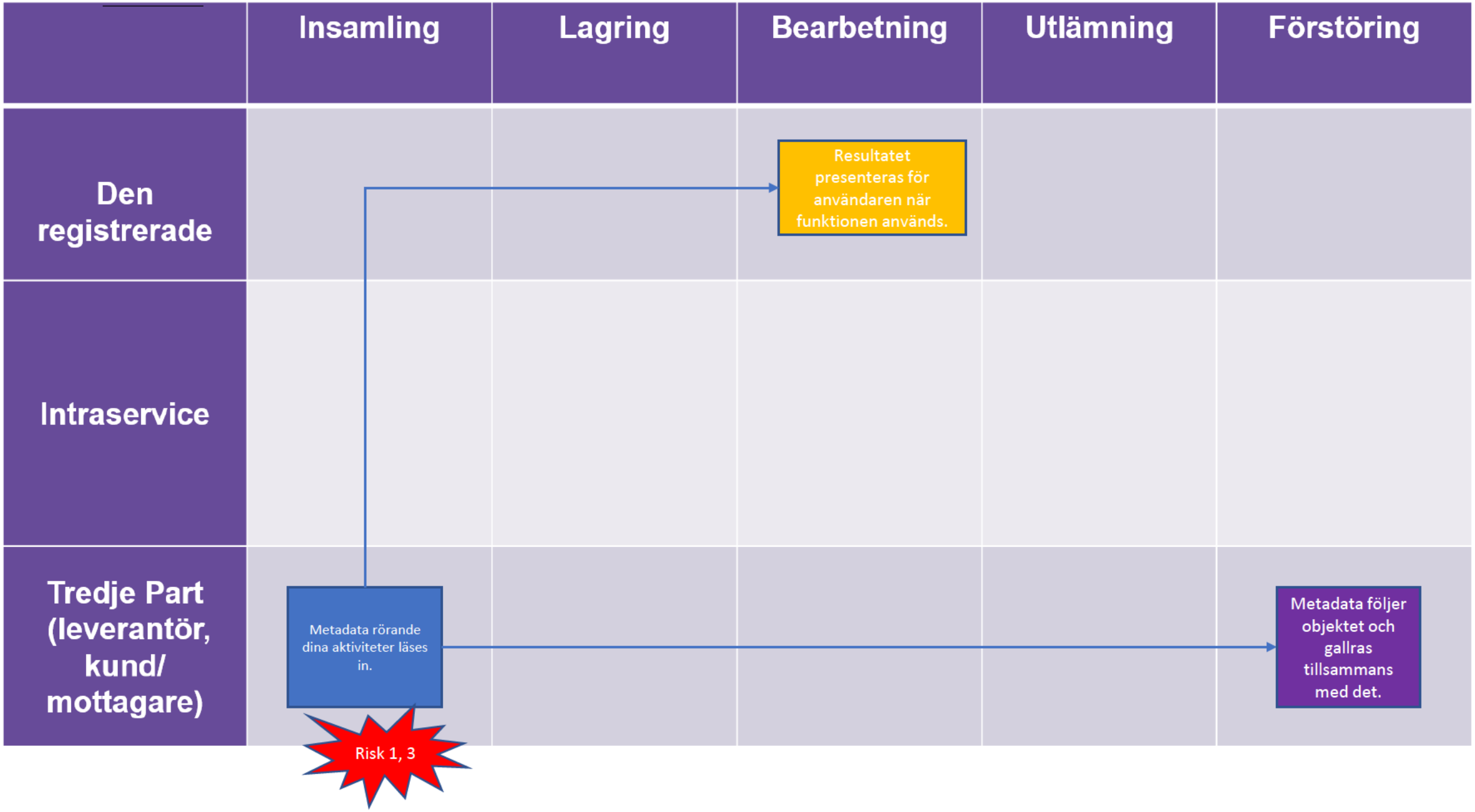
M365/Navet

28 - Viva Insights



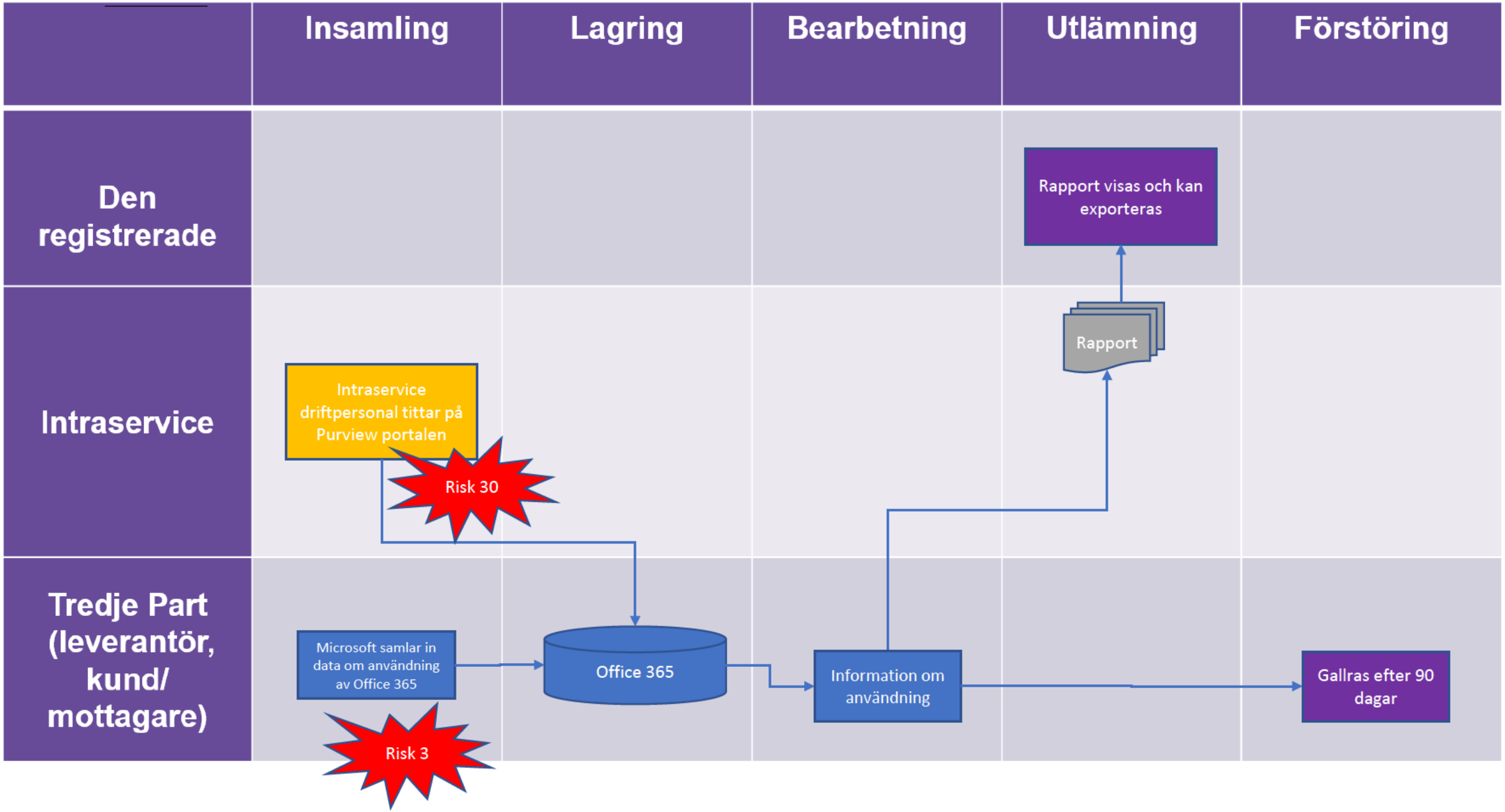
M365/Navet

29 - Delve och liknande SharePoint funktioner



M365/Navet

30 - Granskningsloggar



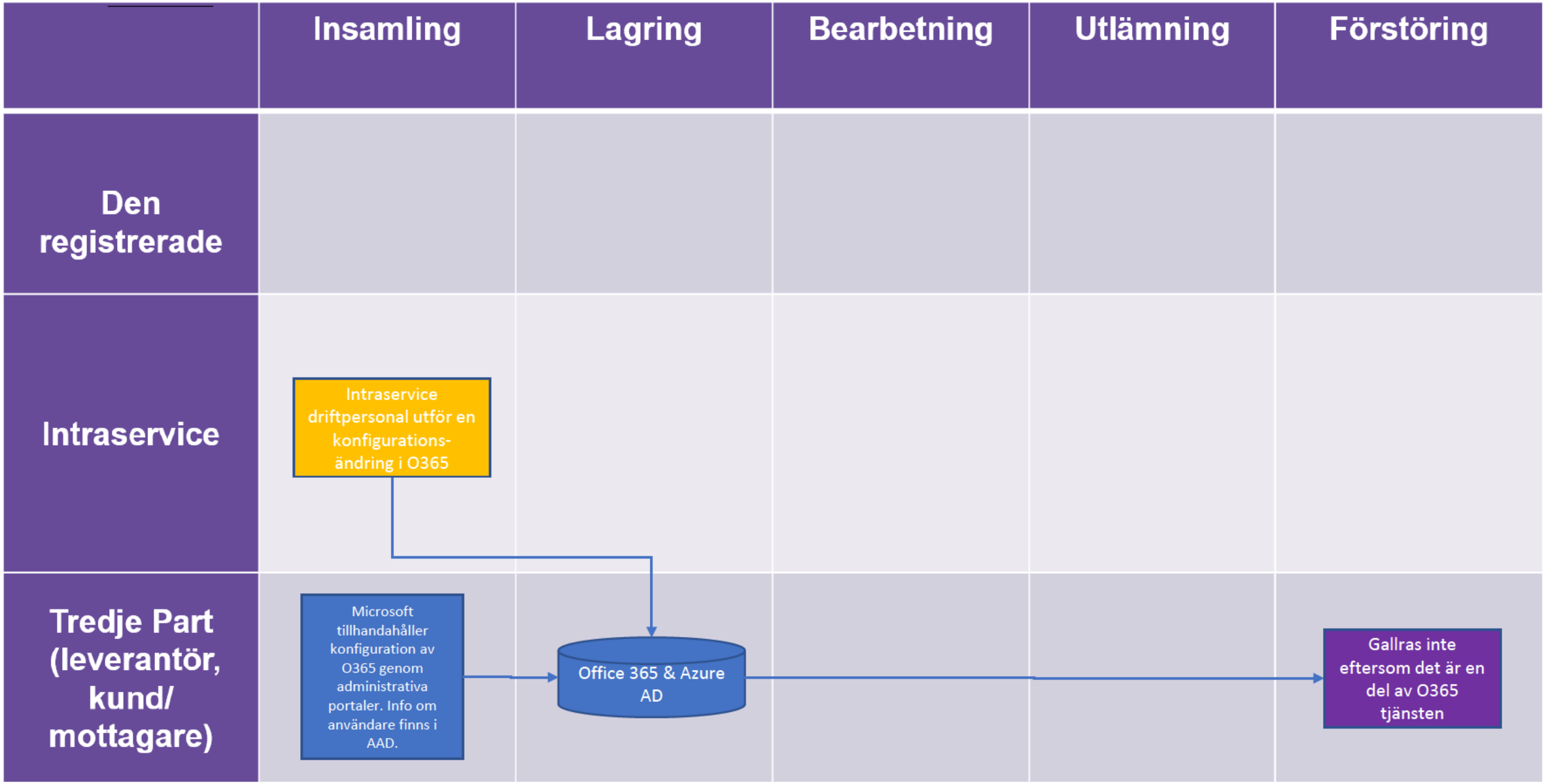
M365/Navet

31- Kontroll av behörighet

	Insamling	Lagring	Bearbetning	Utlämning	Förstöring
Den registrerade					
Intraservice				Loggar används endast i felsökningssyfte	
Tredje Part (leverantör, kund/ mottagare)	Azure AD håller koll på vad alla konton har rättigheter till. En ny rättighet registreras	Azure AD	Alla förfrågningar om access går till Azure AD och tillträden delas ut därifrån		Loggarna rensas efter 30 dagar

