Göteborgs Stad

Konsekvensbedömning enligt dataskyddsförordningen

Personuppgiftsbehandlingarna:
Att informera och kommunicera i Digitala navet

2023-11-21

Versionshantering

Datum	Version	Beskrivning	Ändrat av
2023-09-22	1.0	Första bearbetning av utkast för stadsrevisionen baserad på intraservice konsekvensbedömning 2023-06-14.	Linda Bengtsson, Anders Landkvist, Sven Lindström Mia Eriksson
2023-10-06	1.1	Andra bearbetning av utkast för stadsrevisionen baserad på intraservice konsekvensbedömning 2023-06-14.	Linda Bengtsson, Anders Landkvist, Sven Lindström Mia Eriksson
2023-10-25	1.2	Tredje bearbetning av utkast för stadsrevisionen baserad på intraservice konsekvensbedömning 2023-06-14.	Linda Bengtsson, Anders Landkvist, Sven Lindström Mia Eriksson
2023-11-02	1.3	Fjärde bearbetning av utkast för stadsrevisionen baserad på intraservice konsekvensbedömning 2023-06-14.	Linda Bengtsson, Anders Landkvist, Sven Lindström Mia Eriksson
2023-11-10	1.4	Femte bearbetningen av utkast för stadsrevisionen baserad på intraservice konsekvensbedömning 2023-06-14. Fokus på korrektur, tillgänglighet och layout.	Sven Lindström

Innehåll

1 Inledning

1.1 Bakgrund och behov av 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.

För att skydda den personliga integriteten är det samtidigt viktigt att staden är restriktiv med att publicera uppgifter om medarbetare. Därför går Göteborgs Stad från det gamla intranätet, som var en delvis öppen webbplats, till att införa Digitala navet som är en helt intern webbplats.

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 under rubrikerna 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 i hela Göteborgs Stad
- möjliggöra informationsspridning vid kris eller andra större händelser.
- 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 ska en konsekvensbedömning genomföras när en personuppgiftsbehandling sannolikt innebär hög risk för de registrerade.

Stadsrevisionen 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 viss volym av personuppgifter som behandlas över tid.

Nämnden för intraservice (i det följande intraservice) har gjort en konsekvensbedömning för Digitala navet som utgår från intraservices dubbla roll som leverantör av tjänsten och användare av tjänsten i den egna verksamheten. Denna konsekvensbedömning innefattar därmed två perspektiv.

Stadsrevisionen har i sitt arbete med att genomföra en egen konsekvensbedömning utgått från intraservices bedömning avseende perspektivet som användare av tjänsten. Stadsrevisionen har också beaktat den tekniska och organisatoriska information som framgår av de bilagor som finns fogade till intraservice konsekvensbedömning. Bilagorna beskriver både hur informationsflöden sker inom det digitala navet, de dataskydds-aspekter som intraservice har identifierat och hur den kommungemensamma tjänsteleveransen av underliggande system som används för det digitala navet är utformade. Bilagorna finns fogade till denna konsekvensbedömning som en särskild grupp av underbilagor.

Metodmässigt har stadsrevisionen baserat arbetet på de malldokument som fram-tagits av dataskyddsenheten vi intraservice, som har rollen som stadengemensamma dataskyddsombud i Göteborgs Stad.

1.3 Deltagare och roller

- Linda Bengtsson, administrativ chef, dataskyddsansvarig
- Anders Landkvist, förvaltningsjurist och dataskyddsombud för stadsrevisionen
- Sven Lindström, kommunikationsansvarig.
- Mia Eriksson, registrator.

Linda Bengtsson är dataskyddsansvarig hos stadsrevisionen och har i denna egenskap lett arbetet att ta fram konsekvensbedömningen. Hon har biträtts med råd och stöd av Anders Landkvist

1.4 Personuppgiftsansvar

Revisorskollegiet är personuppgiftsansvarig för det innehåll som stads-revisionen publicerar i Digitala navet.