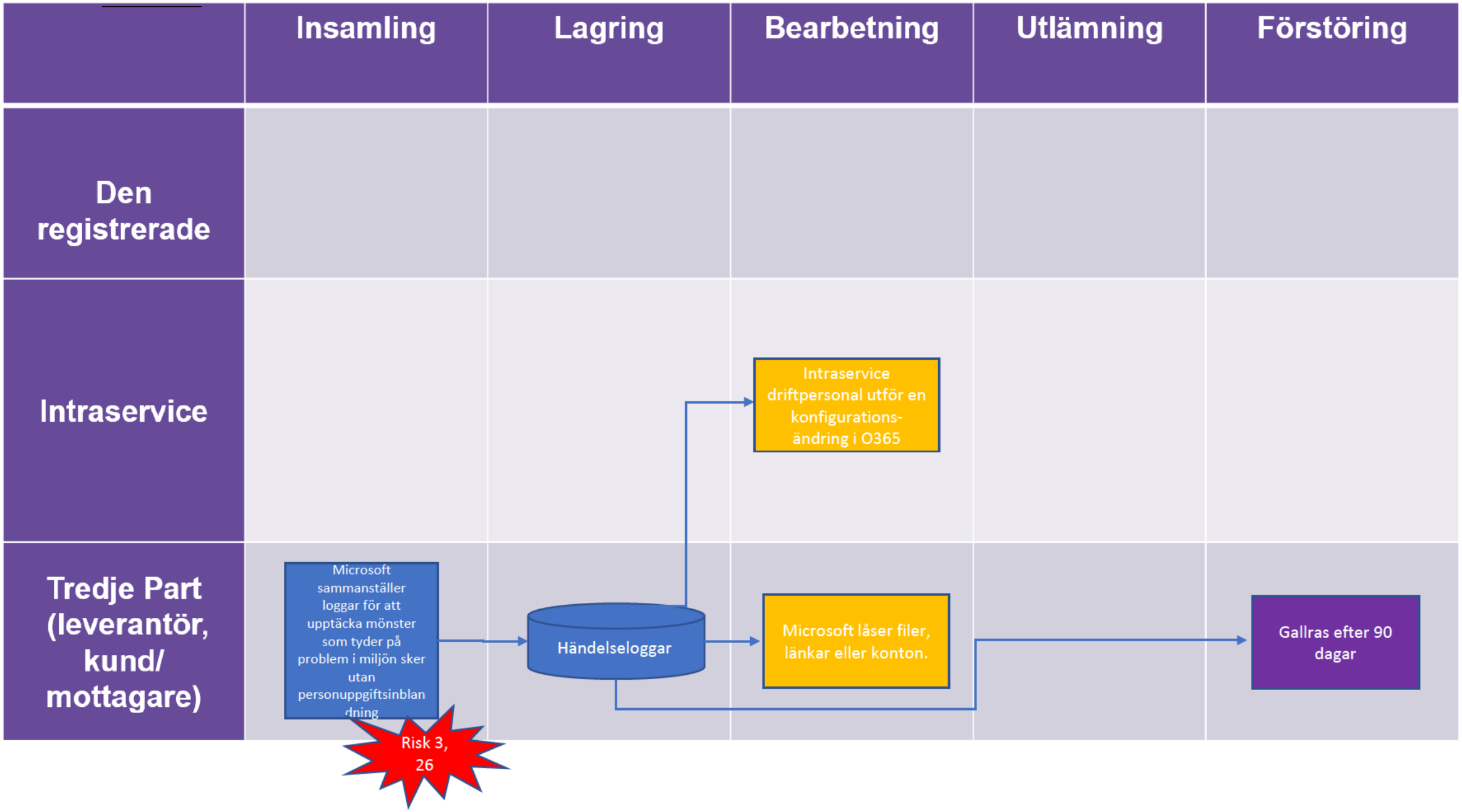
M365/Navet

32- Administrativa portaler

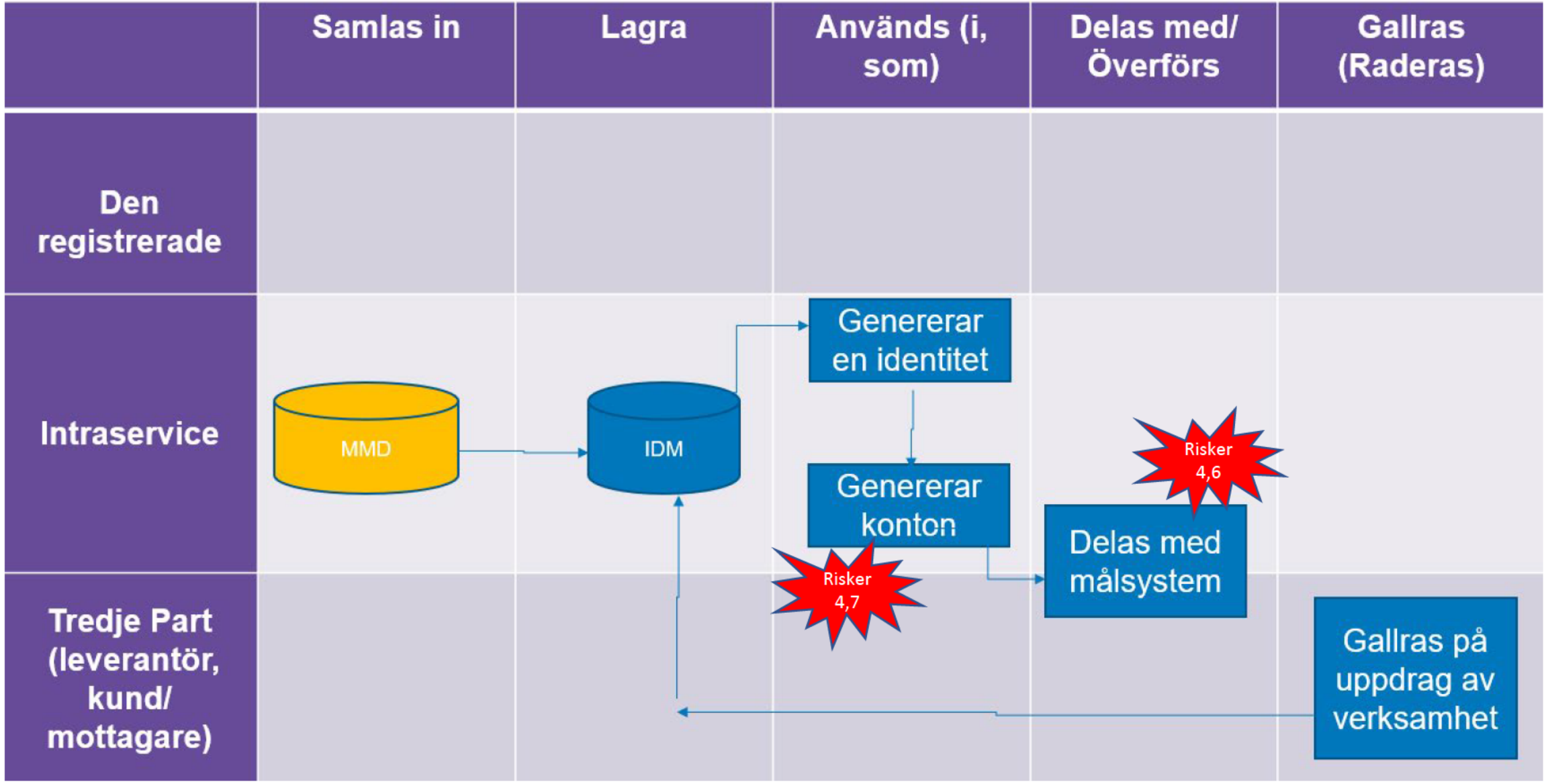


M365/Navet

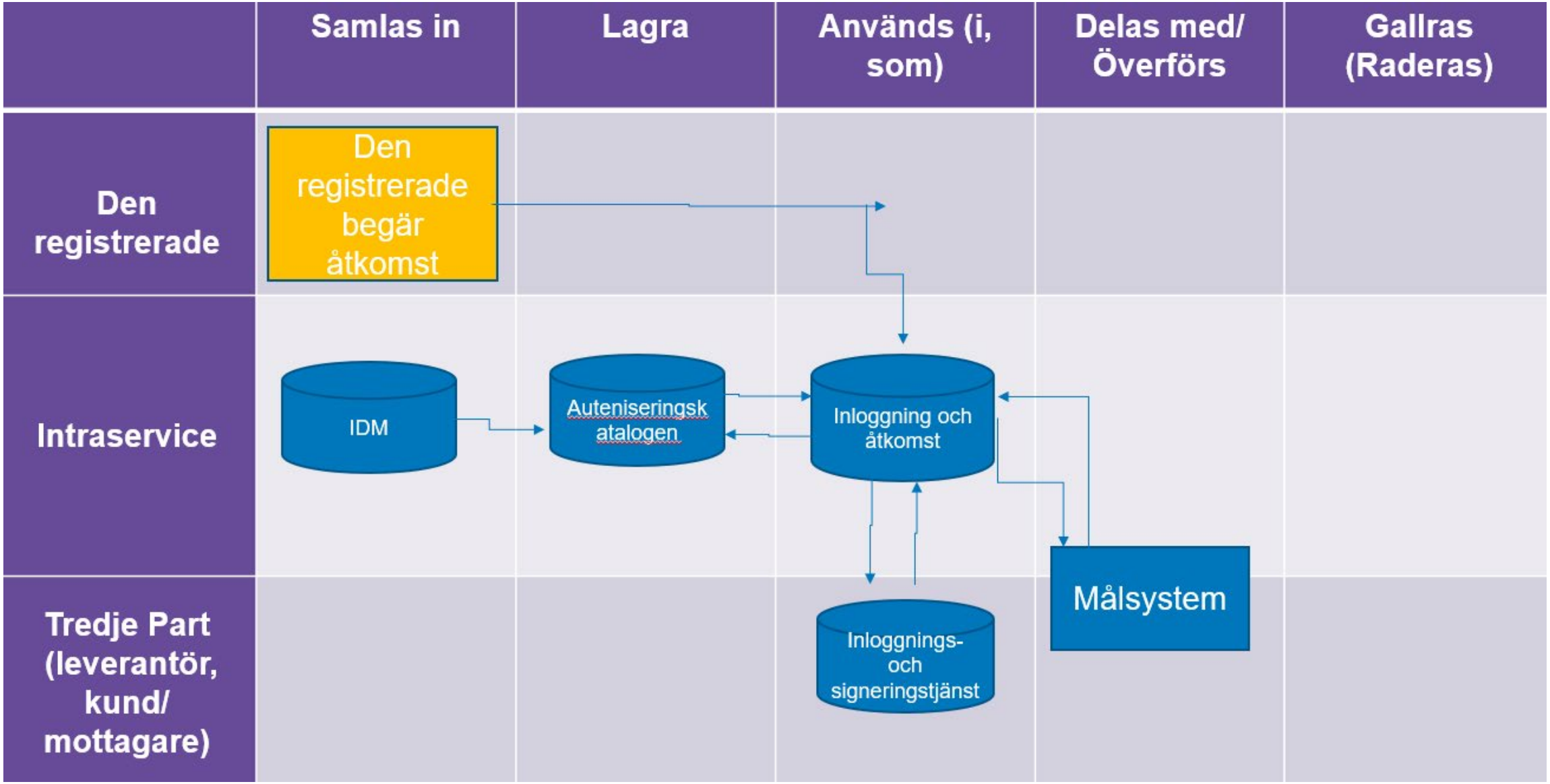
33- Systemkontroller



34. Personuppgiftsflöde Identitet

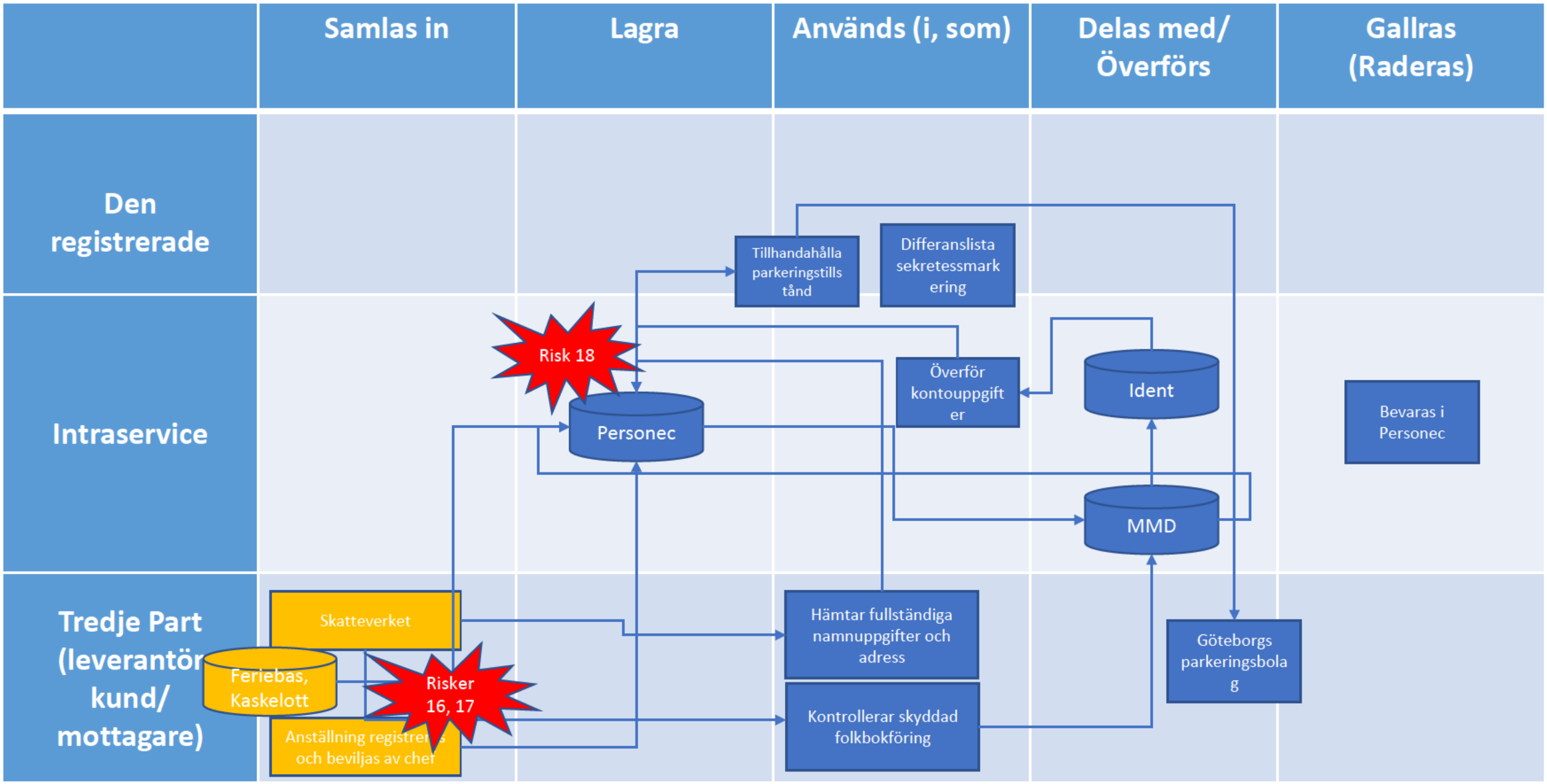


35. Personuppgiftsflöde åtkomst



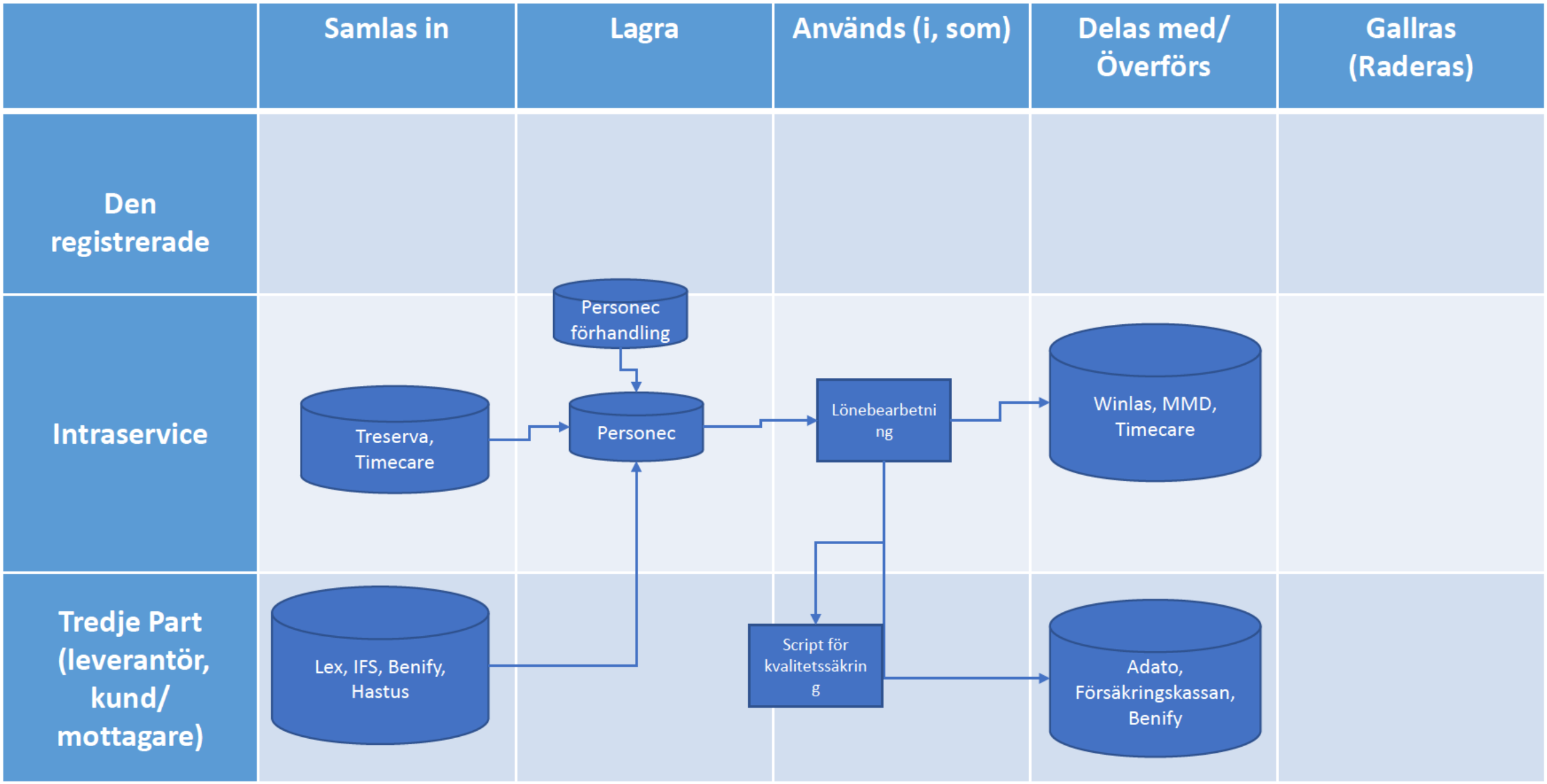
HR & Lön

36. Aktivitet #01 Skapa anställning

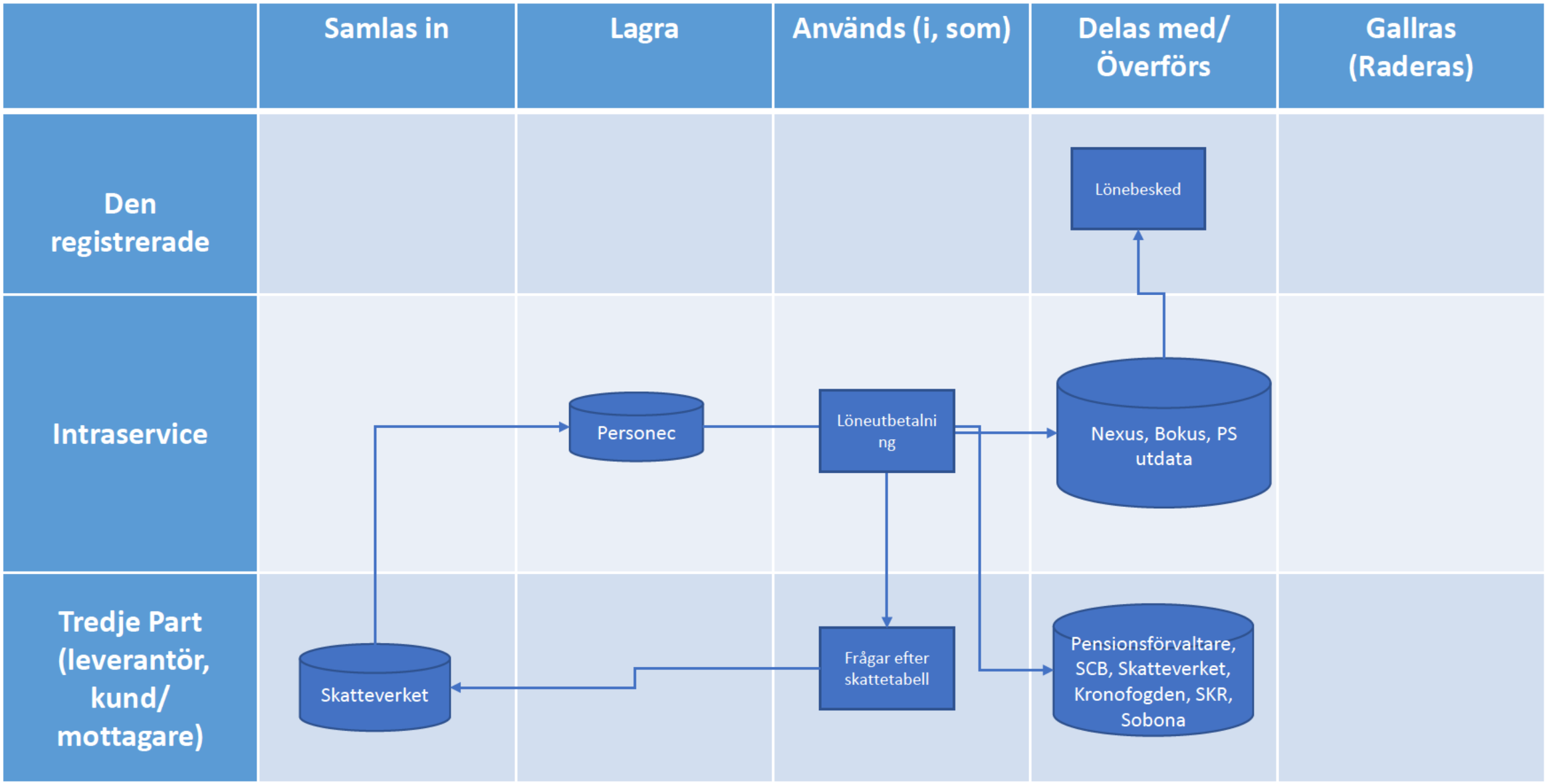


HR & Lön

37. Aktivitet #02 Lönebearbetning



38. Aktivitet #03 Verkställande av lön



Kvalitetssäkrad information

39. Personuppgiftsflöde MMD (Navet)

	Samlas in	Lagra	Används (i, som)	Delas med/ Överförs	Gallras (Raderas)
Den registrerade					
Intraservice	Personec ISIM KU-synk Serviceportalen CMG	MMD	Skapar en person från ett flertal källor	Risk 29 Målsystem	
Tredje Part (leverantör, kund/ mottagare)	[redacted]				

Göteborgs Stad

Digitala navet

Tjänstespecifikation gällande teknisk säkerhet och dataskydd

2023-05-19

Tjänsteägare: NN

Versionshantering av detta dokument

Datum	Version	Beskrivning	Ändrat av
2022-11-09	0.1	Skapat ett första utkast	Marcus Broman
2022-12-19	0.2	Skapat ett andra utkast där funktioner är separerade från tjänsten	Fredrik Andersson
2023-04-04	0.3	Utförligare beskrivning under funktioner inom tjänsten	Andreas Öien Jons
2023-05-18	0.4	Korrigerat innehåll för samstämmighet med andra dokument	Marcus Broman

Innehåll

1 Dokumentets syfte ... 4
1.1 Allmänt ... 4
1.2 Ägarskap och dokumenthantering ... 4
2 Inledning ... 5
2.1 Övergripande beskrivning av tjänsten ... 5
2.2 Funktioner inom tjänsten ... 6
2.2.1 Sidor i ämnesstrukturen ... 7
2.2.2 Inlägg i kommunikativa kanaler ... 9
2.2.3 Redaktörsingången ... 11
2.2.4 Personuppgiftshantering ... 17
2.3 Intraservice roll för personuppgiftshantering ... 21
2.3.1 Intraservice användning av personuppgifter ... 21
2.4 Tekniska säkerhetsåtgärder som är vidtagna inom tjänsten ... 23
2.5 Organisatoriska säkerhetsåtgärder ... 23
2.6 Intraservice användning av personuppgifter ... 23
2.7 Biträden/underbiträden ... 23
2.7.1 Underbiträdes användning av personuppgifter ... 23
3 Bilagor ... 23
4 Referenser ... 24

1 Dokumentets syfte

En *Tjänstespecifikation* dokumenterar säkerhets och dataskyddsaspekter. Specifikationen anger övergripande olika underliggande tekniska funktioner som ingår i tjänsten

Två nivåer av dokumentation:

1. Tjänstespecifikation (kopplad till Intraservice tjänst - övergripande)
2. Funktionsbeskrivning (underliggande funktion som kan ingå i flera tjänster)

*Tjänstespecifikation*en kan återanvändas för olika syften och för att förklara aspekter på säkerhet och dataskydd i en tjänst som Intraservice tillhandahåller.

1.1 Allmänt

Detta dokument är skapat med utgångspunkt att stödja stadens bolag och förvaltningar i olika bedömningar, ställningstaganden och utredningar gällande informationssäkerhet och dataskydd. Dokumentet uppdateras löpande.

1.2 Ägarskap och dokumenthantering

TBD

2 Inledning

2.1 Övergripande beskrivning av tjänsten

Digitala navet är en teknisk lösning som ska stödja medarbetare i Göteborgs Stad i sitt arbete. Via Digitala navet får medarbetare tillgång till information som möjliggör samarbete, kommunikation och produktivitet anpassat för roll och organisation.

Digitala navet finns tillgängligt på olika enheter såsom mobiltelefon, surfplatta och dator.

Tjänsteerbjudandet innebär utveckling, leverans, uppföljning och förvaltning av de IT-stöd som möjliggör leverans av Digitala navet.
I erbjudandet ingår en huvudredaktör, stöd och utbildning för redaktörer och support vid behov.

För att fullt ut nyttja tjänsteerbjudandet krävs ett staden-konto och Microsoft 365-tjänst som tillhandahåller den grundläggande tekniska plattformen som möjliggör Digitala navet.

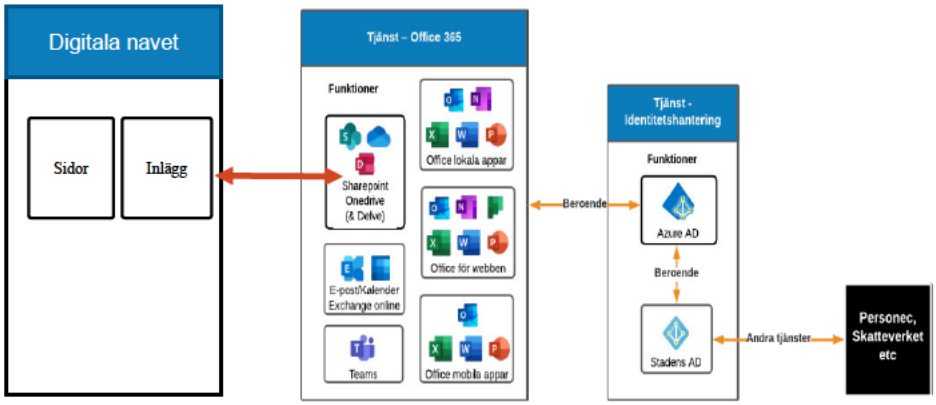
För den som ska fungera som redaktör är det obligatoriskt att gå redaktörsutbildningen och därigenom få access som redaktör.
För att nå Digitala navet om man inte har tillgång till Intraservice gemensamma Microsoft 365-tjänst kan man få så kallad gästkontoaccess. Tjänsten begränsas då till information gemensam för Göteborgs stad och anpassas inte efter roll / organisation.

För kompletterande beskrivning av Microsoft 365, se *Tjänstespecifikation O365*.

2.2 Funktioner inom tjänsten

Redaktörer som uppdaterar innehållsdata ges behörighet till det Digitala navet efter att man genomgått en utbildning med ett teoretiskt och ett praktiskt avsnitt. Som redaktör läggs personens konto till i en eller flera grupper i Azure AD beroende på vilken behörighet som man tilldelas. Den som är lokalt ansvarig för det digitala navet (intranätsansvarig) avgör vilken behörighet redaktören behöver för att kunna utföra det sitt arbete.

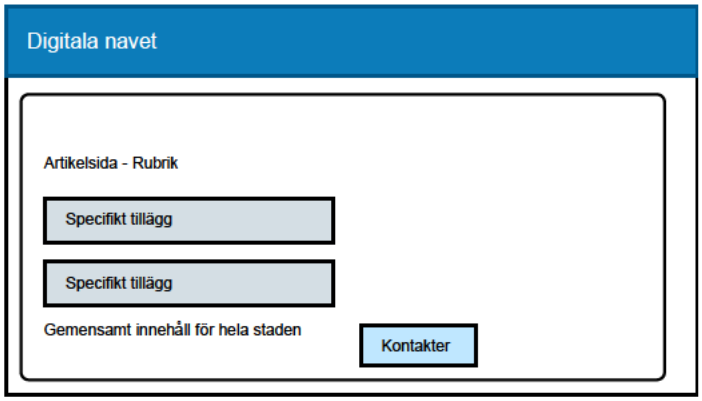
Som redaktör kan man skapa innehåll på sidor i ämnesstrukturen och inlägg i nyhetskanaler som riktar sig till medarbetare inom olika verksamhetsområden och med olika roller. Sharepoint loggar alla sidor/inlägg som skapas och vem som skapat dem. Data baseras på den typen av data som syns i tabellen från Azure AD, se *Funktions-beskrivning - Azure AD*. Innehållet är versionshanterat. Det går därmed att följa upp vem som skapar och eller ändrat information i det Digitala navet.



Funktion	Beskrivning
Artikelsida i ämnesstrukturen	Informationssida med gemensamt innehåll till hela staden
Specifikt tillägg till artikelsida	Förvaltnings- eller bolagsspecifikt tillägg till en artikelsida
Inlägg i kommunikativ kanal	Nyheter samt inlägg i de andra kommun kativa kanalerna: Nytt från, Vi delar med oss och Kommande händelser

Tabell 2-1: Lista över funktioner

2.2.1 Sidor i ämnesstrukturen



Artikelsidor i ämnesstrukturen innehåller gemensam information som är till för alla medarbetare i Göteborgs stad, dessa sidor skapas och publiceras av den förvaltning eller bolag som har till uppgift att tillhandahålla tjänster och/eller styrning inom det sakområde som innehållet avser.

Specifika tillägg till artikelsidor är en annan typ av sida som visas upp tillsammans med artikelsidan. Redaktörer på alla förvaltningar och bolag har möjlighet att skapa specifika tillägg för sin egen verksamhet till alla gemensamma artikelsidor. Dessa tillägg innehåller information som relaterar till artikelsidan, men är anpassad för den förvaltning eller det bolag som ansvarar för tillägget.

Alla sidor i ämnesstrukturen har en namngiven publiceringsansvarig och en namngiven innehållsansvarig, dessa anges av redaktören som skapar sidan. Den publiceringsansvarige ansvarar för att rätta fel eller göra uppdateringar av innehållet på sidan. Den innehållsansvarige ansvarar för att sidans sakinnehåll är korrekt. Publicerings- och innehållsansvarig ansvarar för livscykelhantering av publicerat innehåll. Innehåll kan visas för alla medarbetare i staden eller för en eller flera förvaltningar/bolag. Publiceringsansvarig, innehållsansvarig, information om vem som skapat och senast ändrat sidan sparas i sidans sidinformation (metadata).

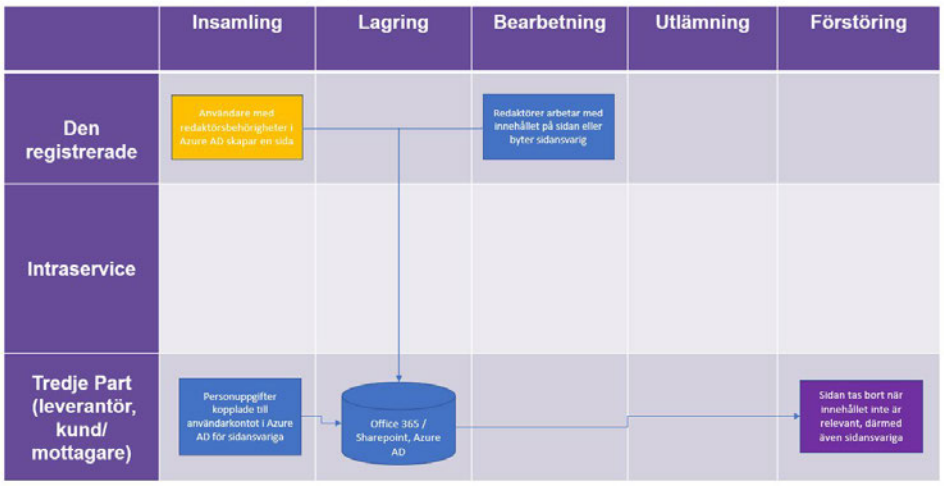
Det finns även möjlighet att inkludera kontakter relaterat till innehållet, både på artikelsidor och specifika tillägg. Kontakter kan exempelvis vara handläggare eller administratörer och behöver inte vara de som ansvarar för sidan. Kontakter kan fyllas i manuellt av redaktören eller via Sharepoints personväljare som hämtar uppgifterna om kontakpersonen från Azure AD via Delve och visar upp informationen i form av ett kontaktkort på sidan.

2.2.1.1 Aktivitet artikelsida

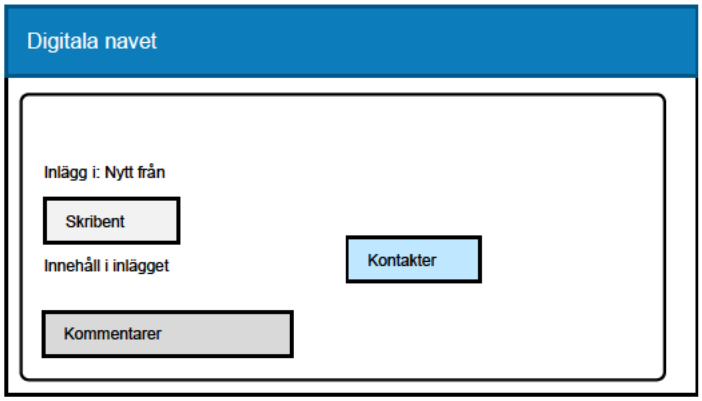
Varje verksamhet som producerar innehåll i artikelsida ansvarar för aktiviteten nedan, vilket är en personuppgiftsbehandling som förvaltning utför med enligt egna mål och medel.

- Insamling
  - När en redaktör skapar en sida så sparas namn på redaktören som skapar sidan, innehållsansvarig och publiceringsansvarig i sidinformationen. Kontakter sparas som innehåll på sidan.
- Lagring
  - Uppgifterna i kontaktkorten hämtas från Azure AD och innehållet samt sidinformationen lagras i Sharepoint.
- Bearbetning
  - Uppgifterna uppdateras när en redaktör gör en ändring på sidan eller byter sidansvarig.
- Utlämning
  - Uppgifterna i sidinformationen är bara synliga för redaktörer i Digitala navet, alla användare kan se kontaktkort på sidan.
- Förstöring
  - När sidan tas bort tas även sidinformationen bort.

Artikelsidor och specifika tillägg



2.2.2 Inlägg i kommunikativa kanaler



Samlingsnamnet för de olika nyhetsflödena i Digitala navet är kommunikativa kanaler. Inlägg i kommunikativa kanaler är en annan typ av sida än artikelsidor och specifika tillägg, med anpassat utseende och funktionalitet. Varje inlägg har en namngiven publiceringsansvarig och en namngiven innehållsansvarig. Den publiceringsansvarige ansvarar för att rätta fel eller göra uppdateringar av innehållet på sidan. Den innehållsansvarige ansvarar för att sidans sakinnehåll är korrekt. Publicerings- och innehållsansvarig ansvarar för livscykelhantering av publicerat innehåll. För varje inlägg skapas en mapp om filer laddas upp till inlägget, till filerna registreras namn på redaktören som laddat upp filen och vem som senast ändrat den. Filer gallras löpande enligt dokumenthanteringsplanen eller när inlägget tas bort.

Inläggen kan vara riktade till alla medarbetare i Göteborgs Stad eller till medarbetare på en viss förvaltning/bolag eller med en viss roll. Det är förvaltningen eller bolaget som redaktören som skapar inlägg i kommunikativa kanaler arbetar på som ansvarar för innehållet i inlägget.

Kontakter kan inkluderas i inläggen och behöver inte vara de som ansvarar för inlägget. Kontakter kan fyllas i manuellt av redaktören eller via Sharepoints personväljare som hämtar uppgifterna om kontakpersonen från Azure AD via Delve.

Nytt från-inlägg är skrivna ur perspektivet av en skribent och riktas från skribenten till respektive förvaltning eller bolag som skribenten arbetar på. Skribentens kontaktkort inklusive titel visas överst i dessa inlägg, och behöver inte vara samma person som publicerar eller ansvarar för innehållet i inlägget. Information om skribenten hämtas automatiskt med Sharepoints personväljare från Azure AD via Delve, skribentens titel fylls i manuellt.

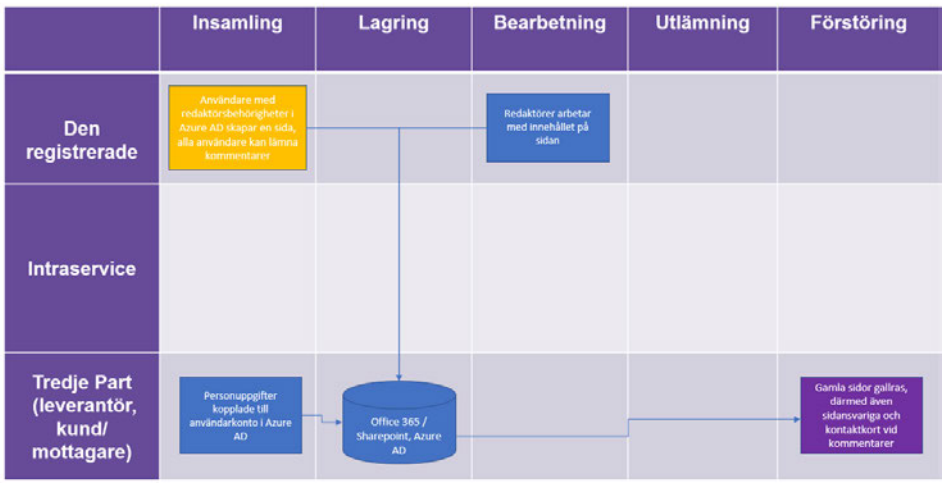
Kommentarsfält kan användas på inlägg i kommunikativa kanaler. I kommentarsfältet kan alla medarbetare lämna kommentarer på inlägget,

och i anslutning till en kommentar visas ett kontaktkort med information om medarbetaren som hämtas automatiskt från Azure AD via Delve.

2.2.2.1 Aktivitet Inlägg i kommunikativa kanaler

- Insamling
  - När en redaktör skapar en sida så sparas namn på redaktören som skapar sidan, innehållsansvarig och publiceringsansvarig i sidinformationen. Kontakter och kontaktkort för användare som lämnar kommentarer sparas som innehåll på sidan.
- Lagring
  - Uppgifterna i kontaktkorten hämtas från Azure AD och innehållet samt sidinformationen lagras i Sharepoint.
- Bearbetning
  - Uppgifterna uppdateras när en redaktör arbetar med innehållet på sidan eller byter sidansvarig.
- Utlämning
  - Uppgifterna i sidinformationen är bara synliga för redaktörer i Digitala navet, alla användare kan se kontaktkort och kommentarer på sidan.
- Förstöring
  - Gamla sidor gallras enligt varje organisations dokumenthanteringsplan efter eventuell arkivering, när sidan tas bort tas även sidinformationen och kommentarer bort.

Inlägg i kommunikativa kanaler



2.2.3 Redaktörsingången

I det Digitala navet finns en webbplats som kallas Redaktörsingången, den är endast tillgänglig för redaktörer och innehåller funktioner, stöd och information till redaktörer. I redaktörsingången finns ett antal listor som sammanställer information om sidor, behörigheter och funktionalitet i Digitala navet, de personuppgifter som behandlas i varje lista anges i följande underkapitel.

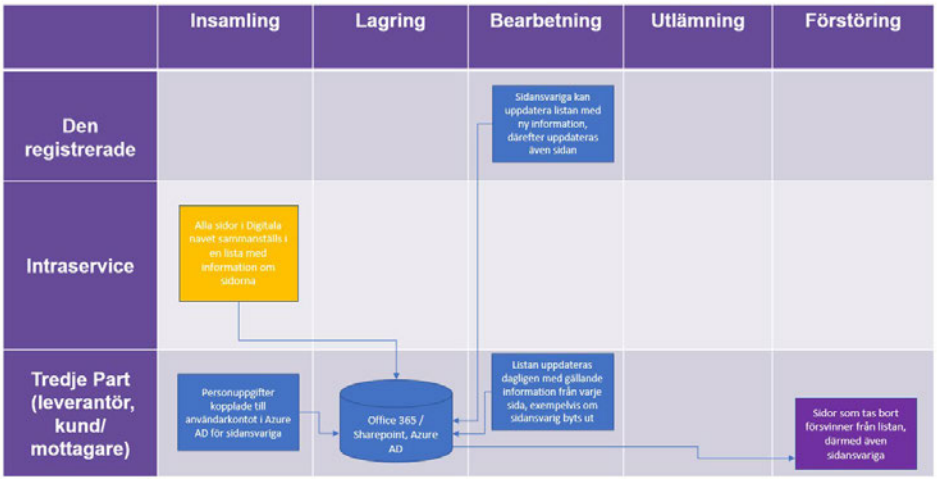
Dessa listor är till för att ge redaktörer en god möjlighet att kunna organisera sitt arbete och en tydlig överblick över varje redaktörs ansvarsområde. Det ska även gå att sortera fram innehåll baserat på vilken förvaltning som ansvarar för innehållet och vara enkelt att ta reda på vem man ska kontakta vid frågor om innehållet.

2.2.3.1 Lista över alla sidor i Digitala Navet

Listar alla artikelsidor, specifika tillägg och inlägg i kommunikativa kanaler med information om varje sida samt ansvariga personer.

- Insamling
  - Alla sidor i Digitala navet sammanställs i en lista med information om sidorna, bland annat:
    - Innehållsansvarig
    - Publiceringsansvarig
    - Redaktör som senast ändrat sidan
    - Redaktör som skapat sidan
- Lagring
  - Uppgifterna i kontaktkorten hämtas från Azure AD och listan lagras i Sharepoint.
- Bearbetning
  - Listan uppdateras automatiskt dagligen, baserat på gällande sidinformation. Via listan kan fälten innehålls- och publiceringsansvarig även uppdateras manuellt av sidansvariga vilket också uppdaterar sidinformationen på sidan.
- Utlämning
  - Uppgifterna är bara synliga för redaktörer i Digitala navet.
- Förstöring
  - Sidan och tillhörande sidinformation tas bort från listan när sidan tas bort.

Lista över alla sidor i Digitala navet

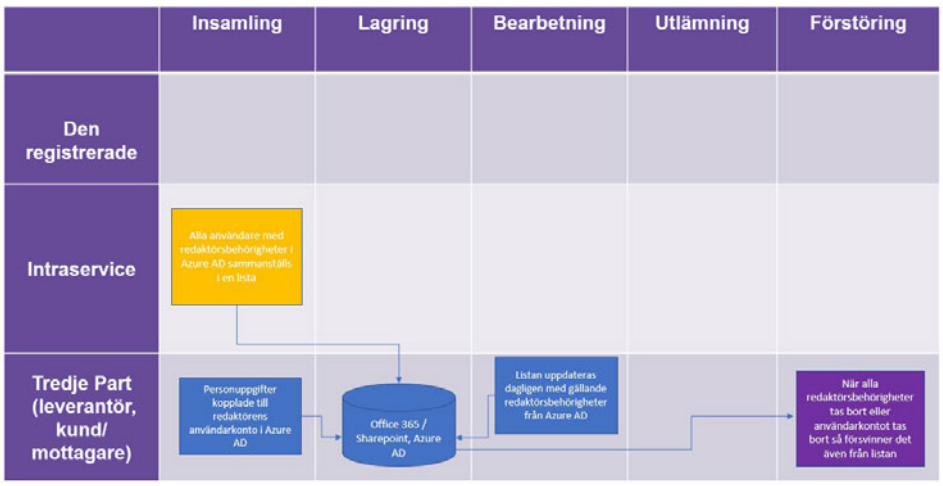


2.2.3.2 Lista över redaktörsbehörigheter

Listan sammanställer alla redaktörer i Digitala navet och deras behörigheter utifrån organisationstillhörighet. Denna lista kan exempelvis användas av redaktörer för att hitta rätt bland andra redaktörer att fråga om innehåll på sidor eller vart i ämnesstrukturen nytt innehåll ska skapas.

- Insamling
  - Alla redaktörer i Digitala navet sammanställs i en lista där deras redaktörsbehörigheter visas, följande information sparas i listan:
    - Namn på redaktören.
    - Förvaltning/bolag som redaktören tillhör.
    - Behörighetsgrupper i Azure AD som redaktören tillhör.
- Lagring
  - Listan lagras i Sharepoint.
- Bearbetning
  - Listan uppdateras automatiskt varje dag med gällande grupptillhörighet i Azure AD för varje redaktör.
- Utlämning
  - Uppgifterna är bara synliga för redaktörer i Digitala navet.
- Förstöring
  - När en redaktörs användarkonto tas bort eller alla redaktörsbehörigheter tas bort så tas även användaren bort från listan.

Lista över redaktörsbehörigheter

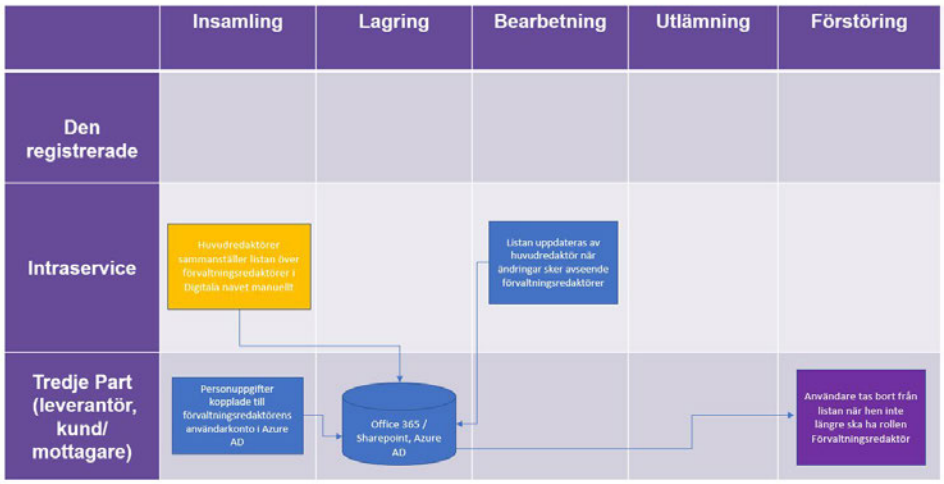


2.2.3.3 Lista över förvaltningsredaktörer

Förvaltningsredaktörer, alltså de som är lokalt ansvariga för Digitala navet vid varje förvaltning eller bolag sammanställs i en lista för att andra redaktörer enkelt kunna hitta rätt person i vissa frågor, exempelvis när man behöver andra redaktörsbehörigheter. Denna lista uppdateras manuellt av det centrala förvaltningsteamet.

- Insamling
  - Huvudredaktör i det centrala förvaltningsteamet lägger till namnet på varje förvaltningsredaktör genom att använda Sharepoints personväljare som hämtar informationen från Azure AD. Följande uppgifter sparas i listan:
    - Namn på förvaltningsredaktör.
    - Organisation i Digitala navet som förvaltningsredaktören ansvarar för.
- Lagring
  - Listan lagras i Sharepoint.
- Bearbetning
  - Huvudredaktör kan uppdatera listan med nya namn eller organisatoriska ansvarsområden.
- Utlämning
  - Uppgifterna är bara synliga för redaktörer i Digitala navet.
- Förstöring
  - Förvaltningsredaktören tas bort från listan ifall hen inte längre ska ha rollen.

Lista över förvaltningsredaktörer

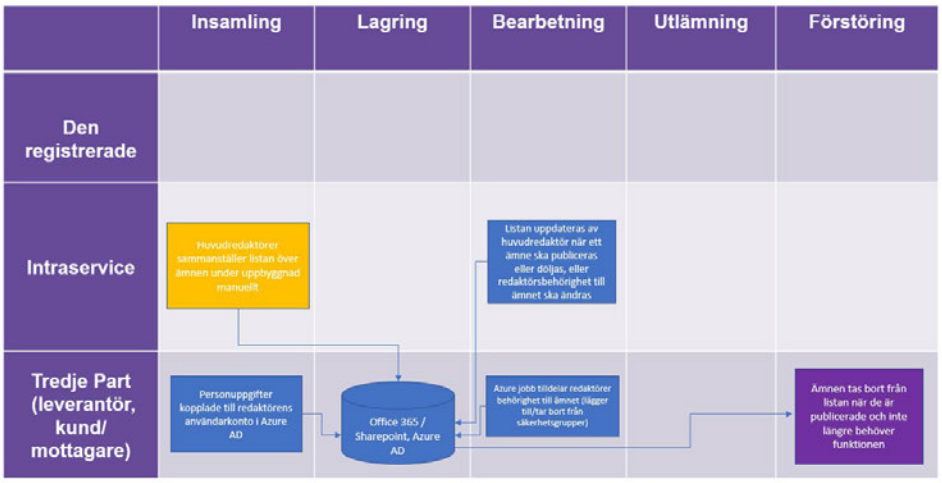


2.2.3.4 Lista för ämnen under uppbyggnad

Listar ämnen i Digitala navet som är dolda för vanliga användare, exempelvis för att sidorna under ämnet är under uppbyggnad. Listan uppdateras manuellt av det centrala förvaltningsteamet.

- Insamling
  - Huvudredaktör i det centrala förvaltningsteamet lägger till namnet på varje förvaltningsredaktör genom att använda Sharepoints personväljare som hämtar informationen från Azure AD. Följande uppgifter sparas i listan:
    - Ämne / Rubrik.
    - Namn på redaktörer (eller säkerhetsgrupp i Azure AD) med behörighet att se och redigera ämnen under uppbyggnad.
    - Säkerhetsgrupp för behörighet till ämnet.
- Lagring
  - Listan lagras i Sharepoint.
- Bearbetning
  - Listan uppdateras manuellt av huvudredaktör när ett ämne ska publiceras eller placeras under uppbyggnad. Listan uppdateras även när en redaktör ska tilldelas behörighet till ämnet eller när behörigheten ska tas bort.
- Utlämning
  - Uppgifterna är bara synliga för redaktörer i Digitala navet.
- Förstöring
  - Redaktörer som inte längre ska ha tillgång till ämnen under uppbyggnad tas bort från listan. Ett ämne tas bort från listan när behovet att kunna dölja ämnet inte längre finns, därmed även de redaktörer som låg i listan kopplat till ämnet.

Lista för ämnen under uppbyggnad

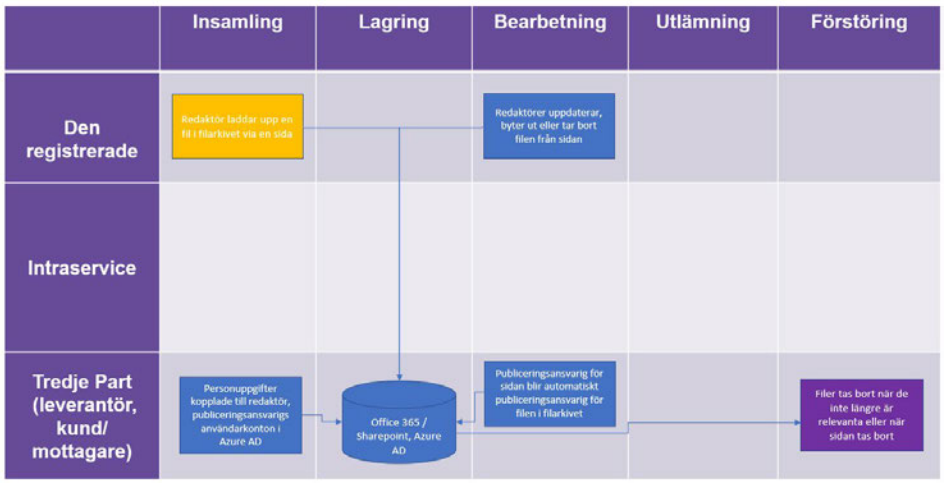


2.2.3.5 Filarkivet i Digitala navet

Filarkivet är ett dokumentbibliotek i Sharepoint för filer som laddas upp till Digitala navet. En fil i filarkivet är alltid kopplad till en sida i ämnesstrukturen och alla användare har läsbehörighet till filerna. I bilagan *Funktionsbeskrivning – Sharepoint och Onedrive* beskrivs filhanteringen i Sharepoint mer utförligt.

- Insamling
  - Redaktör laddar upp en fil till en sida i ämnesstrukturen.
    Följande uppgifter sparas i dokumentbiblioteket:
    - Namn på publiceringsansvarig för filen, hämtas automatiskt från sidinformationen då publiceringsansvarig för sidan och filen är samma.
    - Skapad av (redaktör)
    - Ändrad av (redaktör)
- Lagring
  - Filerna sparas i ett dokumentbibliotek i Sharepoint, informationen i kontaktkort hämtas från Azure AD.
- Bearbetning
  - Redaktörer kan uppdatera, byta ut eller ta bort filer från sidan. Om publiceringsansvarig för sidan byts ut uppdateras även publiceringsansvarig på alla filer som hör till sidan.
- Utlämning
  - Filer är synliga för alla användare i Digitala navet.
- Förstöring
  - Filer tas bort av redaktören när de inte längre är relevanta, de tas även bort från filarkivet ifall sidan tas bort.

Filer i Digitala navets filarkiv



2.2.4 Personuppgiftshantering

Digitala navet bygger på plattformen Sharepoint Online som är en del av M365-plattformen inom Göteborgs Stad. När en användare loggar på M365 med sitt staden-konto får användaren även tillgång till det Digitala navet. Varje användare tilldelas ett unikt ID av M365 (s.k. GUID = Globally Unique Identifier) som består av bokstäver och siffror. När användaren navigerar till Digitala navet så sparas användarens GUID i en Azure-databas för användarinställningar som tillhör Digitala navet. Tillsammans med användarens GUID sparas även information från MMD-tjänsten så som användarens organisatoriska tillhörighet och huruvida användaren har en chefsroll. Det sparas inga namn i databasen.

Informationen i Digitala navets databas för användarinställningar används för att tillämpa förvalda inställningar för varje användare, dessa kan användaren sedan uppdatera manuellt via sidan för användarinställningar. Användare kan fritt lägga till och ta bort organisationer och roller i sina användarinställningar och databasen uppdateras därefter, dessa inställningar avgör bland annat vilket innehåll som kommer att visas upp för användaren på startsidan.

Användare i Digitala navet har även möjligheten att skapa en personlig lista med styrande dokument som visas på startsidan. Styrande dokuments ID sparas tillsammans med användarinställningarna i Azure-databasen. Användare kan även spara sidor i en lista på sin startsida. Länkar till dessa sidor sparas inte i Digitala navet utan hämtas från Sharepoints standardfunktion ”Sparat till senare”. De Sharepoint-sidor användaren sparat som hör till Digitala navet visas på användarens startsida.

Följande information sparas i Digitala navets Azure-databas:

Typ av data	Beskrivning
Azure AD ID	Användarens unika ID (GUID)
Organisationslista	Lista med ID tillhörande användarens valda organisationer i Digitala navet
Rollista	Lista med ID tillhörande användarens valda roller i Digitala navet
MMD information	OrganisationsID, Organistionskod och eventuellt chefskod
Styrande dokument ID	ID för de styrande dokument som användaren har sparat

2.2.4.1 Listor, bibliotek och sidor

Sharepoint innehåller anpassningsbara sidor och listor där personer kan läggas till i form av namn med bild vilken utvidgas till ett kontaktkort när muspekaren förs över objektet. I dessa fall hämtas information om personen från Azure AD via Delve, nedan listas de olika typerna av information som används i Digitala navet med Azure AD som källa:

Publiceringsansvarig och Innehållsansvarig: sidor taggas med namnet på de personer som ansvarar över sidan. En vanlig användare ser ej dessa namn men har möjlighet att kontakta dessa personer via ett formulär på botten av sidan. När en användare kontaktar en ansvarig skickas ett e-postmeddelande till den ansvarige med informationen som användaren uppgav samt namn på avsändaren. Inga personuppgifter sparas därefter i Digitala navet om kontakten med den ansvarige. Namnen på de ansvariga finns registrerade i sidinformationen som andra redaktörer kan se.

Skapad av: namnet på personen som skapade sidan eller dokumentet.

Senast ändrad av: namnet på personen som senast ändrade sidan eller dokumentet.

Filägare/publiceringansvarig för filen: namnet på personen som ansvarar för en fil i dokumentbiblioteket för Digitala navets filarkiv.

Skribent: namn, bild och titel på personen som är att betrakta som avsändare för inlägg i den kommunikativa kanalen Nytt från.

Kontaktkort: en Sharepoint-standardfunktion som visar kontaktinformation till personer som är relevanta för innehållet på sidan. Kan läggas till på alla sidtyper och återfinns som standard på artikelsidor och specifika tillägg.

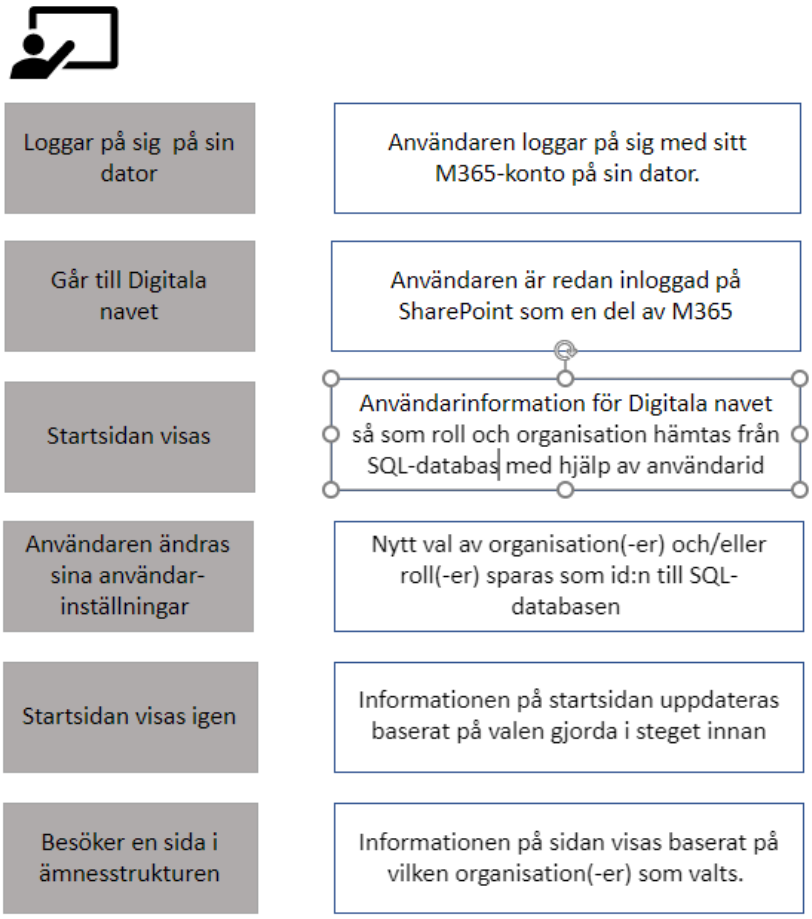
Kommentarer: en sektion i botten på inlägg i kommunikativa kanaler, där vanliga användare kan kommentera inlägget och även tagga andra användare.