2 Beskrivning av behandlingar

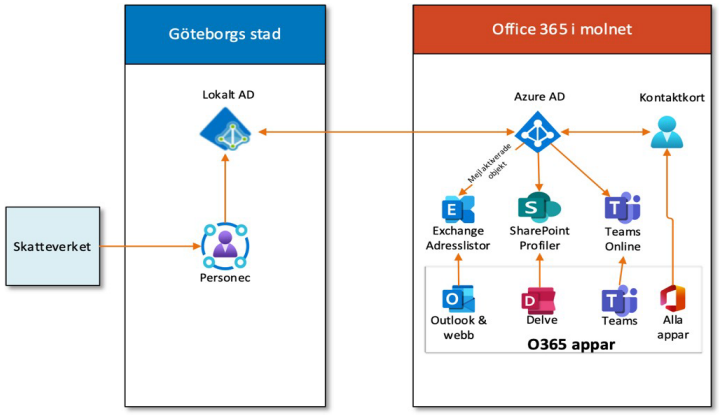
Personuppgiftsbehandlingarna i Digitala navet sker genom att stadsrevisionen informerar och kommunicerar i Digitala navet. Detta innebär att vi ger medarbetare internt inom stadsrevisionen och i hela staden kunskap om organisationen, arbetssätt och rutiner, rättigheter och skyldigheter som anställd, information om förändringsarbeten och vid kris, samt ger ökad delaktighet och möjlighet att skapa dialog och påverka.

2.1 Översiktlig beskrivning av behandlingarna

Digitala navet bygger på plattformen Sharepoint Online som är en del av Office 365-plattformen inom Göteborgs Stad. När en användare loggar in på sin staden-dator, har hen automatisk tillgång till Office 365 och till det Digitala navet.

Digitala navet hämtar uppgifter (förnamn, efternamn, e-postadress och av användaren publicerat foto) från den underliggande tjänsten Office 365 (Delve/Azure) och publicering av sidor sker via den underliggande tjänsten Office 365 (Sharepoint). Risker som är specifika för personuppgiftsbehandlingarna i Digitala navet behandlas i bilaga 1; Riskbedömning Digitala navet hos stadsrevisionen.

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



Figur 1: Beskrivning av hur personuppgifter hämtas ur de underliggande källorna.

Personuppgifterna hämtas ur de underliggande källorna av kvalitetssäkringsskäl, för att minimera risken att felaktiga personuppgifter publiceras.

Utöver de personuppgifter som hämtas från underliggande tjänster sker manuella tillägg där personuppgifter ska förekomma i redaktionellt bearbetade