Kontaktkort blir tillgängliga genom att föra muspekaren över namnet på en användare som kommenterar eller blir taggad i en kommentar. När en användare blir taggad i ett inlägg så skickas ett e-postmeddelande till användaren med hänvisning till inlägget. Redaktören avgör om kommentarer ska användas på inlägget.

Innehållstyp	Sharepoint metadata / sidinformation					Information från Azure AD via Delve		
	Publiceringsansvarig	Innehållsansvarig	Skapad av	Senast ändrad av	Filägare	Skribent	Kontaktkort	Kommentarer
Artikelsida (sida)	X	X	X	X			X	
Specifikt tillägg (sida)	X	X	X	X			X	
Nyheter (sida)	X	X	X	X			X	X
Nytt från (sida)	X	X	X	X		X	X	X
Kommande händelser (sida)	X	X	X	X			X	X
Vi delar med oss (sida)	X	X	X	X			X	X
Digitala navets filarkiv (dokument)			X	X	X			

2.2.4.2 Personuppgifter kopplat till användare:

Digitala navet bygger på plattformen Sharepoint Online som är en del av M365-plattformen inom Göteborgs Stad. När en användare loggar på sin “staden-dator”, har hen automatisk access till M365 och till det Digitala navet. Informationen som skapas består av unika ID:n (s.k. GUID = Globally Unique Identifier) i form av bokstäver och siffror. Det finns ingen personinformation sparad i Digitala navet. Den information som finns ligger redan i M365-plattformen.



All information som ska publiceras ska förhålla sig till de styrande dokument som gäller för staden (exempelvis Riktlinjer för informationssäkerhet) och behandlas utifrån de krav som ställs.

Anställningsinformation innebär: information om namn och organisatorisk tillhörighet.

Kontaktinformation innebär: En redaktör som publicerar innehåll på digitala navet kan tillföra mer information om den registrerade, så som kontaktinformation. Vanliga kontaktuppgifter är förnamn, efternamn, e-postadress, telefonnummer, roll, funktion, uppdrag. Dessa uppgifter förhåller sig till stadens styrande dokument kopplat till hantering av personuppgifter och generella regler för kommungemensamma tjänster.

Personliga egenskaper, utbildning och arbete: En redaktör som publicerar innehåll i nyhetskanaler kan tillföra mer information om den registrerade, så som uppgifter om utbildning, tidigare arbetsplatser och uppdrag. Detta sker då i samband med intervju och efter avstämning med den registrerade. Även dessa uppgifter förhåller sig till stadens styrande dokument kopplat till hantering av personuppgifter och generella regler för kommungemensamma tjänster.

Tekniskt metadata: I denna kategori finns funktionsdata, diagnos samt gemensamt innehållsdata. Dessa hanteras i riskanalysen för Office 365.

2.3 Intraservice roll för personuppgiftshantering

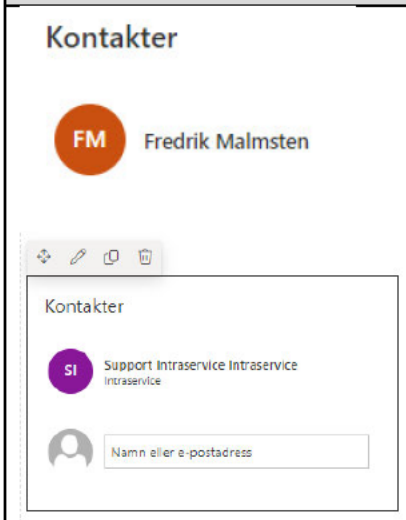
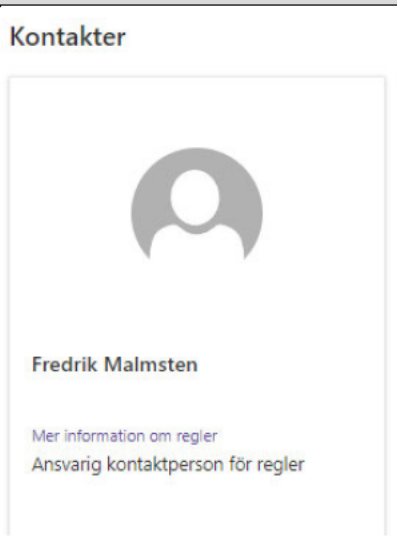
2.3.1 Intraservice användning av personuppgifter

Utveckling och förvaltning av tjänsten sker av Intraservice för stadens användare inom följande områden:

- Funktionalitet levererad genom ny kod
- Funktionalitet levererad genom nya konfigurationer
- Övergripande strukturella förändringar och relaterat gemensamt innehåll
- Utbildning och hantering av behörigheter för redaktörer

Gemensamt innehåll
Tillhandahålls av Intraservice för alla stadens medarbetare.
Personuppgifter behandlas enligt följande:

- Innehållsansvarig och publiceringsansvarig anges för varje sida med gemensamt innehåll. Besökaren på sidan kan inte se namnen men kan kontakta dem via ett formulär som genererar ett mejl till den ansvarige. Som redaktör kan en lista filtreras fram med namn på de ansvariga. Redaktören behöver ha behörighet till de sidor som avses för att kunna filtrera fram namnen.
- i löptext sparsamt efter utbildning och riktlinjer till redaktören.
- i kontaktkort där del av informationen kommer från systemet (Delve) och där ytterligare information kan påföras redaktionellt efter utbildning och riktlinjer till redaktören

Kontaktkort information från Delve	Kontaktkort information från Delve kompletterad med redaktionell informaton
	

Bild, namn och vilken förvaltning hen arbetar på hämtas från Delve. Den undre posten är sökrutan som syns för redaktörer.	Bild, namn och vilken förvaltning hen arbetar på hämtas från Delve. Resten av informationen uppdateras redaktionellt

Intraservice tar även del av gemensamt innehåll som tillhandhålls av andra förvaltningar. Samma behandling av personuppgifter gäller för alla förvaltningar som tillhandahåller gemensamt innehåll.

Lokalt innehåll

- Intraservice tillhandahåller även lokalt innehåll för sina medarbetare. Detta innehåll presenteras tillsammans med det gemensamma innehållet på samma sida för samma ämne. En sida som visas för en medarbetare kan således bestå av gemensamt innehåll och när det är relevant även en del lokalt innehåll. För det lokala innehållet gäller samma personuppgiftsbehandling som för det gemensamma dvs. innehållsansvarig och publiceringsansvarig anges för varje lokalt tillägg, personuppgiftsbehandling i löptext sparsamt efter utbildning och riktlinjer till redaktören och i kontaktkort där del av informationen kommer från systemet (Delve) och där ytterligare information kan påföras redaktionellt efter utbildning och riktlinjer till redaktören.

2.4 Tekniska säkerhetsåtgärder som är vidtagna inom tjänsten

Digitala navet har behörighetshantering som bygger på redaktörsgrupper med tillgång att skapa innehåll inom de olika områdena på digitala navet. För skyddsåtgärder kopplat till Microsoft 365 se *tjänstespecifikation O365* samt funktionsbeskrivningar för underliggande funktioner.

2.5 Administrativa säkerhetsåtgärder

Administrativa åtgärder för navet finns i form av redaktörsutbildning som alla användare måste genomgå innan de får behörighet att skapa innehåll i digitala navet.

För skyddsåtgärder kopplat till Microsoft 365 se *tjänstespecifikation O365* samt funktionsbeskrivningar för underliggande funktioner.

2.6 Intraservice användning av personuppgifter

TBD

2.7 Biträden/underbiträden

Underbiträde	
Hänvisning till O365	För digitala navet finns inga underbiträden, utöver samma som för O365. För de underliggande funktioner som digitala navet baseras på, se de enskilda tjänstespecifikationerna

Tabell 3-2: Lista över underbiträden

2.7.1 Underbiträdes användning av personuppgifter

3 Bilagor

Dokumentnamn	Version	Beskrivning
Funktionsbeskrivning - Sharepoint, Onedrive och Delve	0.1	En *funktionsbeskrivning* som dokumenterar underliggande säkerhets och dataskyddsaspekter specifika för funktionen *Sharepoint, OneDrive och Delve.*
Funktionsbeskrivning – Azure AD	0.1	En *funktionsbeskrivning* som dokumenterar underliggande säkerhets och dataskyddsaspekter specifika för funktionen Azure AD
Tjänstespecifikation - O365	0	En tjänstespecifikation som dokumenterar tjänsten Microsoft 365 och dess koppling till funktionsbeskrivningar.

Tabell 5-1: Lista över bilagor

4 Referenser

Göteborgs kommunfullmäktige (2019). "Riktlinjer för styrning av kommungemensamma interna tjänster." Version: 8, Gällande from 2019-10-31. https://intranat.goteborg.se/wps/portal/int?uri=gbglnk:Intranat.styrandedokument&dominoURL=https://www5.goteborg.se/prod/Stadsledningskontoret/LIS/Verksamhetshandbok/Forfattn nsf/0/DC85A7D50DEB1DDAC12580730028A637?OpenDocument

Göteborgs Stad (2017). "IT-kontroller." Version: 1.6 Gällande from 2017-05-26. https://intranat.goteborg.se/wps/wcm/connect/9bd23df5-cdf2-42d5-b7f0-65ae99e6b018/IT-kontroller_rad_1.6.pdf?MOD=AJPERES

Göteborgs Stad (2017). "Säkerhet i molntjänster " Version: 1.5 Gällande from 2017-02-13. https://intranat.goteborg.se/wps/wcm/connect/d0916c6f-a8d5-4f9c-8495-262ce3d7e30f/sakerhet_molntjanster_rad_1.5.pdf?MOD=AJPERES

Göteborgs Stads kommunstyrelse (2021). "Göteborgs Stads generella regler för kommungemensamma interna tjänster " Version: 6, Gällande from 2021-04-21. https://intranat.goteborg.se/wps/portal/int?uri=gbglnk:Intranat.styrandedokument&dominoURL=https://www5.goteborg.se/prod/Stadsledningskontoret/LIS/Verksamhetshandbok/Forfattn nsf/0/DC85A7D50DEB1DDAC12580730028A637?OpenDocument

Microsoft (2022). "Microsoft Products and Services Data Protection Addendum (DPA) September (English) " https://www microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA?year=2022

Göteborgs Stad

Microsoft Office 365

Tjänstespecifikation gällande säkerhet och dataskydd

2023-05-19

Tjänsteägare: <Namn>

Versionshantering av detta dokument

Datum	Version	Beskrivning	Ändrat av
2023-03-20	0.1	Skapat ett första utkast	Mikael Schou Maegaard, Robert Hansson
2023-05-18	0.4	Korrigerat innehåll för samstämmighet med andra dokument	Marcus Broman

Innehåll

1 Dokumentets syfte ... 4
1.1 Allmänt ... 4
1.2 Ägarskap och dokumenthantering ... 4
2 Inledning ... 5
2.1 Övergripande beskrivning av tjänsten ... 5
2.1.1 Behörigheter inom tjänsten ... 6
2.2 Funktioner inom tjänsten ... 6
2.3 Personuppgiftsaktiviteter ... 10
2.3.1 Intraservice roll för personuppgiftsbehandling ... 12
2.3.2 Intraservice användning av personuppgifter ... 12
2.4 Tekniska säkerhetsåtgärder som är vidtagna inom tjänsten ... 13
2.5 Organisatoriska säkerhetsåtgärder ... 15
3 Bilagor ... 16
Appendix 1 - Säkerhetsåtgärder ... 16
Tekniska säkerhetsåtgärder ... 16
Organisatoriska säkerhetsåtgärder ... 18

1 Dokumentets syfte

En *Tjänstespecifikation* dokumenterar säkerhets och dataskyddsaspekter. Specifikationen anger övergripande olika underliggande tekniska funktioner som ingår i tjänsten

Två nivåer av dokumentation:

1. Tjänstespecifikation (kopplad till Intraservice tjänst - övergripande)
2. Funktionsbeskrivning (underliggande funktion som kan ingå i flera tjänster)

*Tjänstespecifikation*en kan återanvändas för olika syften och för att förklara aspekter på säkerhet och dataskydd i en tjänst som Intraservice tillhandahåller.

1.1 Allmänt

Detta dokument är skapat med utgångspunkt att stödja stadens bolag och förvaltningar i olika bedömningar, ställningstaganden och utredningar gällande informationssäkerhet och dataskydd. Dokumentet uppdateras löpande.

Innehållsdata som användarna tillför i tjänsten ingår inte i kartläggningen av personuppgiftbehandlingar.

1.2 Ägarskap och dokumenthantering

<Lämna tomt>

2 Inledning

2.1 Övergripande beskrivning av tjänsten

Office 365 är en molnbaserad plattform som omfattar verktyg för att underlätta dagens arbetssätt. Tjänsten innefattar dels den tekniska plattformen, dels stöd till förvaltningar och bolag och deras medarbetare i att använda och få nytta av digitala verktyg i Office 365.

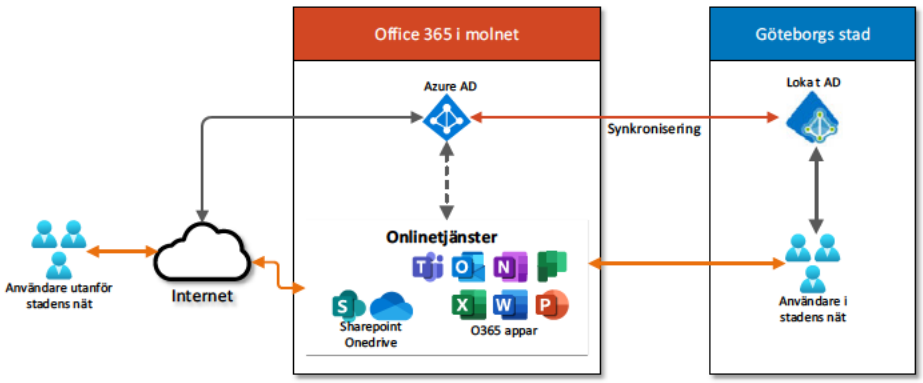
Genom tjänsten kan stadens medarbetare kommunicera, samarbeta och på ett effektivt och säkert sätt få saker gjorda oavsett var man är.

I plattformen ingår:

- Flertalet Out-Of-The-Box (OOTB) program från Microsoft Office 365.
- Gemensamma kommunikationsverktyg som bland annat möjliggör distansmöten med ljud och bild
- Verktyg för kommunikation, samarbete och planering inom grupper
- Programvaror som till exempel Excel, Word, Powerpoint och Outlook i kombination med kraftfulla molntjänster med lagringsmöjligheter såsom Onedrive och Sharepoint.
- Office 365 ger oss möjligheten att skapa och dela filer och information oavsett geografisk plats och enhet; dator, mobiltelefon eller läsplatta.

Plattformen kommer att kunna utvecklas modulärt med olika tjänster och tillämningar. Den är därmed en viktig komponent i framtida digitalisering i staden.

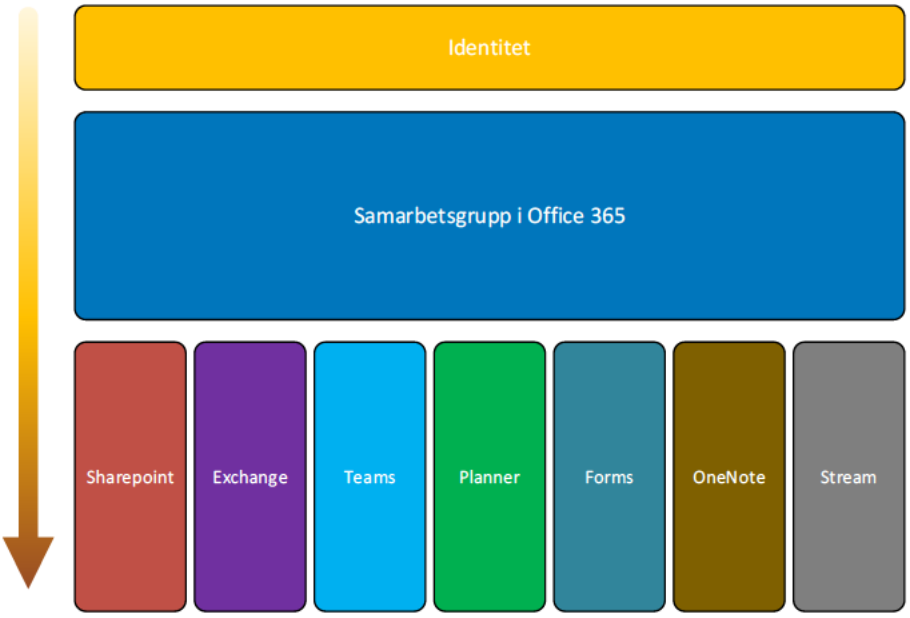
Tjänsten utvecklas utifrån stadens samlade behov. Arbetet med att utveckla tjänsten sker i en utvecklingsorganisation där kundrepresentanter deltar för att fånga in behov kopplade till tjänsten, analysera och prioritera behoven, lansera nya lösningar och förändra arbetssätt.



Microsoft molntjänster för att visualisera Office 365 och koppling till användare och stadens nät.

2.1.1 Behörigheter inom tjänsten

För att tilldela behörigheter inom tjänsten så används samarbetsgrupper i Office 365. I dessa samlas grupper av personer som behöver samarbeta. Gruppen får tillgång till verktyg såsom SharePoint, Planner, Stream och Teams. Gruppen använd också för att ge medlemmarna behörighet till gemensamma filer.



Principen med samarbetsgrupper i Office 365 för behörighetstilldelning.

2.2 Funktioner inom tjänsten

<Beskriv de funktioner eller grupper av funktioner som sammantaget utgör tjänsten. För varje funktion ska en funktionsbeskrivning bifogas denna tjänstespecifikation. Funktionsbeskrivningarna kan delas av flera tjänster. Beskriv översiktligt hur funktionerna hänger samman i tjänsten>

Funktion	Beskrivning
Automatiska basleveranser	Våra organisatoriska grupper och livscykelprocesser.
Beställningsbara tjänster	Allt som beställs via Serviceportalen eller liknande.
Rapport och statistik leveranser	I syfte att förstå användningen av tjänsten.
Metadata	Håller ordning på vem som skapar innehållsdata.

Aktivitetsloggar	Förändringar i behörigheter och gemensamma resurser loggas.
Administrativa portaler	Gränssnitt för konfiguration av tjänsten.
Systemkontroller	Maskinell monitorering för att upptäcka intrång eller skadlig kod.
Teams	**Microsoft Teams** är ett verktyg för samarbete och kommunikation med möjlighet att chatta, ha möten och dela information i en grupp på en och samma plats. Teams är också en ingång till andra verktyg och funktioner.
Sharepoint, Onedrive och Delve	**Sharepoint Online** är en funktion för att spara, dela och samarbeta med dokument och data. Tillhandahåller webbplatser för gruppsamarbete. Sharepoint möjliggör för versionshantering och medförfattarskap. Användningen av funktionen integreras med andra delar av Office 365 för dokumentredigering och delning. **Onedrive** är del av samma tekniska funktion som Sharepoint och ger medarbetare en egen lagringsplats för dokument och innehåll, som de kan dela. **Delve** är ett presentationsgränssnitt som tillhandahåller möjligheten att kunna se andras dokument en användare har tillgång till och baseras på hens behörigheter Sharepoint Online och Onedrive. Delve ger även en visualisering av organisationstillhörighet.
Exchange Online – E-post, Kalender	**Exchange Online** är en produkt hos Microsoft som tillhandahåller den funktionalitet som används i Outlook. Här har vi funktioner som e-post, kalender, adressbok, att-göra lista.
Microsoft Apps for Enterprise	**Microsoft Apps for Enterprise** är ett paket av programvaror som installeras lokalt på en Windows eller Mac OS dator. Tidigare kallades detta för Officepaketet och består av Outlook, Word, Excel, PowerPoint, OneNote, Teams samt Publisher och Access. **Outlook**: Ett verktyg för e-post, adressbok, kalender och Att-göra-lista. **Word**: Ett ordbehandlingsprogram för att skapa dokument. **Excel**: Ett program för att hantera kalkyler och datamängder. **PowerPoint**: Ett verktyg för att skapa och visa bildspel. **OneNote**: Ett verktyg för personliga eller gemensamma digitala anteckningar, organiserade i anteckningsböcker med avsnitt och sidor.

	Teams: Ett verktyg för chatt och möten, samt för kommunikation och samarbete i en grupp. **Publisher**: Skapa egna layouts. Finns inte som online app. **Access**: Skapa egna databaser. Finns inte som online app.
Office mobil appar	För mobila enheter och operativsystem finns Word, Excel, Powerpoint och Teams samt andra appar där användare kan skapa, kommunicera och samarbeta. Microsoft Office mobile apps motsvarar Microsoft 365 Apps for enterprise men körs på Android eller iOS mobila enheter.
Office för webben	Office för webben är en webbtjänst som körs i Microsoft Office 365 miljö. Office för webben hanterar Office-filer var som helst med en internetanslutning.
Viva insikter	Viva Insikter är ett verktyg som ger dig insikter om hur du spenderar din tid och hur du samarbetar. Verktyget hjälper dig att avsätta fokustid innan veckans schema fylls med möten. Du får även hjälp med att hålla dig uppdaterad gällande uppgifter och e-postmeddelanden.
Samarbetsgrupper i Office 365	En grupp i Office 365 är sätt att hantera roller och behörigheter för en grupp personer som har behov av att samarbeta och producera tillsammans. Beskrivning av hur vi hanterar en grupp i Office 365 med ägare och informationsansvarig beskrivs i 'Automatiska basleveranser'.

Tabell 1: Lista över funktioner

Det finns mindre centrala tjänster/funktioner inom O365 som beskrivs härunder. Dessa tjänster har det inte skapats ett extra dokument för eftersom det inte behandlas andra personuppgifter än det som redan har beskrivits.

Mindre centrala tjänster/funktioner:

Funktion	Beskrivning
Stream	Stream är en app på webben där du kan ladda upp, visa och dela videor med kollegor i stadens Office 365-miljö. Du kan dela en video med vissa personer eller en samarbetsgrupp, och du kan ordna dem i kanaler så att de blir lättare att hitta.
Planner	Planner är ett enkelt planeringsverktyg som kan användas till att fördela och följa upp uppgifter i en grupp. Den kan läggas till som en app i Teams och visas då antingen för ett specifikt Teams eller ifall du vill ha en översikt över samtliga dina aktiviteter i både Planner och To Do.

Microsoft Bookings	Bookings är en bokningskalender där du kan publicera bokningsbara tider för olika typer av tjänster. Du kan tillgängliggöra bokningssidan för kollegor i staden, eller vem som helst på internet.
Forms	Ett verktyg för att skapa enkla undersökningar och frågeformulär, eller omröstningar i Teams-möten.
Lists	Ett verktyg för att skapa interaktiva listor för att ordna och följa upp information. Till exempel en checklista, inventarielista, eller en lista över steg i en process eller projekt. Listor kan skapas i Sharepoint, appen lists eller Teams.
To-Do	To Do hjälper dig att fokusera på det som är viktigt genom att samla dina uppgifter i Office 365 på ett ställe. To Do är ett verktyg för att hantera dina uppgifter och att-göralista.
Whiteboard	Whiteboard är en öppen digital arbetsyta - en vit kanvas - där du kan rita, skriva, använda gula lappar, infoga bilder och så vidare. Whiteboard finns tillgänglig i Teams, som en app på webben och en lokalt installerat app (valfritt).
Powerplattform	Powerplattform gör det möjligt att analysera data, bygga lösningar, automatisera processer, och skapa egna chattbotar. Plattformen består av flera olika produkter: • **Power Automate** (automatisera): Förenkla processer med automatisering utan kod. • **Power Bi** (analysera): Hitta insikter i olika typer av data. Finns i olika varianter, gratis, pro, premium. Pro kan beställas från Serviceportalen. • **Power Apps** (agera): Skapa lösningar på affärsutmaningar nästan helt utan kod. • **Power Virtual Agents** (hjälpa): Hantera rutinförfrågningar i stor skala med AI-baserad konversation genom att skapa chattbottar. • **Power Pages** (websidor): Skapa företagswebbplatser för att informera. Powerplattformen körs som test och är inte tillgänglig för alla användare.
Viva	Microsoft Viva består av flera olika produkter: Insights (insikter), Connections (utforska nyheter), Goals (mål), Learning (lära), Topics (hitta innehåll och expertis i organisationen),

	Engage (tidligare Yammer, kommunicera med ditt Team) och Sales (sälj). Endast Viva insikter som beskrivs under centrala tjänster är aktiverat i Stadens Office 365 miljö.

2.3 Personuppgiftsaktiviteter

För att nyttja tjänsten behövs ett konto som kommer tilldelas rättigheter i miljön. Detta konto skulle kunna innehålla påhittade eller slumgenererade personuppgifter men då skulle inte kraven på spårbarhet uppfyllas. Alltså behövs riktiga personuppgifter användas i skapandet av konton. Från AD tas ett urval av personuppgifter för att skapa kontona. Vid avslut tar dessa bort efter en 30 dagars fördröjning. Fördröjningen används då misstag har begåtts eller data behöver sparas undan.

Följande personuppgifter behandlas i tjänsten:

Fält	Vad visas
Displayname	Förnamn + Efternamn
First name	Förnamn
Last name	Efternamn
User principle name	E-postadress
Job title	Förvaltningsnamn
Company name	Förvaltningsnamn
Department	Förvaltningsnamn
Manager	Chef
Email	E-postadress
AD konto	Namn på kontot (Staden-konto)

AD-kontot synkroniseras till Azure AD där kontakt-kortet finns tillgänglig för tjänsterna i Office 365. Organisationstillhörighet är synlig eftersom chefattribut finns på användare och detta visualiseras genom kontakt-kortet i Outlook, SharePoint Teams, osv.

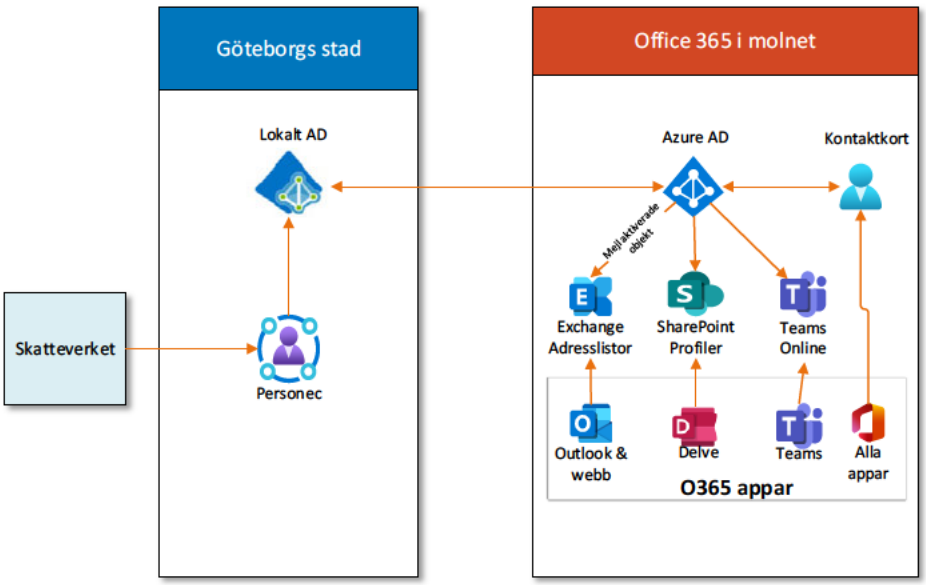


Illustration av personuppgift flödet i Office 365 och den centrala delen kontaktkortet.

Vi använder personuppgifter i följande aktiviteter:

Aktivitet	Beskrivning
Se funktionsbeskrivningarna.	

Tabell 2: Lista över personuppgiftsaktiviteter

2.3.1 Intraservice roll för personuppgiftsbehandling

<Lämna tomt>

2.3.2 Intraservice användning av personuppgifter

<Lämna tomt>

2.4 Tekniska säkerhetsåtgärder som är vidtagna inom tjänsten

I grunden är allt data i 365 tjänsten lagrad på servrar i stora datacentraler med mycket starkt skalskydd. Utöver detta är alla diskar speglade och krypterade för att säkerställa driftsäkerhet och skydd mot data stöld.

Merparten av data är flyttat från Europa till Microsofts datacenter i Sverige.

Larmsystem finns implementerat som söker efter mönster som antyder till olaglig verksamhet. Som exempel, används ett konto på två olika platser så det är omöjligt att samma person gör inloggningen så går larmet och åtgärder vidtas.

Användare behöver ladda ner och upp data till/från klienter för att kunna jobba lokalt. För att bibehålla säkerhetsnivån så har detta begränsats till Stadens kontrollerade maskiner där disken är krypterad med kontroll av virusskydd och versioner på applikationerna.

Överföringen mellan dessa klienter och datacentralen sker krypterat och är helt skyddad från stöld och avlyssning. I de fall data behöver nås, når man detta via mobiltelefoner så är det endast godkända appar där data inte läcker som går att använda. Dessa begränsningar påverkar tillgängligheten men är vägda mot att bibehålla säkerhetsnivån i säkerhetslösningen.

I användningen av O365 har det tekniskt tätats möjligheter till dataläckage samt med leverantörsavtal uppnås att allt är inneslutet i säkerhetslösningen.

För att kommunicera och samverka med personer och organisationer utanför den tekniska lösningen. Därför öppnas den upp och det finns information om hur tjänsten ska användas. E-post är den mest uppenbara öppningen i säkerhetskonceptet. Här kan alla data flöda fritt ut och in. Däremot finns mailtvätt och kontroller efter skadlig kod och länkar implementerat samt domänhantering och globala blocklistor. Att dela filer med externa användare är ett nytt sätt att jobba som också är en öppning in i säkerhetslösningen. Kontroll behålls men med möjlighet att ”stänga” tillgången utifrån.

Mänskliga faktorn är fortsatt den största risken för dataläckage. Styrande dokument och dokumenthanteringsinstruktioner hanterar dessa risker.

Att över tid bibehålla denna säkerhetsnivå och skydda data i denna säkerhetslösning är den viktigaste uppgiften för en leverantör av tjänsten till Stadens anställda. En stor säkerhets review på miljön görs årligen för att genomlysa och införa förbättringar.

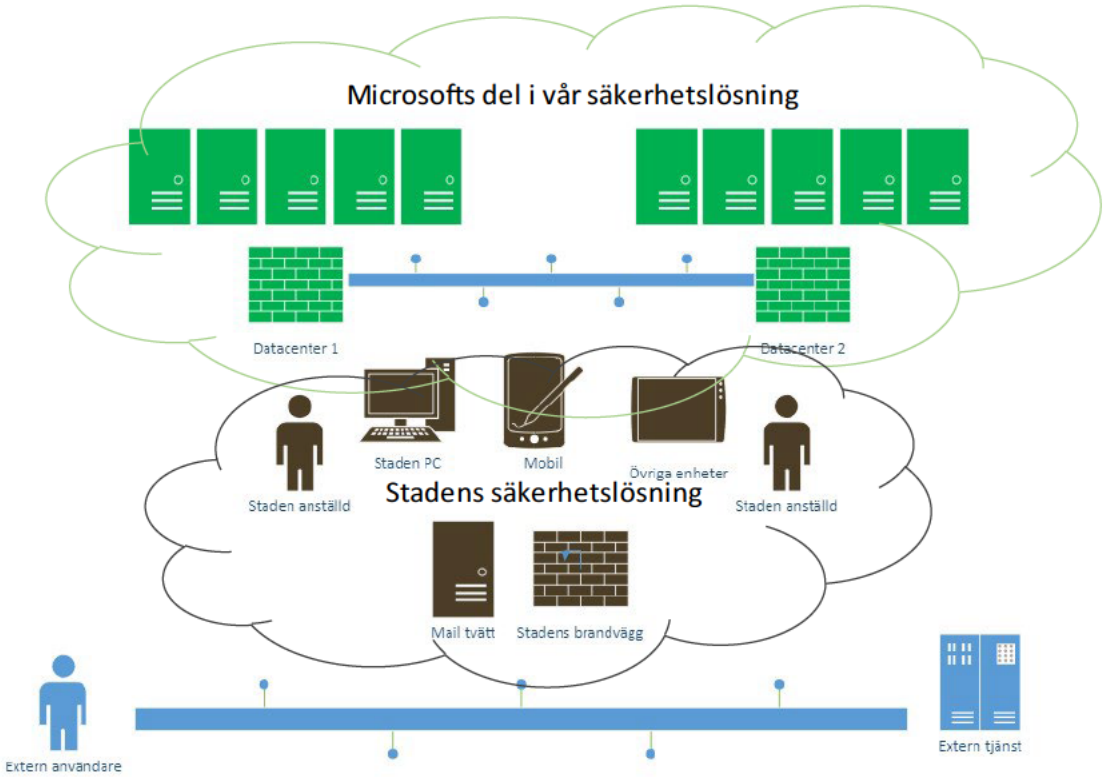


Illustration av tekniska säkerhetslösningen för O365.

Säkerhetsåtgärder	**Beskrivning**
<Säkerhetsåtgärdens namn>	<Beskrivning>
T1 Behörighetskontroll	Att förhindra att obehörig användning eller åtkomst. Exempelvis genom bekräftning av identiteter, personligt lösenord, engångslösenord eller biometriska metoder.
T5 Dataseparering	Separering av information, och enbart ge åtkomst till de data som är nödvändigt
T6 Logisk åtkomstkontroll	Definierar begränsning av åtkomst till data genom vem som ska ha åtkomst till information, när och under vilka omständigheter. Exempelvis genom tekniker för cybersäkerhet såsom identifiering, autentisering och auktorisering.
T7 Loggning	Dokumentering av behandlingar som utförs i ett system för att identifiera obehörig åtkomst, missbruk eller liknande.
T15 Spårbarhet	Dokumentering av vem som lagt till, ändrat eller tagit bort information i ett system
T17 Segmentering av personuppgifter	Metoder för att minska möjligheten att korrelera eller härleda personuppgifter till en individ. Exempelvis begränsa personuppgifter till sektioner/enheter eller logisk separering
T21 Autentisering	Kontroll av den uppgivna identiteten, exempelvis genom personligt lösenord

Säkerhetsåtgärder	**Beskrivning**
<Säkerhetsåtgärdens namn>	<Beskrivning>

T19 Kryptering vid överföring	Kryptering av all trafik vid överföring av uppgifter.
T20 Kryptering vid vila	Kryptering vid lagring av information
T22 Flerfaktorsautentisering (MFA)	Krav på två eller fler former av information som styrker den uppgivna identiteten. Hantera säker inloggning för Office 365 möjliggörs genom bank-id och användare kan komma i gång från en inte staden-dator.
Begränsningar i Onedrive	Förhindrar ofrivilligt dataläckage
Begränsningar i Mobil appar	Förhindrar ofrivilligt dataläckage
Gallring av chatt- och mejlloggar	Tillämpningsbeslut finns
Livscykel hantering	Hjälper verksamheterna att tillsätta viktiga roller och städa bort oanvända resurser
Lagring i Sverige	Lagring i datacenter i Sverige
*Monitorering av system	larmsystem som söker efter mönster som antyder till olaglig verksamhet
Managering av stadendator	För att bibehålla säkerhetsnivån är det begränsat detta till Stadens kontrollerade maskiner där disken är krypterad, kontroll på virusskydd och versioner på applikationerna
Rutiner för extern kommunikation	Implementerade rutiner för extern kommunikation via exempelvis e-post.
Skalskydd	Implementerat för att stadens servrar ska lagras säkert

Tabell 3: Lista över säkerhetsåtgärder

2.5 Organisatoriska säkerhetsåtgärder

<Beskriv vilka organisatoriska säkerhetsåtgärder som är vidtagna i syfte att skydda personuppgifter i tjänsten. Se lista i Appendix 1 - Säkerhetsåtgärder över förslag på säkerhetsåtgärder. Anpassa beskrivningen till den implementation som sker i tjänsten. Ange även eventuella hänvisningar till andra tjänster eller styrande dokument.

Säkerhetsåtgärder	Beskrivning
<Säkerhetsåtgärdens namn>	<Beskrivning>
O7 Informationssäkerhetspolicy	Styrande dokument som tydliggör den personuppgiftsansvarigas informationssäkerhetsarbete, implementerade åtgärder och instruktioner gällande arbetssätt.
O14 Integritetspolicy och riktlinjer	Styrande dokument som reglerar integritetsskyddsfrågor inom verksamheten.
O16 Regler för kunskapshöjning och utbildning (redaktörsutbildning)	Regelbundna utbildningar för medarbetare gällande dataskydd och informationssäkerhet. Detta görs innan man får behörighet att skapa innehåll i digitala navet.
Redaktionella riktlinjer	Riktlinjer som redaktörer ska följa vid publicering i Digitala navet

Säkerhetsåtgärder	Beskrivning
<Säkerhetsåtgärdens namn>	<Beskrivning>
O23 Intern tillsyn	Rutiner för kontroller av att implementerade åtgärder är effektiva

Kundskapsportalen	Information om hur tjänsten ska användas.
Instruktioner vid nybeställning	Information om hur tjänsten ska användas.

3 Bilagor

Dokumentnamn	Version	Beskrivning
<Bilagans namn>		

Tabell 5-: Lista över bilagor

Appendix 1 - Säkerhetsåtgärder

Nedan lista på allmänt beskrivna tekniska och organisatoriska säkerhetsåtgärder är övergripande beskrivet och kan användas för beskrivningar.[1]

Tekniska säkerhetsåtgärder

Nr	Tekniska åtgärder	Definition
T1	Behörighetskontroll	Att förhindra att obehörig användning eller åtkomst. Exempelvis genom bekräftning av identiteter, personligt lösenord, engångslösenord eller biometriska metoder.
T2	Behandlingshistorik	Åtkomst till personuppgifter kan kontrolleras genom att behandlingshistorik sparas under en specificerad tid.
T3	Avidentifiering	Omöjliggör återidentifieringen av en individ.
T4	Kryptering	Åtgärder för att personliga data är obegriplig för obehöriga. Se även asymmetrisk och symmetrisk kryptering.
T5	Dataseparering	Separering av information, och enbart ge åtkomst till de data som är nödvändigt

[1] Listan är sammanställd med hjälp av *Säkerhet för personuppgifter – Datainspektionen allmänna råd* (Integritetskyddsmyndighetens, IMY:s tidigare namn) samt en taxonomi i *Privacy Impact Assessment (PIA) – PIA guides samt PIA Software* av IMY:s franska motsvarighet Commission Nationale Informatique & Libertés (CNIL).

T6	Logisk åtkomstkontroll	Definierar begränsning av åtkomst till data genom vem som ska ha åtkomst till information, när och under vilka omständigheter. Exempelvis genom tekniker för cybersäkerhet såsom identifiering, autentisering och auktorisering.
T7	Loggning	Dokumentering av behandlingar som utförs i ett system för att identifiera obehörig åtkomst, missbruk eller liknande.
T8	Dataminimering	Lagrade/behandlade personuppgifter minimeras genom exempelvis filtrering och borttagning, minskning av datainsamling eller begränsning av datatillgång.
T9	Riktlinjer för driftsäkerhet	Styrande dokument som begränsar sannolikheten för risker mot fysisk utrustning, exempelvis dokumentation av driftsförvaranden, inventering och uppdatering av program- och hårdvara, redundans av data, begränsning av fysisk tillgång till servrar etc.
T10	Skydd av webbplats	Metoder för att minska möjligheten att webbplatser utnyttjas för att kränka personuppgifter. Exempelvis allmänna säkerhetsrutiner, SSL-kryptering, cookiepolicy, säkerhetsuppdateringar)
T11	Säkerhetskopiering	Dokumenterad säkerhetskopieringsrutin/back-uprutin för att säkerställa tillgänglighet, integritet och konfidentialitet
T12	Policy för underhåll av utrustning	Styrande dokument som tydliggör förekomst av fysiskt underhåll av utrustning samt eventuellt specificerar om/hur leverantörer kan användas. Inkluderar även reglering av fjärrskrivbord samt hantering av kasserat material.
T13	Policy för nätverkssäkerhet	Styrande dokument gällande vilken typ av nätverk som behandlingen ska utföras på. Inklusive tydliggörande av adekvata skyddssystem exempelvis brandväggar, intrångsdetektering samt aktiva eller passiva metoder för att nätverkets säkerhet.
T14	Fysisk åtkomstkontroll	Begränsning av åtkomsten till en fysisk plats. Exempelvis genom lås och nycklar, lösenordskyddade dörrar, vakter, zonindelning eller ID-brickor.
T15	Spårbarhet	Dokumentering av vem som lagt till, ändrat eller tagit bort information i ett system
T16	Pseudonymisering	Ersätter identifierande information med en pseudonym. Kodnyckeln lagras på en separat plats (även kallad för anonymisering)
T17	Segmentering av personuppgifter	Metoder för att minska möjligheten att korrelera eller härleda personuppgifter till en individ. Exempelvis begränsa personuppgifter till sektioner/enheter eller logisk separering
T18	Filtrering och radering	Rutiner för borttagning av överflödiga metadata vid import av data, exempelvis EXIF-data som är kopplade till en bildfil.
T19	Kryptering vid överföring	Kryptering av all trafik vid överföring av uppgifter.

T20	Kryptering vid vila	Kryptering vid lagring av information
T21	Autentisering	Kontroll av den uppgivna identiteten, exempelvis genom personligt lösenord
T22	Flerfaktorsautentisering (MFA)	Krav på två eller fler former av information som styrker den uppgivna identiteten
T23	Patchning	Regelbundna mjukvaruuppdateringar av programvara i syfte att upprätthålla säkerheten.

Organisatoriska säkerhetsåtgärder

Nr	Organisatoriska åtgärder	Definition
O1	Låsutrustning	Tillgång till utrustning som möjliggör att låsa/låsa in uppgifter och därmed enbart blir tillgängliga med nyckel
O2	Inpasseringskontroll	Fysiska hinder för obehöriga att få åtkomst till verksamhetens lokaler och information.
O3	Larmutrustning	Larmutrustning som kan detektera inbrott, brand och andra oönskade händelser.
O4	Säkerhetsskåp	Ett skåp som vid provning under minst 10 minuter, ska stå emot angrepp, enligt Svensk standard SS 2492/SSF 3492.
O5	Tillträdeskontroll	Att säkerställa att enbart behörig personal får tillträde till utrymmen där IT-utrustning genom exempelvis upprättandet av rutiner för tillträdeskontroll.
O6	Lösenordspolicy	Styrande dokument som tydliggör användares lösenords längd, tecken samt automatisk begäran om byte av lösenord.
O7	Informationssäkerhetspolicy	Styrande dokument som tydliggör den personuppgiftsansvarigas informationssäkerhetsarbete, implementerade åtgärder och instruktioner gällande arbetssätt.
O8	Rutin för distansarbete	Styrande dokument som tydliggör hur verksamhetens information ska hanteras utanför den kontrollerande nätverks- och kontorsmiljön.
O9	Arkivering	Uppgifter som inte används i vardagligt arbete arkiveras i säkra arkiv.
O10	Policy för hantering av pappersdokument	Instruktioner och tydliga arbetssätt för medarbetare att förhålla sig till vid hantering av pappersdokument med personuppgifter
O11	Policy för arbetsstationshantering	Styrande dokument som tydliggör arbetssätt gällande arbetsstationer för att minska möjligheten att mjukvaror kan utnyttjas. Exempelvis mjuvaruuppdateringar, fysiskt skydd och åtkomstkontroll, arbete på ett krypterat nätverk, integritetskontroller och loggning)

O12	PUB-avtal	Personuppgiftsbiträdesavtal. Dokumentation på överenskommelse mellan PUA och PUB gällande säkerhetspolicy, instruktioner till PUB samt planerade åtgärder så som säkerhetsrevisioner. PUB-avtal definierar hur PUB ska hantera personuppgifter samt de säkerhetsåtgärder som ska implementeras.
O13	Implementerad dataskyddsorganisation	Tydlig dataskyddsorganisation om verksamheten som arbetar med samt följer upp dataskyddsarbetet och behandlingar.
O14	Integritetspolicy och riktlinjer	Styrande dokument som reglerar integritetsskyddsfrågor inom verksamheten.
O15	Implementerad och förankrad process för PUI	Arbetssätt för att identifiera, rapportera och hantera personuppgiftsincidenter i verksamheten. Inklusive utpekat ansvar för hantering, implementering av åtgärder samt anmälan till tillsynsmyndighet.
O16	Regler för kunskapshöjning och utbildning	Regelbundna utbildningar för samtliga medarbetare gällande dataskydd och informationssäkerhet
O17	Hantering av tredjeparter	Dokumenterat arbetssätt gällande hantering av behandlingar som inkluderar tredjeparter. Inklusive identifiering av tredjepart, skrivande av PUB-avtal och andra avtalsmässiga åtgärder.
O18	Rutin för tillsyn av integritetsskyddande åtgärder	Regelbundna granskningar och tillsyner (interna och externa) som ger en övergripande bild av dataskyddsarbetet och efterlevnaden av GDPR.
O19	Riktlinjer för säkerhet finns hos (leverantörens namn)	Styrande dokument gällande säkerhet finns upprättade hos leverantören som PUA tagit del av.
O20	(Leverantörens namn) har utsett informationssäkerhetsansvarig	Leverantören har utsett en informationssäkerhetsansvarig som PUA fått kontaktuppgifter till samt kan kontakta vid behov.
O21	Sekretessavtal	Vid användning av tjänster/information finns ett sekretessavtal framtaget
O22	Säkra lokaler	Områden som upprättats för att minska avbrott eller störningar
O23	Intern tillsyn	Rutiner för kontroller av att implementerade åtgärder är effektiva
O24	Leverantörskontroller	Rutiner för återkommande leverantörskontroller under avtalstiden

Göteborgs Stad

Identitet och Åtkomst

Tjänstespecifikation gällande säkerhet och dataskydd

2023-05-19

Tjänsteägare: Jonas Wahlström

Versionshantering av detta dokument

Datum	Version	Beskrivning	Ändrat av
2023-03-27	0.1	Skapat ett första utkast	Fredrik Nikander Finman
2023-05-18	0.4	Korrigerat innehåll för samstämmighet med andra dokument	Marcus Broman

Innehåll

1 Dokumentets syfte ... 4
1.1 Allmänt ... 4
1.2 Ägarskap och dokumenthantering ... 4
2 Inledning ... 5
2.1 Övergripande beskrivning av tjänsten ... 5
2.2 Funktioner inom tjänsten ... 6
2.3 Personuppgiftsaktiviteter ... 7
2.3.1 Intraservice roll för personuppgiftsbehandling ... 9
2.3.2 Intraservice användning av personuppgifter ... 9
2.4 Tekniska säkerhetsåtgärder som är vidtagna inom tjänsten ... 10
2.5 Organisatoriska säkerhetsåtgärder ... 11
3 Bilagor ... 11
Appendix 1 - Säkerhetsåtgärder ... 11
Tekniska säkerhetsåtgärder ... 11
Organisatoriska säkerhetsåtgärder ... 13

1 Dokumentets syfte

En *Tjänstespecifikation* dokumenterar säkerhets och dataskyddsaspekter. Specifikationen anger övergripande olika underliggande tekniska funktioner som ingår i tjänsten

Två nivåer av dokumentation:

1. Tjänstespecifikation (kopplad till Intraservice tjänst - övergripande)
2. Funktionsbeskrivning (underliggande funktion som kan ingå i flera tjänster)

*Tjänstespecifikation*en kan återanvändas för olika syften och för att förklara aspekter på säkerhet och dataskydd i en tjänst som Intraservice tillhandahåller.