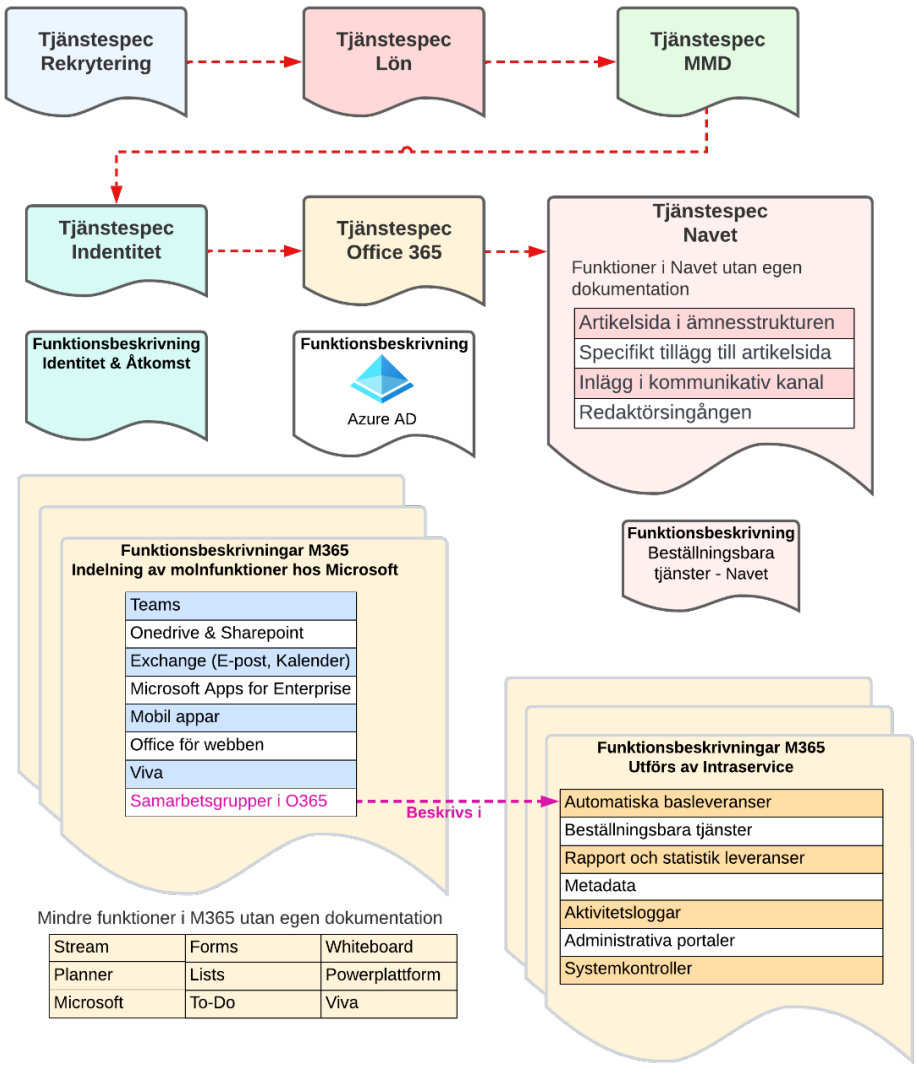
texter. Ett exempel på detta kan vara att användaren publicerar telefonnummer, foto, uppdrag/roll och facklig tillhörighet.

Olika funktionella delar och personuppgiftsflöden som ingår i Digitala navet beskrivs i de dokumenten från intraservice som finns i form av underbilagor till denna konsekvensbedömning. I underbilagorna förklaras hur tjänsterna fungerar med hänsyn till säkerhet och dataskydd. Dokumentationen sker i två nivåer:

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

Underbilagorna är följande:

Underbilaga	**Beskrivning**
Underbilaga 1	Underlag för DPIA-O365 Riskanalys Dataskydd 2022-12-08
Underbilaga 2	Underlag för DPIA - Digitala navet Riskanalys Dataskydd 2023-01-20
Underbilaga 3	Underlag för DPIA - Flöden - Digitala navet (O365, Identitet & åtkomst, Lön samt MMD)
Underbilaga 4	Underlag för DPIA - Tjänstespecifikation - Digitala navet
Underbilaga 5	Underlag för DPIA - Tjänstespecifikation - O365
Underbilaga 6	Underlag för DPIA - Tjänstespecifikation - Identitet och Åtkomst
Underbilaga 7	Underlag för DPIA - Funktionsbeskrivning - Azure AD
Underbilaga 8	Underlag för DPIA - Funktionsbeskrivning - Sharepoint och OneDrive



Figur 2: Tjänstespecifikationer och funktionsbeskrivningar med teknisk dokumentation.

För fördjupad relevant teknisk beskrivning med flöden för personuppgiftsbehandlingarna, se underbilagan Tjänstespecifikation Digitala navet samt de övriga underbilagorna som listas nedan under Tillgångar 2.1.1.

(Under arbetets gång har Microsoft bytt namn på sin tjänst Office 365 till Microsoft 365. Därför benämns tjänsten ibland som Microsoft 365 eller M365 i materialet.)

2.1.1 Tillgångar

Informationsbärare och informationstillgångar är:

- Azure AD (hantering av behörighet och autentisering) – se underbilaga *Funktionsbeskrivning Azure AD*

- Sharepoint (publicering av sida) – se underbilaga *Funktionsbeskrivning Sharepoint och OneDrive*
- Delve (presentation av organisatorisk information i Azure AD) – se underbilaga *Funktionsbeskrivning Sharepoint och OneDrive*
- Digitala navet – se underbilaga *Tjänstespecifikation Digitala navet*
- Office 365 – se underbilaga *Tjänstespecifikation O365*
- Identitet och åtkomst – se underbilaga *Tjänstespecifikation Identitet och Åtkomst*
- Kvalitetssäkrad information (Master Meta Data = MMD) – se underbilaga 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 den tidigare styrmodellen i Göteborgs Stad (*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) då de levererar Digitala navet till andra förvaltningar. (I dessa fall är respektive nämnd PUA – i stadsrevisionens fall är revisorskollegiet 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 beskrivningen ovan.

I arbetet med anpassning till Göteborgs Stads nya riktlinje för styrning, samordning och finansiering av digital utveckling och förvaltning pågår ett 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 behandlingar

<table>
<tr><th>Behandling</th><th>Personuppgifter</th><th>Känsliga personuppgifter</th></tr>
<tr><td>Informera och kommunicera i Digitala navet</td><td>Manuella (redaktionella) tillägg: av användaren publicerat telefon-nummer, foto, och uppdrag/ roll.

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><td>Fält</td><td>Vad visas</td></tr>
<tr><td>Display name</td><td>Förnamn och 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>Stadsrevisionen kommer inte att publicera några känsliga personuppgifter i Digitala navet.</td></tr>
</table>

2.2.1 Personuppgifter om lagöverträdelser

Förekommer inte.

2.2.2 Kategorier av registrerade

Behandling	Kategorier av registrerade
Informera och kommunicera i Digitala navet	Anställda vid stadsrevisionen och i Göteborgs Stad.

	Konsulter med uppdrag för stadsrevisionen och i Göteborgs Stad.

2.2.3 Behandlingarnas omfattning

Behandlingarna omfattar fler 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.

Stadsrevisionen har mot bakgrund av ovanstående valt att begränsa tillgången till viss information avseende den egna verksamheten. På så sätt har bara revisionskontorets medarbetare tillgång till den via andra kommunikationskanaler än Digitala navet. Den information som omfattas gäller:

- lokala styrdokument
- lokal information som rör säkerhet
- lokala anställningsförmåner och aktiviteter
- information om våra revisionella arbetssätt
- information som innehåller personuppgifter (i den mån det är möjligt).

Behörighetsbegränsning sker praktiskt genom att ovan angiven information inte publiceras via det Digitala navet.

2.3 Ändamål

Behandling	Ändamål
Informera och kommunicera i Digitala navet	För att kunna använda Digitala navet är det nödvändigt att behandla personuppgifter i systemet. Behandlingen är en förutsättning för att genom systemet erbjuda stöd till anställda och konsulter i staden när det kommer till förändringsarbete, att tillhandahålla krisinformation, öka delaktighet och skapa möjligheter till dialog och påverkan.

2.4 Rättslig grund

Behandling	Rättslig grund	Motivering och hänvisning
Informera och kommunicera i Digitala navet	Uppgift av allmänt intresse	Digitala navet är stadens prioriterade kanal för intern kommunikation (se Göteborgs Stads policy för kommunikation beslutad i kommunfullmäktige 2019-12-10). Stadsrevisionen är en del av Göteborgs Stad och har som uppdrag att årligen granska all verksamhet som bedrivs i staden i enlighet med lag och god sed. Granskningen utgör i sig inte myndighetsutövning utan bedöms hänföras till den rättsliga grunden ”uppgift av allmänt intresse”. Stadsrevisionen har en lagstadgad rätt till de upplysningar som krävs för att genomföra granskningen. Stadsrevisionens tillgång till information för planering och genomförande av granskningen säkerställs på olika sätt, såsom genom intervjuer och insamling av dokument. Användning av intranät eller det digitala navet är ett viktigt hjälpmedel för att samla och utvärdera information runt verksamheterna som granskas. Den information som stadsrevisionen delar i det digitala navet med staden i övrigt bedöms understödja och främja intern kommunikation kopplad till stadsrevisionens verksamhet och uppdrag.