1.1 Allmänt

Detta dokument är skapat med utgångspunkt att stödja stadens bolag och förvaltningar i olika bedömningar, ställningstaganden och utredningar gällande informationssäkerhet och dataskydd. Dokumentet uppdateras löpande.

1.2 Ägarskap och dokumenthantering

<Lämna tomt>

2 Inledning

2.1 Övergripande beskrivning av tjänsten

<Beskriv översiktligt tjänsten, vilket syfte tjänsten har och på vilket sätt tjänsten brukas av användare i staden.>

Identitet och Åtkomst hanterar livscykeln för användaridentiteter och deras rättigheter.

Hanteringen består av;

- Skapande av identitet för användare
- Skapande av konto(n) för användare
- Ändring av konto(n) för användare
- Borttag av konto(n) för användare*
- Autentisering, identifiering och verifiering av användare i samband med åtkomst till IT-system.
- Auktorisation, vad en användare ska kunna utföra i ett IT-system.
- Federering, ger behöriga användare tillgång till flera IT-system och domäner genom en uppsättning av inloggningsuppgifter.

2.2 Funktioner inom tjänsten

<Beskriv de funktioner eller grupper av funktioner som sammantaget utgör tjänsten. För varje funktion ska en funktionsbeskrivning bifogas denna tjänstespecifikation. Funktionsbeskrivningarna kan delas av flera tjänster. Beskriv översiktligt hur funktionerna hänger samman i tjänsten>

Funktion	Beskrivning
<Funktionens eller grupp av funktioners namn samt hänvisning till bilaga>	<Kort beskrivning av funktionen>
Skapande av identitet för användare	Fysisk person som är uppbyggt av anställningsinformation; *Personnummer, Alla Förnamn, Efternamn, Tilltalsnamn, Mellannamn, Sekretessmarkerad, Giltig from, Giltig tom, Avtalskod, Enhet och AID kod.*
Skapande av konto(n) för användare	Konto är en unik identitet för en användare som används i relationen mellan en användare och IT-system. Konton tilldelas ett un kt kontonamn eller användarnamn. Vanligaste kontotyperna inom Staden är AD konto och TDS konto (autentiseringskatalog). Ett konto är uppbyggt av anställningsinformation och organisationsinformation.
Ändring av konto(n) för användare	Ändring av konto(n) för användare sker vid förändringar av anställningsinformation, organisationsinformation och eller användarinformation.
Borttag av konto(n) för användare*	Borttag av konton för person kommer att ske per automat k i samband med att anställning avslutas för anställda. För externa är respektive verksamhet ansvariga för användarnas konton. Verksamheten är också ansvarig för att gallring av data sker när deras medarbetare lämnar verksamheten. Generella gällande regler för Stadens centrala katalogtjänst(er) → Konton med inaktiva identiteter kommer tas bort efter 30 dagar. → Identiteter utan konton kommer att tas bort efter 90 dagar.
Autentisering	Autentisering, identifiering och verifiering av användare sker genom uppslag mot centrala katalogtjänster där alla användare har ett konto.
Auktorisation	Auktorisation för vad en användare ska kunna utföra styrs på olika sätt beroende på IT system. Det kan exempelvis styras via central behörighetsinformation eller direkt inne i ett IT system. Alternativt i en kombination av dessa nämnda exempel.
Federering	Federering bygger på tillit mellan tjänsteleverantörer som möjliggör för användare att verifiera sig via central tjänst där identitetsinformation överförs via token(s), som är bärare av utvalda användardata. Exempel på användardata; *Kontonamn, Personnummer, telefonnummer, epost-adress osv.* Inloggning till ett IT system mha BankID är ett exempel på federering.

Tabell 1: Lista över funktioner

2.3 Personuppgiftsaktiviteter

<Beskriv de olika aktiviteter som omfattar personuppgifter, direkt eller indirekt som sker inom tjänsten exempelvis insamling, lagring, bearbetning, utlämning eller förstöring.>

Aktivitet	Beskrivning
<Namn på aktivitet>	<Beskrivning av aktivitet>
Skapa konto	**Insamling** Insamling av data sker primärt från kvalitetssäkrade data för Anställda. Se bifogad fil för 'Kontohantering tider' **Lagring** Lagring av identitet och konto uppgifter görs så länge som det finns en aktiv anställning. **Bearbetning** Anställningsinformation och organisationsinformation läses, skrivs och tas bort allt eftersom informationen förändras i källsystemen (primärt kvalitetssäkrade data). **Utlämning** Kontoinformation delas via epost med den anställdes chef(er). Information om förändring av anställning delas med chef för respektive anställning (berör främst de med flera anställningar).
Ändra Konto	**Bearbetning** Anställningsinformation och organisationsinformation läses, skrivs och tas bort allt eftersom informationen förändras i källsystemen (primärt kvalitetssäkrade data). (Telefonnummer information kan användaren själv lägga till). Se bifogad fil för 'Kontohantering tider' **Utlämning** Information om förändring av anställning delas med chef för respektive anställning (berör främst de med flera anställningar).
Borttag av Konto	**Bearbetning** Anställningsinformation och organisationsinformation läses, skrivs och tas bort allt eftersom informationen förändras i källsystemen (primärt MMD). **Förstöring** Generella gällande regler för Stadens centrala katalogtjänst(er) → Konton med inaktiva identiteter kommer tas bort efter 30 dagar. → Identiteter utan konton kommer att tas bort efter 90 dagar. **Lagring** Anställningsinformation och organisationsinformation lagras ändamålsenligt utifrån Staden som arbetsgivare.
Autentisering	**Bearbetning** Uppslag och verifiering mot centrala katalogtjänster och/eller IT system samt läsning av anställningsinformation och organisationsinformation.

Aktivitet	Beskrivning
Auktorisation	**Insamling** Konto tilldelas medlemskap i bestämda data strukturer ,som definierar rättigheter för en användare i IT system, för de centrala katalogtjänsterna via automation utifrån anställningsinformation och organisationsinformation eller manuellt utifrån beställning. **Bearbetning** Uppslag av kontonamn (eller annan av IT systemet efterfrågad användarinformation) mot centrala katalogtjänster och/eller enskilda IT system för att läsa och verifiera en användares behörighet och vad användare har rättighet att utföra i respektive IT system. **Förstöring** Konto fråntas medlemskap i bestämda data strukturer ,som definierar rättigheter för en användare i IT system, för de centrala katalogtjänsterna via automation utifrån anställningsinformation och organisationsinformation eller manuellt utifrån beställning.
Federering	**Bearbetning** Uppslag mot centrala katalogtjänster och läsning av anställningsinformation och organisationsinformation utifrån begärd information för token. **Utlämning** Utlämning till tredje part av anställningsinformation och organisationsinformation utifrån överenskommen information.

Tabell 2: Lista över personuppgiftsaktiviteter

2.3.1 Intraservice roll för personuppgiftsbehandling

<Lämna tomt>

2.3.2 Intraservice användning av personuppgifter

<Lämna tomt>

2.4 Tekniska säkerhetsåtgärder som är vidtagna inom tjänsten

<Beskriv vilka tekniska säkerhetsåtgärder som redan är vidtagna i syfte att skydda personuppgifterna som behandlas i tjänsten. Se lista i Appendix 1 - Säkerhetsåtgärder över förslag på säkerhetsåtgärder. Anpassa beskrivningen till den implementation som sker i tjänsten. Ange även eventuella hänvisningar till andra tjänster eller styrande dokument.>

Teknisk säkerhetsåtgärd	Beskrivning
<Säkerhetsåtgärdens namn>	<Beskrivning av säkerhetsåtgärden>
T1 Behörighetskontroll T21, T22 Autentisering, Flerfaktorsautentisering (MFA)	Användarnamn + lösenord, administrativa konton skyddade av PAM lösning (digitalt kassaskåp).
T2, T7 Behandlingshistorik, Loggning	Loggar för inloggningar och systemaktiviteter/händelser till förändringar för enskilda konton ex lösenordsbyten.
T4 Kryptering	Vissa personuppgiftsdata skyddas antingen med asymmetrisk eller symmetrisk kryptering
T10 Skydd av webbplats	Intern/extern trafik skyddad via certifikat och SSL-kryptering.
T19 Kryptering vid överföring	Se T10
T20 Kryptering vid vila	Se T4
T5 Dataseparering	Vi ger enbart åtkomst till de data som är nödvändigt. Sker genom behörighetsstyrning i våra produkter.
T6 Logisk åtkomstkontroll	Vi använder oss av identifiering, autentisering och auktorisering för behörig personal.
T8 Dataminimering	Lagrade/behandlade personuppgifter görs endast utifrån legala eller funktionella krav.
T11 Säkerhetskopiering	Säkerhetskopieringsrutin/back-uprutin för att säkerställa tillgänglighet, integritet och konfidentialitet görs enligt befintlig infrastrukturtjänst.
T15 Spårbarhet	Dokumentering av vem som lagt till, ändrat eller tagit bort information hanteras mha logghantering.
T23 Patchning	Patchning görs men inte med fastslagen periodicitet för produkterna. OS patchning görs månadsvis.

Tabell 3: Lista över tekniska säkerhetsåtgärder

2.5 Organisatoriska säkerhetsåtgärder

<Beskriv vilka organisatoriska säkerhetsåtgärder som är vidtagna i syfte att skydda personuppgifter i tjänsten. Se lista i Appendix 1 - Säkerhetsåtgärder över förslag på säkerhetsåtgärder. Anpassa beskrivningen till den implementation som sker i tjänsten. Ange även eventuella hänvisningar till andra tjänster eller styrande dokument.>

Organitoriska säkerhetsåtgärd	Beskrivning
<Säkerhetsåtgärdens namn>	<Beskrivning av säkerhetsåtgärden>
O2, Inpasseringskontroll	Ja, i enlighet med skalskydd för Intraservice lokaler
O3, Larmutrustning	Ja, i enlighet med skalskydd för Intraservice lokaler
O5, Tillträdeskontroll	Ja, i enlighet med skalskydd för Intraservice lokaler
O6, Lösenordspolicy	Ja, se länk här
O15, Implementerad och förankrad process för PUI	Ja, enligt Stadens incidentprocess
O21, Sekretessavtal	Ja, enligt Stadens anställningsavtal och HR process

Tabell 4: Lista över organitoriska säkerhetsåtgärder

3 Bilagor

Dokumentnamn	Version	Beskrivning
<Bilagans namn>		
Kontohantering tider.xlsx		Visar alla schemalagda flöden kopplat till identitet- och kontoskapande

Tabell 5-: Lista över bilagor

Appendix 1 - Säkerhetsåtgärder

Nedan lista på allmänt beskrivna tekniska och organisatoriska säkerhetsåtgärder är övergripande beskrivet och kan användas för beskrivningar.[1]

Tekniska säkerhetsåtgärder

Nr	Tekniska åtgärder	Definition

[1] Listan är sammanställd med hjälp av *Säkerhet för personuppgifter – Datainspektionen allmänna råd* (Integritetskyddsmyndighetens, IMY:s tidigare namn) samt en taxonomi i *Privacy Impact Assessment (PIA) – PIA guides samt PIA Software* av IMY:s franska motsvarighet Commission Nationale Informatique & Libertés (CNIL).

T1	Behörighetskontroll	Att förhindra att obehörig användning eller åtkomst. Exempelvis genom bekräftning av identiteter, personligt lösenord, engångslösenord eller biometriska metoder.
T2	Behandlingshistorik	Åtkomst till personuppgifter kan kontrolleras genom att behandlingshistorik sparas under en specificerad tid.
T3	Avidentifiering	Omöjliggör återidentifieringen av en individ.
T4	Kryptering	Åtgärder för att personliga data är obegriplig för obehöriga. Se även asymmetrisk och symmetrisk kryptering.
T5	Dataseparering	Separering av information, och enbart ge åtkomst till de data som är nödvändigt
T6	Logisk åtkomstkontroll	Definierar begränsning av åtkomst till data genom vem som ska ha åtkomst till information, när och under vilka omständigheter. Exempelvis genom tekniker för cybersäkerhet såsom identifiering, autentisering och auktorisering.
T7	Loggning	Dokumentering av behandlingar som utförs i ett system för att identifiera obehörig åtkomst, missbruk eller liknande.
T8	Dataminimering	Lagrade/behandlade personuppgifter minimeras genom exempelvis filtrering och borttagning, minskning av datainsamling eller begränsning av datatillgång.
T9	Riktlinjer för driftsäkerhet	Styrande dokument som begränsar sannolikheten för risker mot fysisk utrustning, exempelvis dokumentation av driftsförvaranden, inventering och uppdatering av program- och hårdvara, redundans av data, begränsning av fysisk tillgång till servrar etc.
T10	Skydd av webbplats	Metoder för att minska möjligheten att webbplatser utnyttjas för att kränka personuppgifter. Exempelvis allmänna säkerhetsrutiner, SSL-kryptering, cookiepolicy, säkerhetsuppdateringar)
T11	Säkerhetskopiering	Dokumenterad säkerhetskopieringsrutin/back-uprutin för att säkerställa tillgänglighet, integritet och konfidentialitet
T12	Policy för underhåll av utrustning	Styrande dokument som tydliggör förekomst av fysiskt underhåll av utrustning samt eventuellt specificerar om/hur leverantörer kan användas. Inkluderar även reglering av fjärrskrivbord samt hantering av kasserat material.
T13	Policy för nätverkssäkerhet	Styrande dokument gällande vilken typ av nätverk som behandlingen ska utföras på. Inklusive tydliggörande av adekvata skyddssystem exempelvis brandväggar, intrångsdetektering samt aktiva eller passiva metoder för att nätverkets säkerhet.
T14	Fysisk åtkomstkontroll	Begränsning av åtkomsten till en fysisk plats. Exempelvis genom lås och nycklar, lösenordskyddade dörrar, vakter, zonindelning eller ID-brickor.
T15	Spårbarhet	Dokumentering av vem som lagt till, ändrat eller tagit bort information i ett system
T16	Pseudonymisering	Ersätter identifierande information med en pseudonym. Kodnyckeln lagras på en separat plats (även kallad för anonymisering)
T17	Segmentering av personuppgifter	Metoder för att minska möjligheten att korrelera eller härleda personuppgifter till en individ. Exempelvis begränsa personuppgifter till sektioner/enheter eller logisk separering

T18	Filtrering och radering	Rutiner för borttagning av överflödiga metadata vid import av data, exempelvis EXIF-data som är kopplade till en bildfil.
T19	Kryptering vid överföring	Kryptering av all trafik vid överföring av uppgifter.
T20	Kryptering vid vila	Kryptering vid lagring av information
T21	Autentisering	Kontroll av den uppgivna identiteten, exempelvis genom personligt lösenord
T22	Flerfaktorsautentisering (MFA)	Krav på två eller fler former av information som styrker den uppgivna identiteten
T23	Patchning	Regelbundna mjukvaruuppdateringar av programvara i syfte att upprätthålla säkerheten.

Organisatoriska säkerhetsåtgärder

Nr	Organisatoriska åtgärder	Definition
O1	Låsutrustning	Tillgång till utrustning som möjliggör att låsa/låsa in uppgifter och därmed enbart blir tillgängliga med nyckel
O2	Inpasseringskontroll	Fysiska hinder för obehöriga att få åtkomst till verksamhetens lokaler och information.
O3	Larmutrustning	Larmutrustning som kan detektera inbrott, brand och andra oönskade händelser.
O4	Säkerhetsskåp	Ett skåp som vid provning under minst 10 minuter, ska stå emot angrepp, enligt Svensk standard SS 2492/SSF 3492.
O5	Tillträdeskontroll	Att säkerställa att enbart behörig personal får tillträde till utrymmen där IT-utrustning genom exempelvis upprättandet av rutiner för tillträdeskontroll.
O6	Lösenordspolicy	Styrande dokument som tydliggör användares lösenords längd, tecken samt automatisk begäran om byte av lösenord.
O7	Informationssäkerhetspolicy	Styrande dokument som tydliggör den personuppgiftsansvarigas informationssäkerhetsarbete, implementerade åtgärder och instruktioner gällande arbetssätt.
O8	Rutin för distansarbete	Styrande dokument som tydliggör hur verksamhetens information ska hanteras utanför den kontrollerande nätverks- och kontorsmiljön.
O9	Arkivering	Uppgifter som inte används i vardagligt arbete arkiveras i säkra arkiv.
O10	Policy för hantering av pappersdokument	Instruktioner och tydliga arbetssätt för medarbetare att förhålla sig till vid hantering av pappersdokument med personuppgifter
O11	Policy för arbetsstationshantering	Styrande dokument som tydliggör arbetssätt gällande arbetsstationer för att minska möjligheten att mjukvaror kan utnyttjas. Exempelvis mjuvaruuppdateringar, fysiskt skydd och åtkomstkontroll, arbete på ett krypterat nätverk, integritetskontroller och loggning)
O12	PUB-avtal	Personuppgiftsbiträdesavtal. Dokumentation på överenskommelse mellan PUA och PUB gällande säkerhetspolicy, instruktioner till PUB samt planerade åtgärder så som säkerhetsrevisioner. PUB-avtal definierar hur PUB ska hantera personuppgifter samt de säkerhetsåtgärder som ska implementeras.

O13	Implementerad dataskyddsorganisation	Tydlig dataskyddsorganisation om verksamheten som arbetar med samt följer upp dataskyddsarbetet och behandlingar.
O14	Integritetspolicy och riktlinjer	Styrande dokument som reglerar integritetsskyddsfrågor inom verksamheten.
O15	Implementerad och förankrad process för PUI	Arbetssätt för att identifiera, rapportera och hantera personuppgiftsincidenter i verksamheten. Inklusive utpekat ansvar för hantering, implementering av åtgärder samt anmälan till tillsynsmyndighet.
O16	Regler för kunskapshöjning och utbildning	Regelbundna utbildningar för samtliga medarbetare gällande dataskydd och informationssäkerhet
O17	Hantering av tredjeparter	Dokumenterat arbetssätt gällande hantering av behandlingar som inkluderar tredjeparter. Inklusive identifiering av tredjepart, skrivande av PUB-avtal och andra avtalsmässiga åtgärder.
O18	Rutin för tillsyn av integritetsskyddande åtgärder	Regelbundna granskningar och tillsyner (interna och externa) som ger en övergripande bild av dataskyddsarbetet och efterlevnaden av GDPR.
O19	Riktlinjer för säkerhet finns hos (leverantörens namn)	Styrande dokument gällande säkerhet finns upprättade hos leverantören som PUA tagit del av.
O20	(Leverantörens namn) har utsett informationssäkerhetsansvarig	Leverantören har utsett en informationssäkerhetsansvarig som PUA fått kontaktuppgifter till samt kan kontakta vid behov.
O21	Sekretessavtal	Vid användning av tjänster/information finns ett sekretessavtal framtaget
O22	Säkra lokaler	Områden som upprättats för att minska avbrott eller störningar
O23	Intern tillsyn	Rutiner för kontroller av att implementerade åtgärder är effektiva
O24	Leverantörskontroller	Rutiner för återkommande leverantörskontroller under avtalstiden

Göteborgs Stad

Azure AD

Funktionsbeskrivning gällande teknisk säkerhet och dataskydd

2023-05-19

Tjänsteägare: NN

Versionshantering av detta dokument

Datum	Version	Beskrivning	Ändrat av
2022-12-09	0.1	Skapat ett första utkast	Marcus Broman
2022-12-12	0.2	Skapat ett andra utkast där funktioner är separerade från tjänsten	Marcus Broman
2022-12-14	0.3	Uppdaterad och integrerat info efter avstämning med FA	Marcus Broman
2023-05-18	0.4	Korrigerat innehåll för samstämmighet med andra dokument	Marcus Broman

Innehåll

1 Dokumentets syfte 4
1.1 Allmänt 4
1.2 Ägarskap och dokumenthantering 4
2 Funktionsbeskrivning 5
2.1 Övergripande beskrivning av funktionen 5
2.1.1 Tillgängliga plattformar 6
2.2 Datatyper som hanteras inom funktionen 6
2.2.1 Personuppgiftsflöde 8
2.2.2 Gästkontohantering 8
2.3 Beroenden 9
2.4 Säkerhetsåtgärder 9
2.4.1 Azure AD tekniska säkerhetsåtgärder 10
2.4.2 Azure AD administrativa säkerhetsåtgärder 10
3 Bilagor 10
4 Referenser ..... Fel! Bokmärket är inte definierat.

1 Dokumentets syfte

En *funktionsbeskrivning* dokumenterar underliggande säkerhets och dataskyddsaspekter till en *Tjänstespecifikation*.

Två nivåer av dokumentation:

1. Tjänstespecifikation (kopplad till Intraservice tjänst - övergripande)
2. Funktionsbeskrivning (underliggande funktion som kan ingå i flera tjänster)

Funktionsbeskrivningen kan återanvändas för olika syften och för att förklara aspekter på säkerhet och dataskydd i en tjänsts funktion som Intraservice tillhandahåller.

1.1 Allmänt

Detta dokument är skapat med utgångspunkt att stödja stadens bolag och förvaltningar i olika bedömningar, ställningstaganden och utredningar gällande informationssäkerhet och dataskydd. Dokumentet uppdateras löpande.

1.2 Ägarskap och dokumenthantering

TBD

2 Funktionsbeskrivning

2.1 Övergripande beskrivning av funktionen

Azure Active Directory (Azure AD) är en molnbaserad plattform för identitets- och åtkomsthantering. Funktionen syftar till att tillhandahålla identitetshantering och behörighetsstyrning för de tjänster som tillhandahålls inom ramen för Azure och möjliggör anställda att komma åt externa resurser som exempelvis Office 365.

Azure AD är en så kallad Identity as a service (IdaaS) lösning som agerar som en sammanhållande mekanism i Microsofts molntjänster. Azure AD är beroende av att behandla data i klartext för att funktionen ska fungera. Detta innebär att Azure AD behöver tillgång till krypteringsnycklar och att en extern styrning och innehav av en krypteringsnyckel inte stöds av Microsoft i Azure AD-funktionen. Azure AD möjliggör även för hantering av användare genom att enkelt kunna addera, uppdatera och radera användare, managera enheter samt hantera tillstånd och behörigheter.

Verktyget som används för detta heter Azure AD Connect. Vad som synkroniseras styrs av ett regelverk i verktyget som baseras på kravet för systemet som hämtar informationen.

Synkade konton: Användarkonton i stadens AD som ska ha tillgång till tjänster i Office 365. Dessa konton skapas i vårt on-premise AD (staden.gotheborg.net) och sedan synkroniseras till Azure AD.

Gästkonton: Gästkonton används för att ge externa (användare som inte finns i Göteborgs stads katalogtjänst, exempelvis anställd/konsult från annan organisation) användare tillgång till information i stadens Office 365 miljö.

Cloud-only: Dessa konton skapas direkt i Azure AD (funktionskonton, delade brevlådor mm.)

App registrering: Programhantering i Azure Active Directory (Azure AD) är en process för att skapa, konfigurera program i molnet. Upplägg sker enligt fastställt regelverk.

SSPR (Self Service Password Reset): Återställning av lösenord via självbetjäning

Azure AD Connect: Synkroniserar information som behövs för att leverera tjänsten Office 365.

2.1.1 Tillgängliga plattformar

Azure AD är en onlinetjänst som finns hos Microsoft i molnet.

2.2 Datatyper som hanteras inom funktionen

Staden definierar fyra olika typer av data med personuppgifter i hanteringen för att leverera en IT tjänst.

- **Innehållsdata**: Den data som användare skapar genom att använda tjänsten.
- **Gemensamma innehållsdata**: Användarinformation, gemensamma metadatastrukturer, visualisering av organisation
- **Funktionella data**: Konfigurationsdata, inloggningsdata och metadata för att användare ska kunna anslutas till tjänsten.
- **Diagnosdata**: Loggar om användningen för felsökning, säkerhet och spårbarhet. Intraservice som tjänsteleverantör och/eller leverantör samlar in och lagrar diagnosdata

De datatyper som hanteras inom Azure AD skapas av staden och härleds från Personec:

Gemensamma innehållsdata (kontodata) så som e-post, telefonnummer, för- och efternamn, jobbtitel, avdelning och information om chefer samt inloggningstider

Azure AD hanterar olika typer av metadata i syfte att säkerställa funktionalitet av funktionen:

Funktionsdata konfigurationsdata för komponenter som finns vid överföring av elektronisk kommunikation. Data raderas eller anonymiseras direkt efter slutförandet av överföringar i linje med reglerna i ePrivacy-direktivet. Direktivet är införlivat med svensk lag genom *Lag (2022:482) om elektronisk kommunikation.*

Funktionsdata hanteras i Azure AD hanteras i syfte att säkerställa de grundläggande funktionerna, här ingår exempelvis identiteter och inloggnings-/autentiseringsinformation, konfigurationsinformation och accessrättigheter.

Diagnosdata behandlas inom Azure AD för tre specifika syften: för att kunna tillhandahålla och förbättra funktionen, för att uppdatera funktionen samt för att hålla Azure AD säkert. Microsoft behandlar

diagnosdata i rollen som ett personuppgiftsbiträde och enbart för de tre specifika syftena.

Skillnaden mellan funktionsdata och diagnostiska data är att funktionella data är tillfällig. Så länge funktionella data inte lagras, eller om uppgifterna inte är personliga uppgifter under insamlingen (t.ex. exempeldata om temperaturen på en CPU i en server), är de inte diagnostiska data.

Tabell 2-1: Lista över personuppgifter inom funktionen

<table>
<tr><th>Datatyp</th><th>Personuppgifter</th><th>Användning</th></tr>
<tr><td>Gemensamma innehållsdata</td><td>Användarinformation som härrör från HR system och Skatteverkets befolkningsregister. Exempel på gemensamma innehållsdata är kontaktkort från Active Directory (AD), gemensamma metadatastrukturer, visualisering av organisation.

Förnamn, efternamn, titel/befattning, organisation (endast förvaltning)Data från Azure AD:

<table>
<tr><th>Fält</th><th>Vad visas</th></tr>
<tr><td>Displayname</td><td>Förnamn + Efternamn</td></tr>
<tr><td>First name</td><td>Förnamn</td></tr>
<tr><td>Last name</td><td>Efternamn</td></tr>
<tr><td>User principle name</td><td>e-postadress</td></tr>
<tr><td>Job title</td><td>Förvaltningsnamn</td></tr>
<tr><td>Company name</td><td>Förvaltningsnamn</td></tr>
<tr><td>Department</td><td>Förvaltningsnamn</td></tr>
<tr><td>Manager</td><td>Chef</td></tr>
<tr><td>Email</td><td>e-postadress</td></tr>
</table></td><td>Gemensamma innehållsdata nödvändigt att behandla inom funktionen för användarinformation och visualiseringar av organisationen.</td></tr>
<tr><td>Funktionella data</td><td>Exempel på funktionella data är den dataström som krävs för att användaren ska eller verifiera om användaren har en giltig licens.</td><td>Funktionella data är nödvändigt för leverantören att behandla iför att säkerställa att de grundläggande funktionerna i Sharepoint samt säker åtkomst</td></tr>
<tr><td>Diagnost kdata</td><td>Diagnostiska data innehåller teknisk information

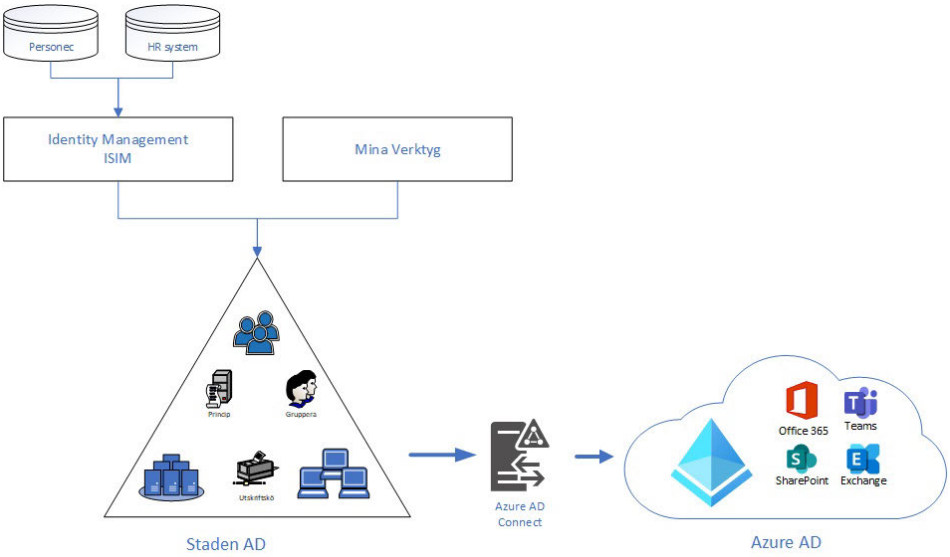
Dessa data omfattar inte användarens namn eller e-postadress eller innehållet i användarens filer.

Obligatoriska diagnostikdata är den minsta mängd data som är nödvändig för att hålla Office säkert och uppdaterat och som ser till att det fungerar som förväntat på den.</td><td>Diagnostikdata samlas inte in via Azure AD

Om dessa onlinetjänster nås via klientprogramvara, samlas diagnost kdata samlas den lokalt installerade programvaran in med inställningen: Endast Obligatoriska diagnostikdata enhet där det är installerat.[1]</td></tr>
</table>

[1] Mer information om diagnostiska data: https://docs.microsoft.com/deployoffice/privacy/required-diagnostic-data. Se även bilaga 2 *Rapport – Analys av Microsofts hantering av diagnostikdata – underlag för konsekvensbedömning*

2.2.1 Personuppgiftsflöde



Personuppgifter flödar igenom Azure AD enligt:

1. Uppgifter Skatteverket överförs uppgifter till Personec.
2. Stadens AD hämtar sedan de uppgifterna från Personec.
3. Azure AD hämtar uppgifter från stadens AD med hjälp av synkroniseringsmotorn Azure AD Connect.
4. Uppgifter från Azure AD används till Office 365 eller andra tekniska funktioner.

2.2.2 Gästkontohantering

Det finns två typer av gästkonton i Azure AD, ägarstyrda och managerade. Båda typer hanteras endast i Azure AD och har ingen koppling tillbaka till stadens AD.

Ägarstyrda gästkonton kan skapas manuellt av medarbetare i Göteborgs Stad. Ägare avser personen som skapar gästkontot, och ägarens namn blir registrerat som gästens chef. För ägarstyrda gästkonton hanteras endast gästens namn och e-postadress i Azure AD. Ett ägarstyrt gästkonto är aktiverat i ett år, därefter skickas ett e-postmeddelande till gästkontots chef som får möjlighet att förlänga gästkontot. Gästen kan själv välja att ta bort sitt ägarstyrda gästkonto. Mer information om ägarstyrda gästkonton finns beskrivet i dokumentet *Gästanvändare i Azure AD*.

Managerade gästkonton hanteras automatiskt genom provisionering, en eller flera källor styr skapandet och livscykeln för gästkontot. Källan kan exempelvis vara ett externt bolags Azure AD. Lösningen är framtagen för att kunna hantera de behov som verksamheter inom Göteborgs Stad har med avseende på gästkontoprovisionering.

Gästanvändare skapas, uppdateras och tas bort utefter förändringar på det kopplade källkontot. Om ett ägarstyrt gästkonto redan finns för en källanvändare kommer detta att övertas av lösningen för managerade

gästkonton och ägaren tas bort. Detta gäller inte gästkonton som skapats manuellt av en administratör, dessa konton förblir manuellt hanterade.

Huvudsakligen baseras källor för managerade gästkonton på externa Azure AD-instanser, men i de fall verksamheten eller bolaget ej använder Azure AD kan även en json-fil användas som källa. Mer information om managerade gästkonton finns beskrivet i dokumentet *Hanterad gästkontoprovisionering*.

Tabellen nedan visar vilka personuppgifter som hanteras för ägarstyrda och managerade gästkonton.

Fält	Vad visas	Ägarstyrt gästkonto	Managerat gästkonto
Displayname	Förnamn + Efternamn	X	X
First name	Förnamn		X
Last name	Efternamn		X
User principle name	E-postadress	X	X
Manager	Chef	X	
Job titel	Titel		X
Company name	Förvaltning-/bolagsnamn		
Department	Avdelning		
Email	e-postadress	X	

2.3 Beroenden

Beroenden är obligatoriska för att funktionerna i Sharepoint, Onedrive och Delve ska fungera.

Funktion	Beroende	Peronsuppgifter	Syfte
Azure AD	Stadens AD	**Fält** / **Vad visas** Displayname: Förnamn + Efternamn First name: Förnamn Last name: Efternamn User principle name: e-postadress Job title: Förvaltningsnamn Company name: Förvaltningsnamn Department: Förvaltningsnamn Manager: Chef Email: e-postadress	Active Directory (stadens AD) är källan till information om användarna. Dessa används sedan i Office grupper för att ge tillgång till funktioner samt sätta behörigheter. Azure AD connect används för att hämta personuppgifter till Azure AD. Personuppgifter som hämtas beskrivs i tabellen

2.4 Säkerhetsåtgärder

Azure AD har såväl tekniska som administrativa säkerhetsåtgärder implementerade. Funktionens säkerhetsåtgärder följer de som

implementerats för Microsoft Office 365 i dokumentet *Tjänstespecifikation Office 365*.

2.4.1 Azure AD tekniska säkerhetsåtgärder

Ytterligare specifika tekniska säkerhetsåtgärder har implementerats i funktionen Azure AD utöver de som finns generellt M365-tjänsten:

- *Autentisering* sker genom en kontroll av den uppgivna identiteten genom exempelvis personligt lösenord.
- *Flerfaktorsautentisering* (MFA) finns implementerat med krav på två eller fler former av information som styrker den uppgivna identiteten.
- Conditional Access (Villkorad åtkomst): Åtkomst regler som kombinerar ett antal faktorer för att ge åtkomst eller neka åtkomst.
- PIM (Privileged Identity Management): Funktion som möjliggör aktivering av tilldelade behörigheter vid behov.
- *Loggning* skapar en förteckning över händelser i tjänsten. Detta innebär att vi kan ha spårbarhet och uppfylla stadens krav på detta. Vem som gör vad i Office 365 miljön.
- SOC monitorering: Integrerat med SOC teamets övervaknings verktyg.
- Blockerat möjligheten för användaren att själva registrera appar i Azure AD.

Utöver dessa åtgärder finns specifika tekniska IT-säkerhetsåtgärder som IT-administratörer kan införa för funktionen.[2]

2.4.2 Azure AD administrativa säkerhetsåtgärder

Ytterligare administrativa säkerhetsåtgärder har implementerats i funktionen Azure AD utöver de som finns generellt M365-tjänsten:

- Rolltilldelning: Sker via formulär i Serviceportalen och kräver attest.

3 Bilagor

Dokumentnamn	Version	Beskrivning
Rapport – Analys av Microsofts hantering av diagnost kdata – underlag för konsekvensbedömning	1.0	

Tabell 5-1: Lista över bilagor

[2] Mer information om åtgärder som kan användas (på Engelska): https://learn.microsoft.com/sv-se/sharepoint/get-started-new-admin-center

Göteborgs Stad

OneDrive och SharePoint

Funktionsbeskrivning gällande teknisk säkerhet och dataskydd

2023-05-19

Tjänsteägare: <Funktion>

Versionshantering av detta dokument

Datum	Version	Beskrivning	Ändrat av
2023-03-20	0.1	Skapat ett första utkast	Mikael Schou Maegaard, Robert Hansson
2023-05-18	0.2	Korrigerat innehåll för samstämmighet med andra dokument	Marcus Broman

Innehåll

1 Dokumentets syfte ... 4
1.1 Allmänt ... 4
1.2 Ägarskap och dokumenthantering ... 4
2 Funktionsbeskrivning ... 5
2.1 Övergripande beskrivning av funktionen ... 5
2.1.1 Tillgängliga plattformar ... 5
2.2 Datatyper som hanteras inom funktionen ... 5
2.2.1 Personuppgiftsflöde ... 7
2.3 Beroenden ... 8
2.4 Allmänt beskrivna säkerhetsåtgärder ... 8
3 Bilagor ... 9
Appendix 1 - Säkerhetsåtgärder ... 9
Tekniska säkerhetsåtgärder ... 9
Organisatoriska säkerhetsåtgärder ... 11

1 Dokumentets syfte

En *funktionsbeskrivning* dokumenterar underliggande säkerhets och dataskyddsaspekter till en *Tjänstespecifikation*.

Två nivåer av dokumentation:

1. Tjänstespecifikation (kopplad till Intraservice tjänst - övergripande)
2. Funktionsbeskrivning (underliggande funktion som kan ingå i flera tjänster)

Funktionsbeskrivningen kan återanvändas för olika syften och för att förklara aspekter på säkerhet och dataskydd i en tjänsts funktion som Intraservice tillhandahåller.

1.1 Allmänt

Detta dokument är skapat med utgångspunkt att stödja stadens bolag och förvaltningar i olika bedömningar, ställningstaganden och utredningar gällande informationssäkerhet och dataskydd. Dokumentet uppdateras löpande.

1.2 Ägarskap och dokumenthantering

<Lämna tomt>

2 Funktionsbeskrivning

2.1 Övergripande beskrivning av funktionen

Sharepoint Online är en funktion för att spara, dela och samarbeta med dokument och data. Onedrive är personlig Sharepoint som ger medarbetare en egen lagringsplats för dokument och innehåll, som kan delas. Här sparas alla filer i O365. Arbete i Teams sparas det i Sharepoint, som är lagringsplatsen för filerna.
Utöver att vara den primära lagringsplatsen för Microsoft 365 tjänsten så tillhandahåller den också en samarbetsyta som kan ta formen av en intern webbsida med en mängd funktioner som verksamheterna kan välja att använda. Alla följer behörighets och säker regelverket vi har för övriga delar i tjänsten.
Servrar är Microsofts datacenter i Sverige där filerna är krypterade under förflyttning och när dom lagras på disk. Alla filer finns speglade i minst två olika datacenter för att ge hög tillgänglighet och skydda från dataförlust. Dessutom finns en versionshantering som ger upp till 500 olika versioner av filen som användarna han återskapa data från. Skulle en fil tas bort av misstag så går den att återskapa i 3 månader.

Delve är ett presentationsgränssnitt som tillhandahåller möjligheten att kunna se andras dokument en användare har tillgång till och baseras på hens behörigheter Sharepoint Online och Onedrive. Delve ger även en visualisering av organisationstillhörighet.

2.1.1 Tillgängliga plattformar

Valfri webbläsare och mobil app. Onedrive för företag finns installerat som en programvara på Stadens datorer och har tillsyfte att synkronisera filer från Onedrive i molnet lokalt till datorn.

2.2 Datatyper som hanteras inom funktionen

Staden definierar fyra olika typer av data med personuppgifter i hanteringen för att leverera en IT tjänst.

- **Innehållsdata**: Den data som användare skapar genom att använda tjänsten.
- **Gemensamma innehållsdata**: Användarinformation, gemensamma metadatastrukturer, visualisering av organisation
- **Funktionella data**: Konfigurationsdata, inloggningsdata och metadata för att användare ska kunna anslutas till tjänsten.
- **Diagnosdata**: Loggar om användningen för felsökning, säkerhet och spårbarhet. Intraservice som tjänsteleverantör och/eller extern leverantör samlar in och lagrar diagnosdata

Innehållsdata
Är de datatyper som hanteras inom funktionen. Innehållsdata kan skapas av såväl staden som slutanvändaren. Exempel på innehållsdata är dokument, bildfiler, videor, uppgiftslistor etcetera. Omfattningen är vanligtvis beroende av hur medarbetaren väljer att använda funktionaliteten eller av hur systemadministratörer konfigurerar funktioner. Även metadata kopplat till filer och annat innehåll räknas som innehållsdata i funktionen, exempelvis data gällande versionshistorik, ändrandedatum samt skapat av.

Gemensamma innehållsdata
Kan vara information som kommer från stadens gemensamma identitetshantering, Active Directory (AD). Informationen är gemensam i staden och kan användas i funktionen för att exempelvis kunna visualisera organisation, hantera metadatastrukturer eller tillhandahålla autentisering. Exempel på gemensamma innehållsdata som är personuppgifter är kontaktkort som innefattar fullständigt namn, e-postadress, chef och förvaltning. Användare kan även själv addera information som exempelvis mobiltelefonnummer.

Funktionella data
Konfigurationsdata för komponenter som finns vid överföring av elektronisk kommunikation.

Skillnaden mellan funktionsdata och diagnostiska data är att funktionella data är tillfällig. Så länge funktionella data inte lagras, eller om uppgifterna inte är personliga uppgifter under insamlingen (t.ex. exempeldata om temperaturen på en CPU i en server), är de inte diagnostiska data.

Diagnosdata
Det kan förekomma att Intraservice som tjänsteleverantör och/eller leverantör av *Software as a Service* (SaaS) tjänst samlar in och lagrar data om den individuella användningen av tjänstens IT-stöd.

Datatyp	**Personuppgifter** **Personuppgifter är all slags information som direkt eller indirekt kan knytas till en person. Exempelvis namn, personnummer IP-adress mm.**		**Användning**
Gemensamma innehållsdata	**Gemensamminnehållsdata typ**	**Personuppgift**	
	Displayname	Förnamn + Efternamn	
	First name	Förnamn	
	Last name	Efternamn	
	User principle name	e-postadress	
	Job title	Förvaltningsnamn	
	Company name	Förvaltningsnamn	

	Department	Förvaltningsnamn	
	Manager	Chef	
	Email	e-postadress	
Funktionella data	**Funktionsdatatyp**	**Personuppgift**	
Diagnostikdata	**Diagnostikdatatyp**	**Personuppgift**	
	Det är samma obligatoriska diagnostik data som skickas med Onedrive för företag som för de andra appl kationer som ingår i Microsoft Apps for Enterprise paketet.		

Tabell 1: Lista över personuppgifter inom funktionen

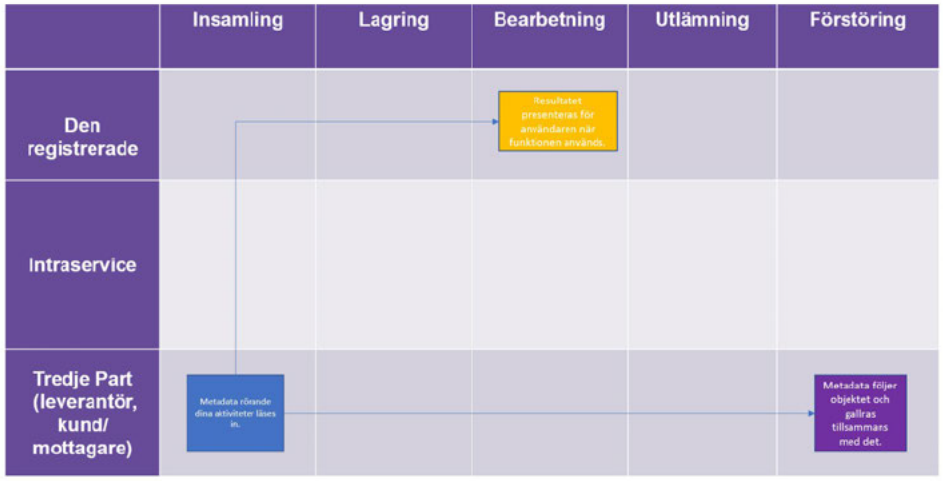
2.2.1 Personuppgiftsflöde

2.2.1.1 Delve och liknande SharePoint funktioner

Sammanställning av filer, personer och grupper som kan vara intresserad av görs i flera olika funktioner där SharePoint och OneDrive är den bakomliggande källan. Gemensamt med alla dessa är att man aldrig ser mer än vad rättigheter medger. Vyn är baserad på personlig information och visas inte för någon annan.

- Insamling (inkl. registrering och organisering)
  - Metadata rörande dina aktiviteter läses in.
- Lagring (inkl. loggning)
  - Ingen extra lagring av uppgifter görs.
- Bearbetning (inkl. ändring, användning)
  - Resultatet presenteras för användaren när funktionen används.
- Utlämning (spridning eller annan typ av tillhandahållande av uppgifterna, sammanställning eller samkörning)
  - Ingen utlämning av uppgifter görs.
- Förstöring
  - Metadata följer objektet och gallras tillsammans med det.

Delve och liknande SharePoint funktioner



2.3 Beroenden

<Beskriv de beroenden funktionen har till andra tjänster eller funktioner, exempelvis Active directory, Personec eller externa datakällor>

Funktion	Beroende	Syfte
Azure Ad	IDM	Azure AD är källan till användarna.

Tabell 2: Lista över beroenden

2.4 Tekniska säkerhetsåtgärder

<Beskriv vidtagna säkerhetsåtgärder i funktionen som syftar till att skydda personuppgifterna. Se appendix 1.>

Säkerhetsåtgärder	Beskrivning
<Säkerhetsåtgärdens namn>	<Beskrivning>
T1 Behörighetskontroll	När en användare delar ett dokument från Sharepoint eller Onedrive skickas ett meddelande till en funktionsbrevlåda.
T9 Riktlinje för driftsäkerhet	Vi har inaktiverat möjligheten att ladda ner skadliga filer i Sharepoint och Onedrive. Det syns om en fil är skadlig och det går inte att öppna, flytta, kopiera eller dela filen.

Tabell 3: Lista över tekniska säkerhetsåtgärder

2.5 Organisatoriska säkerhetsåtgärder

<Beskriv vidtagna säkerhetsåtgärder i funktionen som syftar till att skydda personuppgifterna. Se appendix 1.>

Säkerhetsåtgärder	Beskrivning
<Säkerhetsåtgärdens namn>	<Beskrivning>

Tabell 4: Lista över organisatoriska säkerhetsåtgärder

3 Bilagor

Dokumentnamn	Version	Beskrivning

Tabell 5: Lista över bilagor

Appendix 1 - Säkerhetsåtgärder

Nedan lista på allmänt beskrivna tekniska och organisatoriska säkerhetsåtgärder är övergripande beskrivet och kan användas för beskrivningar.[1]

Tekniska säkerhetsåtgärder

Nr	Tekniska åtgärder	Definition
T1	Behörighetskontroll	Att förhindra att obehörig användning eller åtkomst. Exempelvis genom bekräftning av identiteter, personligt lösenord, engångslösenord eller biometriska metoder.
T2	Behandlingshistorik	Åtkomst till personuppgifter kan kontrolleras genom att behandlingshistorik sparas under en specificerad tid.
T3	Avidentifiering	Omöjliggör återidentifieringen av en individ.
T4	Kryptering	Åtgärder för att personliga data är obegriplig för obehöriga. Se även asymmetrisk och symmetrisk kryptering.

[1] Listan är sammanställd med hjälp av *Säkerhet för personuppgifter – Datainspektionen allmänna råd* (Integritetskyddsmyndighetens, IMY:s tidigare namn) samt en taxonomi i *Privacy Impact Assessment (PIA) – PIA guides samt PIA Software* av IMY:s franska motsvarighet Commission Nationale Informatique & Libertés (CNIL).