3 Behov/proportionalitet

3.1 Ändamålsbegränsning

Samtliga publiceringsansvariga (redaktörer) genomgår ett gediget utbildningspaket, som tillhandahålls av intraservice. De genomgår bland annat detta för att få kunskap om hur de ska förhålla sig till personuppgifter. Utbildningen är en förutsättning för att få behörighet att publicera innehåll i Digitala navet.

Det finns olika behörighetsnivåer för redaktörer. Intraservice, som är ansvarigt för drift och utveckling av det Digitala navet, avgör vilken behörighet som ges till respektive redaktör.

Varje redaktionell publicering som innehåller personuppgifter ska stämmas av 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.

3.2 Uppgiftsminimering

Det är väsentligt att en PUA vid varje behandling av personuppgifter säkerställer att behandlingen inte behandlar fler personuppgifter än nödvändigt för att uppnå syftet med behandlingen. Detta är viktigt att ha med sig vid användning av det Digitala navet. Det krävs i och med detta en aktiv avvägning av behovet av kommunikation mot behovet av dataskydd. En sådan avvägning ska alltid göras av den som har redaktörsbehörighet och därmed möjlighet att publicera material i systemet. I arbetssättet för publicering ingår också att en avstämning alltid ska ske med eventuella registrerade, för att säkerställa att publicerat innehåll är korrekt.

För att samtliga redaktörer i staden ska ha förutsättningar för att arbeta på detta sätt genomgår de ett gediget utbildningspaket, som bland annat syftar till att belysa vikten av att inte använda onödiga uppgifter. Där ingår också 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

Stadsrevisionen följer *Revisionskontorets riktlinje för kommunikation* när vi använder digitala navet (se vidare bilaga 2).

Riktlinjen anger att kommunikationsansvarig är ansvarig för att säkerställa aktualiteten i informationen i det Digitala navet. Varje år ska därför kommunikationsansvarig gå igenom innehållet i specifika tillägg (information specifik för stadsrevisionen som har publicerats i det digitala navet). Om informationen är inaktuell ska den gallras eller bevaras i enlighet med gällande dokumenthanteringsplan. Stadsrevisionens dokumenthanteringsplan bifogas som bilaga 3.

Av riktlinjen framgår också att kommunikationsansvarig (i rollen som redaktör) vid varje enskild publicering i Digitala navet ska minimera antalet personuppgifter så långt det går utan att informationen förlorar sin innebörd.

Det noteras slutligen att det kommer att krävas utbildning enligt punkt 3.2 ovan för att erhålla redaktörsbehörighet i det Digitala navet.

3.4 Åtgärder som stärker de registrerades rättigheter

3.4.1 Informationsplikt

- Stadsrevisionen informerar om hur vi hanterar personuppgifter på den öppna webbplatsen goteborg.se, där informationen finns tillgänglig för såväl stadens medarbetare som för allmänheten. Länk till webbplatsen är: Så behandlar stadsrevisionen dina personuppgifter - Göteborgs Stad (goteborg.se)
- Stadsrevisionens medarbetare informerar också om verksamhetens personuppgiftsbehandling via en länk i e-postsignaturen.
- Vid anställning hos stadsrevisionen 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).

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 Stadsrevisionen.

Av denna framgår att revisionsdirektören via delegation äger rätt att fatta beslut om:

- att neka utlämnande av registerutdrag med personuppgifter
- att avslå begäran om:
    - Rätt till rättelse
    - Rätt till radering
    - Rätt till begränsning
    - Rätt till invändning

Revisionsdirektören har även rätt att vidaredelegera beslutsrätten enligt ovan.