T5	Dataseparering	Separering av information, och enbart ge åtkomst till de data som är nödvändigt
T6	Logisk åtkomstkontroll	Definierar begränsning av åtkomst till data genom vem som ska ha åtkomst till information, när och under vilka omständigheter. Exempelvis genom tekniker för cybersäkerhet såsom identifiering, autentisering och auktorisering.
T7	Loggning	Dokumentering av behandlingar som utförs i ett system för att identifiera obehörig åtkomst, missbruk eller liknande.
T8	Dataminimering	Lagrade/behandlade personuppgifter minimeras genom exempelvis filtrering och borttagning, minskning av datainsamling eller begränsning av datatillgång.
T9	Riktlinjer för driftsäkerhet	Styrande dokument som begränsar sannolikheten för risker mot fysisk utrustning, exempelvis dokumentation av driftsförvaranden, inventering och uppdatering av program- och hårdvara, redundans av data, begränsning av fysisk tillgång till servrar etc.
T10	Skydd av webbplats	Metoder för att minska möjligheten att webbplatser utnyttjas för att kränka personuppgifter. Exempelvis allmänna säkerhetsrutiner, SSL-kryptering, cookiepolicy, säkerhetsuppdateringar)
T11	Säkerhetskopiering	Dokumenterad säkerhetskopieringsrutin/back-uprutin för att säkerställa tillgänglighet, integritet och konfidentialitet
T12	Policy för underhåll av utrustning	Styrande dokument som tydliggör förekomst av fysiskt underhåll av utrustning samt eventuellt specificerar om/hur leverantörer kan användas. Inkluderar även reglering av fjärrskrivbord samt hantering av kasserat material.
T13	Policy för nätverkssäkerhet	Styrande dokument gällande vilken typ av nätverk som behandlingen ska utföras på. Inklusive tydliggörande av adekvata skyddssystem exempelvis brandväggar, intrångsdetektering samt aktiva eller passiva metoder för att nätverkets säkerhet.
T14	Fysisk åtkomstkontroll	Begränsning av åtkomsten till en fysisk plats. Exempelvis genom lås och nycklar, lösenordskyddade dörrar, vakter, zonindelning eller ID-brickor.
T15	Spårbarhet	Dokumentering av vem som lagt till, ändrat eller tagit bort information i ett system
T16	Pseudonymisering	Ersätter identifierande information med en pseudonym. Kodnyckeln lagras på en separat plats (även kallad för anonymisering)
T17	Segmentering av personuppgifter	Metoder för att minska möjligheten att korrelera eller härleda personuppgifter till en individ. Exempelvis begränsa personuppgifter till sektioner/enheter eller logisk separering
T18	Filtrering och radering	Rutiner för borttagning av överflödiga metadata vid import av data, exempelvis EXIF-data som är kopplade till en bildfil.
T19	Kryptering vid överföring	Kryptering av all trafik vid överföring av uppgifter.
T20	Kryptering vid vila	Kryptering vid lagring av information
T21	Autentisering	Kontroll av den uppgivna identiteten, exempelvis genom personligt lösenord
T22	Flerfaktorsautentisering (MFA)	Krav på två eller fler former av information som styrker den uppgivna identiteten

T23	Patchning	Regelbundna mjukvaruuppdateringar av programvara i syfte att upprätthålla säkerheten.

Organisatoriska säkerhetsåtgärder

Nr	Organisatoriska åtgärder	Definition
O1	Låsutrustning	Tillgång till utrustning som möjliggör att låsa/låsa in uppgifter och därmed enbart blir tillgängliga med nyckel
O2	Inpasseringskontroll	Fysiska hinder för obehöriga att få åtkomst till verksamhetens lokaler och information.
O3	Larmutrustning	Larmutrustning som kan detektera inbrott, brand och andra oönskade händelser.
O4	Säkerhetsskåp	Ett skåp som vid provning under minst 10 minuter, ska stå emot angrepp, enligt Svensk standard SS 2492/SSF 3492.
O5	Tillträdeskontroll	Att säkerställa att enbart behörig personal får tillträde till utrymmen där IT-utrustning genom exempelvis upprättandet av rutiner för tillträdeskontroll.
O6	Lösenordspolicy	Styrande dokument som tydliggör användares lösenords längd, tecken samt automatisk begäran om byte av lösenord.
O7	Informationssäkerhetspolicy	Styrande dokument som tydliggör den personuppgiftsansvarigas informationssäkerhetsarbete, implementerade åtgärder och instruktioner gällande arbetssätt.
O8	Rutin för distansarbete	Styrande dokument som tydliggör hur verksamhetens information ska hanteras utanför den kontrollerande nätverks- och kontorsmiljön.
O9	Arkivering	Uppgifter som inte används i vardagligt arbete arkiveras i säkra arkiv.
O10	Policy för hantering av pappersdokument	Instruktioner och tydliga arbetssätt för medarbetare att förhålla sig till vid hantering av pappersdokument med personuppgifter
O11	Policy för arbetsstationshantering	Styrande dokument som tydliggör arbetssätt gällande arbetsstationer för att minska möjligheten att mjukvaror kan utnyttjas. Exempelvis mjuvaruuppdateringar, fysiskt skydd och åtkomstkontroll, arbete på ett krypterat nätverk, integritetskontroller och loggning)
O12	PUB-avtal	Personuppgiftsbiträdesavtal. Dokumentation på överenskommelse mellan PUA och PUB gällande säkerhetspolicy, instruktioner till PUB samt planerade åtgärder så som säkerhetsrevisioner. PUB-avtal definierar hur PUB ska hantera personuppgifter samt de säkerhetsåtgärder som ska implementeras.
O13	Implementerad dataskyddsorganisation	Tydlig dataskyddsorganisation om verksamheten som arbetar med samt följer upp dataskyddsarbetet och behandlingar.
O14	Integritetspolicy och riktlinjer	Styrande dokument som reglerar integritetsskyddsfrågor inom verksamheten.
O15	Implementerad och förankrad process för PUI	Arbetssätt för att identifiera, rapportera och hantera personuppgiftsincidenter i verksamheten. Inklusive utpekat ansvar för hantering, implementering av åtgärder samt anmälan till tillsynsmyndighet.

O16	Regler för kunskapshöjning och utbildning	Regelbundna utbildningar för samtliga medarbetare gällande dataskydd och informationssäkerhet
O17	Hantering av tredjeparter	Dokumenterat arbetssätt gällande hantering av behandlingar som inkluderar tredjeparter. Inklusive identifiering av tredjepart, skrivande av PUB-avtal och andra avtalsmässiga åtgärder.
O18	Rutin för tillsyn av integritetsskyddande åtgärder	Regelbundna granskningar och tillsyner (interna och externa) som ger en övergripande bild av dataskyddsarbetet och efterlevnaden av GDPR.
O19	Riktlinjer för säkerhet finns hos (leverantörens namn)	Styrande dokument gällande säkerhet finns upprättade hos leverantören som PUA tagit del av.
O20	(Leverantörens namn) har utsett informationssäkerhetsansvarig	Leverantören har utsett en informationssäkerhetsansvarig som PUA fått kontaktuppgifter till samt kan kontakta vid behov.
O21	Sekretessavtal	Vid användning av tjänster/information finns ett sekretessavtal framtaget
O22	Säkra lokaler	Områden som upprättats för att minska avbrott eller störningar
O23	Intern tillsyn	Rutiner för kontroller av att implementerade åtgärder är effektiva
O24	Leverantörskontroller	Rutiner för återkommande leverantörskontroller under avtalstiden

Göteborgs Stad

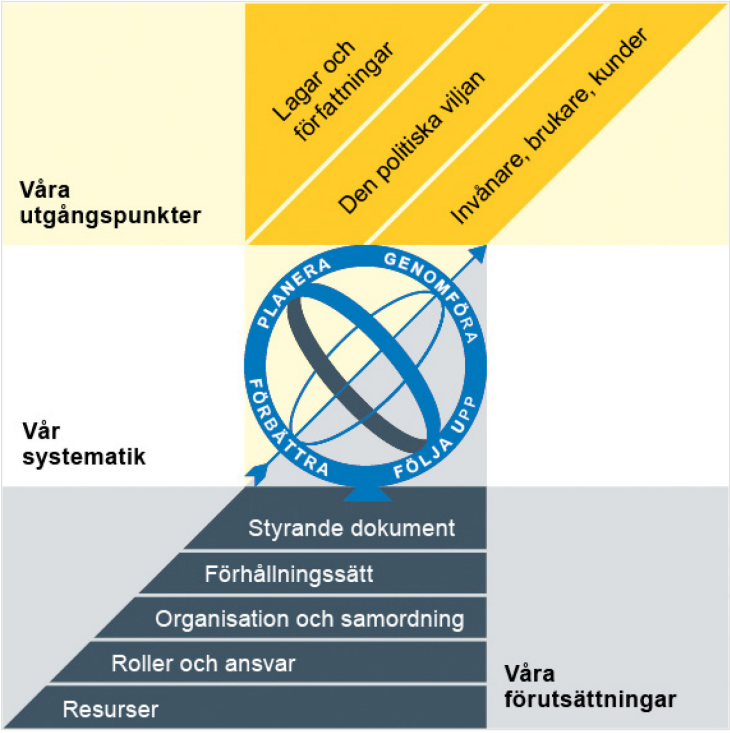
Göteborgs Stads riktlinje för informationssäkerhet

Reglerande styrande dokument

Policy
► **Riktlinje**
Regel
Anvisning
Rutin
Instruktion

Göteborgs Stads styrsystem

Utgångspunkterna för styrningen av Göteborgs Stad är lagar och författningar, den politiska viljan och stadens invånare, brukare och kunder. För att förverkliga utgångspunkterna behövs förutsättningar av olika slag. Stadens politiker har möjlighet att genom styrande dokument beskriva hur de vill realisera den politiska viljan. Inom Göteborgs Stad gäller de styrande dokument som antas av kommunfullmäktige och kommunstyrelsen. Därutöver fastställer nämnder och bolagsstyrelser egna styrande dokument för sin egen verksamhet. Kommunfullmäktiges budget är det övergripande och överordnade styrande dokumentet för Göteborgs Stads nämnder och bolagsstyrelser.

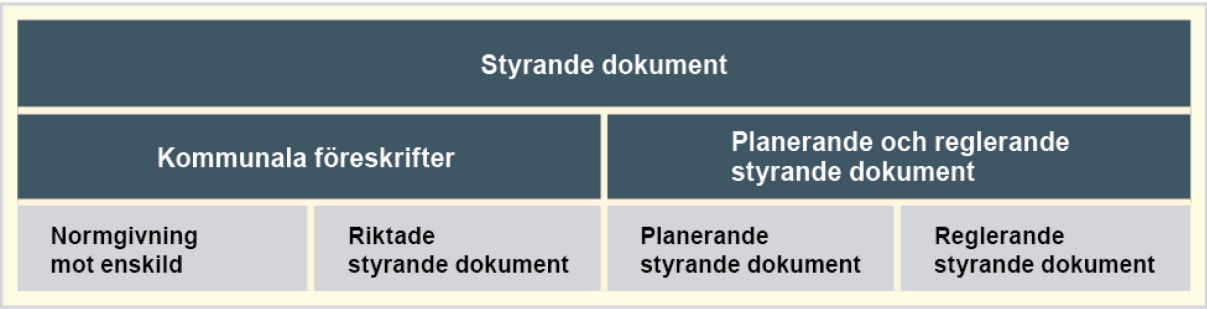


Om Göteborgs Stads styrande dokument

Göteborgs Stads styrande dokument är våra förutsättningar för att vi ska göra rätt saker på rätt sätt. De anger vad nämnder/styrelser och förvaltningar/bolag ska göra, vem som ska göra det och hur det ska göras. Styrande dokument är samlingsbegreppet för dessa dokument.

Stadens grundläggande principer såsom demokratisk grundsyn, principer om mänskliga rättigheter och icke-diskriminering omsätts i praktisk verksamhet genom att de integreras i stadens ordinarie beslutsprocesser. Beredning av och beslut om styrande dokument har en stor betydelse för förverkligandet av dessa principer i stadens verksamheter.

De styrande dokumenten ska göra det tydligt både för organisationen och för invånare, brukare, kunder, leverantörer, samarbetspartners och andra intressenter vad som förväntas av förvaltningar och bolag. De styrande dokumenten ligger till grund för att utkräva ansvar när vi inte arbetar i enlighet med vad som är beslutat.



Dokumentnamn: Göteborgs Stads riktlinje för informationssäkerhet			
Beslutad av: Kommunfullmäktige	Gäller för: Stadens nämnder och styrelser	Diarienummer: 0540/14 (0110/19)	Datum och paragraf för beslutet: 2013-09-05, § 21
Dokumentsort: Riktlinje	Giltighetstid: Tillsvidare	Senast reviderad: 2019-12-16	Dokumentansvarig: Informationssäkerhetschef
Bilagor: [Bilagor]			

Innehåll

Inledning 3

Syftet med denna riktlinje 3

Vem omfattas av riktlinjen 3

Koppling till andra styrande dokument 3

Riktlinje 4

Inledning 4

Klassning av information 4

Hantering av informationstillgångar 4

Personalresurser och säkerhet 5

Fysisk och miljörelaterad säkerhet 5

Styrning av kommunikation och drift 5

Styrning av åtkomst 6

Anskaffning, utveckling och underhåll 6

Hantering av incidenter 6

Kontinuitetsplanering i verksamheten 6

Uppföljning av säkerhetsnivå 7

Definitioner 7

Inledning

Syftet med denna riktlinje

Denna riktlinje syftar till att konkretisera säkerhetspolicyn avseende informationssäkerhetsområdet. Med informationssäkerhet avses att upprätthålla:

- Konfidentialitet, informationstillgångar är tillgängliga endast för behöriga
- Riktighet, informationstillgångar förändras eller påverkas inte oönskat eller utom kontroll
- Tillgänglighet, informationstillgångar kan nyttjas efter behov i förväntad utsträckning och inom önskad tid

Med informationstillgångar avses all information och informationshanterande resurser såsom manuella samt digitaliserade och IT-baserade informationssystem

Vem omfattas av riktlinjen

Denna riktlinje gäller tillsvidare för Stadens nämnder och styrelser.

Koppling till andra styrande dokument

Riktlinjen konkretiseras i underliggande regler.

Riktlinje

Inledning

Denna riktlinje beskriver den grundsäkerhetsnivå som gäller för all informationshantering i Göteborgs Stad som blivit klassad i nivå 1 för ett eller flera av skyddsområdena konfidentialitet, riktighet eller tillgänglighet.

För informationshantering som blivit klassad i nivå 2 och som därmed har ett utökat skyddsbehov ska kompletterande åtgärder införas. Dessa skyddsåtgärder utformas specifikt och tas ej upp i denna riktlinje.

För information som klassats i nivå 0 avseende alla de tre skyddsområdena konfidentialitet, riktighet eller tillgänglighet finns inga stadsövergripande krav på skyddsåtgärder.

Klassning av information

- Informationsklassning ska göras kontinuerligt av informationsägaren
- Informationslassningen ska ligga till grund för hur informationen ska hanteras i verksamheten
- Informationsklassningen skall utformas så att tillgången till information och öppenheten inom stadens verksamheter förblir så stor som möjligt för intressenter och allmänhet
- Tillämpliga lagar och andra giltiga styrdokument skall alltid uppfyllas och vägas in i informationsklassningen
- Nedanstående modell ska användas vid informationsklassningen

Kravnivå		Konfidentialitet	Riktighet	Tillgänglighet
Nivå 2	**Klassningsaspekt**	Känslig information som kan medföra **allvarlig skada** för egen eller annan organisations verksamhet eller för enskild person om den röjs för obehörig	Information som kan medföra **allvarlig skada** för egen eller annan organisations verksamhet eller för enskild person om den är felaktig.	Information som ingår i eller stöder kontinuerlig och kritisk verksamhet där avbrott innebär att man inte kan upprätthålla nödvändig tillgänglighet och servicenivå. Avbrott kan medföra **allvarlig skada** för egen eller annan organisations verksamhet eller för enskild person
Nivå 1 **GRUNDSÄKERHETSNIVÅ**	**Klassningsaspekt**	Information som kan medföra **skada** för egen eller annan organisations verksamhet eller för enskild person om den röjs för obehörig	Information som kan medföra **skada** för egen eller annan organisations verksamhet eller för enskild person om den är felaktig	Information som ingår i eller stöder kontinuerlig verksamhet där avbrott kan medföra **skada** för egen eller annan organisations verksamhet eller för enskild person
Nivå 0	**Klassningsaspekt**	Information som är öppen och avsedd för eller kan spridas till en obestämd krets mottagare utan risk för negativa konsekvenser. Spridning medför **ingen skada.**	Information som kan förändras utan risk för negativa konsekvenser Oriktig information medför försumbar eller **ingen skada**	Information med lågt verksamhetsberoende. Kan vara otillgänglig en längre tid utan risk för negativa konsekvenser. Brist på åtkomst medför försumbar eller **ingen skada.**

Hantering av informationstillgångar

- Samtliga informationssystem ska finnas förtecknade. I förteckningen beskrivs ändamål samt ansvarsfördelning såsom informationsägare, systemägare etc

- Tillämpliga regler, lagar, avtalsrättsliga åtaganden etc ska klart och tydligt definieras och dokumenteras för respektive informationssystem
- Informationsägaren ansvarar för informationsklassningen och att erforderligt skydd införs samt att säkerheten uppfyller ställda och rättsliga krav
- Alla som hanterar informationstillgångar har ett ansvar att upprätthålla informationssäkerheten

Personalresurser och säkerhet

- Kraven som ställs på personer som ska få tillgång till information och informationssystem ska vara definierade
- Personer som ska få tillgång till information och informationssystem ska ha tillräckliga kunskaper om informationssäkerhet i förhållande till sina arbetsuppgifter
- Det ska finnas användarinstruktion för respektive informationssystem
- Användarinstruktionen ska utformas på ett sådant sätt att en användares behov av att sätta sig in i detaljer kring gällande lagstiftning/regler för informationssystemet minimeras

Fysisk och miljörelaterad säkerhet

- Tillträde till lokaler som behöver skyddas mot obehörigt tillträde ska regleras och styras utifrån de krav som ställs av vederbörandes arbetssituation
- För säkerställande av centrala utrymmen med IT-baserade informationssystem, såsom datorhallar, ska
    - det fysiska skyddet ska vara entydigt definierat och dokumenterat där dokumentationen är skyddad från åtkomst av obehöriga
    - vara försett med ett skalskydd som är motståndskraftigt mot forcering och som är i nivå med skyddsklass 3 enligt Svenska Stöldskyddsföreningen
    - tillträde regleras restriktivt och strikt styras utifrån de krav som ställs av vederbörandes arbetssituation
    - det finnas dokumenterade besöksrutiner som inkluderar säkerställd besökslogg
    - besökare lätt kunna identifieras
    - besökare övervakas av behörig personal
    - larm med larmmottagare finnas för inbrott, brand, temperatur och fukt
    - systematiskt brandskyddsarbete enligt statens Räddningsverks allmänna råd bedrivas

Styrning av kommunikation och drift

- Det ska finnas en formellt beslutad driftdokumentation för IT-baserade informationssystem som minst omfattar återstarts- och återställningsrutiner, incidenthantering, ändringshantering samt hantering av logginformation. Ansvar gällande drift inkl system- och säkerhetsadministration ska också vara tydliggjort
- Loggning och skapande av spårbarhet för viktiga och säkerhetskritiska händelser ska ske. Loggning och loggarna ska skyddas för obehöriga samt vid behov analyseras och kunna nyttjas vid incidentutredningar
- Det ska för IT-baserade informationssystem finnas upptäckts- och skyddsåtgärder mot oönskad programkod och obehörigt nyttjande

Styrning av åtkomst

- Åtkomst och behörighet till informationstillgångar ska ges restriktivt och strikt styras utifrån de krav som ställs av vederbörandes arbetssituation
- Ansvarsfördelning och uppdelning av arbetsuppgifter ska tillämpas så att risken för missbruk begränsas
- För IT-baserade informationssystem ska endast ett fåtal personer erhålla privilegierade behörighet samt åtkomst till källprogramarkiv, operativsystem, systemhjälpmedel och revisionshjälpmedel
- Regelverk och rutin för registrering och avregistrering av behörigheter och åtkomst samt tilldelning av lösenord för IT-baserade informationssystem ska dokumenteras och finnas formellt beslutad
- Autentisering och åtkomstkontroll till IT-baserade informationssystem (gäller ej för öppen information) ska baseras på minst lösenord och bygga på unika användaridentiteter som är personliga och som ej får delas med andra
- Det ska finnas dokumenterade regler för vad som är tillåtet för anslutningar mellan IT-baserade informationssystem

Anskaffning, utveckling och underhåll

- Säkerhetsaspekter ska beaktas vid utveckling och anskaffning av informationssystem så att tillräckligt skydd uppnås. Att säkerhetsrutiner och regelverk efterlevs och motsvarar verksamhetens krav under informationssystemets hela livscykel inklusive avveckling och destruktion ska säkerställas och följas upp regelbundet
- System-/programutveckling och tester av modifierade IT-baserade informationssystem ska ske åtskilt från driftmiljön
- Det ska finnas formellt beslutade rutiner för ändringshantering för att inte åsidosätta befintliga skyddsåtgärder samt för att skapa ändringshistorik
- Det ska finnas regler för hur system- och programutveckling ska genomföras samt för installation av programvaror i IT-baserade informationssystem som är i drift
- Upphovsrättsliga frågor ska vara reglerade i avtal
- All systemdokumentation ska i rimlig omfattning och grad vara fullständig och aktuell samt uppdateras vid förändringar i informationssystem. Systemdokumentationen ska minst omfatta vad informationssystemets olika delar består av, en övergripande beskrivning av de olika delarnas uppgift samt en dokumentation över de funktioner som är relevanta för säkerheten
- IT-baserade informationssystem ska regelbundet analyseras för att identifiera sårbarheter eller problem som eventuellt kan orsaka incidenter så att bedömning och åtgärdande kan ske

Hantering av incidenter

- Det ska finnas en formell fastlagd rutin för hur informationssystemets användare ska agera vid incidenter
- Det ska finnas rutiner för rapportering, loggning, åtgärdande, informationsspridning, eskalering, uppföljning och analys av incidenter

Kontinuitetsplanering i verksamheten

- Det ska finnas formella beslut gällande den längsta tid som information kan vara otillgänglig eller informationssystemet bedöms kunna vara ur funktion innan

verksamheten påverkas i oacceptabel omfattning. Till grund för beslut ligger resultat från genomförda riskanalyser

- Grundat på verksamhetskraven ska det finnas en dokumenterad och formellt beslutad kontinuitetsplan. Övervägande om det finns behov av katastrofplanering ska ske
- Kontinuitetsplaner som inkluderar IT-baserade informationssystem ska omfatta återstarts- och reservrutiner för driftverksamheten som vidtas inom ramen för ordinarie drift så att återstart kan ske inom fastställd tid
- Återstarts- och reservrutiner för IT-baserade informationssystem såsom säkerhetskopiering och återläsning ska finnas och vara dokumenterade samt verifierade och anpassade för aktuell verksamhet
- Kontinuitetsplanen ska hållas aktuell och helt eller delvis testas årligen samt finnas tillgänglig för berörda i händelse av avbrott

Uppföljning av säkerhetsnivå

- Verksamhetens ledning ska kontinuerligt följa upp att säkerhetsnivån är acceptabel
- Uppföljning av informationssäkerhetsnivån i form av intern kontroll ska ske minst årligen. Resultatet rapporteras till nämnd/styrelse

Definitioner

Nedan återfinns definitioner på begrepp som tillämpas i denna riktlinje.

Begrepp	Definition
Autentisering	Verifiering av uppgiven identitet.
Identitet	Unik beteckning för en viss individ eller ett visst föremål
Incident	Händelse som resulterat eller som kunnat resultera i en skada eller oönskade konsekvenser för verksamheten
Informationssystem	Rutiner, metoder, procedurer etc organiserade för behandling av information, såväl manuella som helt eller delvis IT-baserade
Informationssäkerhet	Säkerhet beträffande informationstillgångar rörande förmågan att bevara och upprätthålla konfidentialitet, riktighet och tillgänglighet.
Informationstillgång	All information och informationshanterande resurser såsom manuella samt digitaliserade och IT-baserade informationssystem
Informationsägare	Generellt den som bestämmer ändamålen med och medlen för behandling och hantering av informationen. Ansvaret för informationen och dess säkerhet följer med ansvaret för verksamheten.
Kontinuitetsplan	Beskriver hur verksamheten ska bedrivas när kritiska verksamhetsprocesser allvarligt påverkas under en längre tid.
Logg	Insamlad information om händelser som sker/utförs
Lösenord	Teckensträng som anges för att verifiera en identitet
Revisionshjälpmedel	System, program, funktioner etc som kan användas för att identifiera brister och/eller tydliggöra uppfyllelse av krav, regelverk, standarder etc
Skalskydd	Skyddet som finns för den omslutningsyta, såsom väggar, golv, tak, dörrar etc, som avgränsar en lokal från omvärlden
Skyddsåtgärd	Handling, procedur eller tekniskt arrangemang som, genom att minska sårbarheten möter identifierat hot.
Spårbarhet	Möjlighet att entydigt kunna härleda utförda aktiviteter i systemet till en identifierad användare.