All hantering av information sker utifrån gällande lagar och styrande dokument. All radering av personuppgifter hanteras enligt arkivlagen och ska som huvudregel bevaras.

Eventuell radering av personuppgifter sker i enlighet med gallringsbeslut. Gallringsbeslut meddelas av arkivmyndigheten som för Göteborgs Stad utgörs av arkivnämnden.

Gällande gallringsbeslut för stadsrevisionens verksamhet återges i beslutad dokumenthanteringsplan. Dokumenthanteringsplanen bifogas som bilaga 4.

Alla sidor i Digitala navet har utsedda innehållsansvariga och publicerings-ansvariga (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.

Förutom denna kontaktväg kan man också gå via förvaltningsbrevlådan och dataskyddsansvarig vid stadsrevisionen.

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 sidans innehållsansvarig eller publiceringsansvarig för synpunkter på innehållet eller presentation av informationen. Förutom denna kontaktväg kan man också gå via förvaltningsbrevlådan och dataskyddsansvarig vid stadsrevisionen.

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

fastställda delegationsordningen för stadsrevisionen enligt vad som angivits under punkt 3.4.3.

3.4.5 Personuppgiftsbiträdesavtal och instruktioner

I arbetet med anpassning till *Göteborgs Stads nya riktlinje för styrning, samordning och finansiering av digital utveckling och förvaltning* pågår ett arbete inom intraservice – i egenskap av tillhandahållare av den kommungemensamma tjänsten som Digitala navet utgör – med att ta fram förslag till PUB-avtal kopplat till systemet.

I detta kan det konstateras att 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).

Stadsrevisionen inväntar intraservice förslag till PUB-avtal och instruktioner enligt ovan. Ytterligare arbete pågår hos intraservice med att formalisera förhållandena mellan dem och användarna av kommungemensamma system och tjänster i staden i enlighet med ovan angivna riktlinje.

Stadsrevisionen kommer att följa utvecklingen vidare.

3.5 Samlad bedömning av behovet av och proportionaliteten hos behandlingarna

Eftersom intranätet är stadens prioriterade kanal för intern kommunikation och det är en viktig kanal för krisinformation anses stadens behov av ett intranät 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?

☒ Ja

☐ Nej

☒ Risk för tredjelandsöverföring

För motivering se *Underbilaga 1 - Riskanalys O365 Riskanalys Dataskydd*.

4.2 Översikt överföringar

Beskrivning av varje identifierad överföring av personuppgifter till tredjeland.

Behandling	Personuppgifter som överförs	Land de överförs till	Finns adekvans-beslut för mottagarlandet?
Informera och kommunicera i Digitala navet	För redogörelse av tredjelandöverföring se *Tjänste-specifikation O365*, *Tjänstespecifikation Digitala navet*, *O365 Riskanalys dataskydd*, *Digitala navet Riskanalys dataskydd och Riskbedömning Digitala navet på Intraservice*.	USA	Ja Se vidare nedan för ytterligare information runt gällande adekvansbeslut.

4.2.1 Ytterligare information

Vid överföring av personuppgifter till tredjeland, det vill säga överföring till land utanför EU/EES, kräver GDPR att det mottagande landet har en skyddsnivå för personuppgifterna och de registrerades intressen som motsvarar det som gäller där GDPR är direkt tillämplig. Det finns olika sätt för PUA att

säkerställa detta. Det enklaste sättet är om EU-kommissionen fattat ett beslut om att det mottagande landet har en ”adekvat skyddsnivå”, vad som också kallas ett adekvansbeslut. Om det finns ett adekvansbeslut för ett mottagarland så kan PUA med stöd av detta överföra personuppgifter till detta (tredje) landet utan att riskera att bryta mot GDPR:s regler.

I fråga om tredjelandsöverföringar till Förenta staterna (USA) så har kommissionen tidigare fattat två adekvansbeslut (Safe Harbour respektive Privacy Shield). Båda dessa beslut har utmanats i EU-domstolen som otillräckliga och då upphävts av domstolen (i målen Schrems I och II). Detta har fått till följd att det under en tid saknats ett gällande adekvansbeslut för tredjelandsöverföringar till Förenta staterna. I sin tur har det medfört svårigheter för PUA som använder sig av exempelvis leverantören Microsofts tjänster och produkter, eftersom detta är ett multinationellt amerikanskt företag.

Problematiken runt detta avspeglas i de riskanalyser för dataskydd (underbilaga 1 och 2) som enheten för dataskydd vid intraservice tagit fram för Digitala navet. Från och med den 10 juli 2023 gäller dock ett nytt adekvansbeslut. Med anledning av detta har dataskyddsenheten tagit fram nya/modifierade rekommendationer för tredjelandsöverföringar till Förenta staterna. Stadsrevisionen har i beredningen av konsekvensanalysen tagit del av adekvansbeslutet och av dataskyddsenhetens rekommendationer. I detta kan det konstateras att adekvansbeslutet inte gäller generellt för alla typer av överföringar av personuppgifter till USA utan att det är begränsat till att gälla överföringar som sker till organisationer etablerade i detta land, som omfattas av det nya ramverket ”EU-US data privacy framework”. Ramverket är en mekanism för självcertifiering där de organisationer som vill delta får genomgå en särskild process för att godkännas. Certifieringen gäller för ett år i taget och kan därefter förnyas via ytterligare en process. Organisationer som är certifierade förtecknas på en sökbar lista som nås via www.dataprivacyframework.gov

Sammantaget konstateras i detta att de underliggande IT-systemen för Digitala navet och applikationen/systemet i sig – som är Sharepoint-baserad – levereras av det amerikanska företaget Microsoft som är certifierat enligt ovan och därmed omfattas av gällande adekvansbeslut. Sådana tredjelandsöverföringar som kan förekomma i Digitala navet är därmed tillåtna att göra.

5 Risk och åtgärder

5.1 Generella åtgärder

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

Riskerna vid delning av personuppgifter med underleverantören i den underliggande plattformen Microsoft Office 365, hanteras i riskanalys *O365 Riskanalys Dataskydd*, se underbilaga 1.

Åtgärderna nedan är sådana som är kopplade till användning av Digitala navet. Åtgärderna tillhandahålls och utförs av intraservice. Informationen om åtgärderna har presenterats av intraservice för stadsrevisionen och övriga användare av Digitala navet. Åtgärderna har bedömts som ändamålsenliga av stadsrevisionen i samband med genomförandet av denna konsekvensbedömning.

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 har 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 personuppgiftincidenter	Intraservice uppger att system finns för generell detektering av personuppgiftsincidenter i underliggande applikationer.
☒	☐	☐	☐	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.

Genomförd	Pågående	Planerad	Ej tillämplig	Åtgärd	Kommentar
☒	☐	☐	☐	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** Ingen kommentar					
☒ **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 har identifierats.

Genomförd	Pågående	Planerad	Ej tillämplig	Åtgärd	Kommentar
☒	☐	☐	☐	Riktlinjer för datoranvändning	Information om Riktlinjer för IT-användning i Göteborgs Stad lämnas till nyanställda och nya förtroendevalda i samband med introduktion. Information om riktlinjen har lämnats vid kontorsintern utbildning 2023. Löpande information om utveckling av riktlinjen lämnas vid APT.
☒	☐	☐	☐	Utbildning och informationsinsatser	Utbildningsinsatser för de som har rollen Redaktör via Intraservice.

Genomförd	Pågående	Planerad	Ej tillämplig	Åtgärd	Kommentar
☐	☐	☒	☐	Kontinuitetsplan	Är ett kommande projekt för stadsrevisionen för fortsatt utveckling av informations-säkerhetsarbetet.
☒	☐	☐	☐	Incidenthanteringsplan	Stadsrevisionen har en framtagen rutin för incidenthantering.
☐	☐	☒	☐	Katastrofberedskap (Disaster recovery plan)	Är ett kommande projekt för stadsrevisionen för fortsatt utveckling av informations-säkerhetsarbetet.
☐	☐	☐	☒	Behovsenlig behörighet (Need-to-know)	Publicerat innehåll är ämnat för hela staden. Dock är generell tillgång till Digitala navet behörighetsstyrd. Stadsrevisionen begränsar publicering av visst innehåll.
☒	☐	☐	☐	Sekretessavtal	Sekretessavtal skrivs under vid anställning. Sekretessavtal för konsulter skrivs under vid uppdragsstart.
☒	☐	☐	☐	Lösenordspolicy	Följer stadens lösenordspolicy.
☐	☐	☐	☒	Penetrationstestning	Penetrationstestning sker av intraservice i egenskap av tillhandahållare av tjänsten på Microsoft M365-miljö, men är inte applicerbart direkt för Digitala navet.
☒	☐	☐	☐	Säkra fysiska lokaler	Kontrollerad inpassering i lokalerna via elektroniskt skalskydd. Larmade lokaler.
☒	☐	☐	☐	Tillsyn/interna kontroller	Sticksprovsvis efterlevnadskontroll en gång per år (efterlevnad av tillämpliga delar av stadens styrande dokument).
☒	☐	☐	☐	Övervakning	Övervakning ur ett tekniskt perspektiv sker via systemleverantör/ intraservice.
☐	☐	☒	☐	Simulerings- och krisövningar	Är ett kommande projekt för stadsrevisionen för fortsatt utveckling av informations-säkerhetsarbetet.
☒	☐	☐	☐	Bakgrundskontroller	Utförs vid behov.

Genomförd	Pågående	Planerad	Ej tillämplig	Åtgärd	Kommentar
☒	☐	☐	☐	Åtkomstkontroll	Vi har kontroll vid fysisk åtkomst, behörighetskontroll för tillgång till Digitala navet och underliggande tjänster samt loggning av åtkomst.
☒	☐	☐	☐	Leverantörskontroller	Ansvar för leverantörskontroller ligger hos intraservice i egenskap av tjänsteleverantör.
☐	☐	☐	☒	Riktlinjer för hantering av fysiska handlingar	Inga fysiska handlingar i Digitala navet.
☒	☐	☐	☐	Arkivering	Digitala navet kommer väsentligen att spegla dokument och handlingar som hanteras i stadsrevisionens verksamhet. Dessa gallras respektive bevaras i enlighet med dokumenthanteringsplan samt regionarkivets anvisning för webbarkivering.
☐ **Inte säker** Ingen kommentar					
☒ **Annat** Kommentar: De generella administrativa åtgärderna som införts eller kommer att införas hos stadsrevisionen speglar väsentligen de krav som ställs i staden via gällande riktlinje för informationssäkerhet.					

5.2 Bedömning av specifika risker

Riskbedömningen finns i ”Riskbedömning inför driftsättning av Digitala navet hos stadsrevisionen” och biläggs konsekvensbedömningen som bilaga 1.

Riskbedömningen inkluderar 9 risker som kvarstår 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.

ID	Beskrivning av risk	Vidtagna skyddsåtgärder	Nytt riskvärde
4	Lansering av digitala navet innebär fortsatt användning av office360 och dess underliggande risker.	Bevakning av att gällande certifiering finns för företag som tillhandahåller underliggande IT-system för det Digitala navet.	6

ID	Beskrivning av risk	Vidtagna skyddsåtgärder	Nytt riskvärde
	Kommissionens adekvansbeslut från juli 2023 innebär att denna risk reducerats avsevärt. Det förutsätts dock att leverantörerna av underliggande tjänster har giltiga certifieringar.	Bevakning av utvecklingen av rättsläget rörande gällande adekvansbeslut. Om gällande adekvansbeslut ogiltigförklaras av EU-domstolen kommer risken att öka. SR begränsar dock mängden PU aktivt.	
5	Risk för att PUA/PUB-förhållanden förändras utifrån pågående utredningar, vilket leder till behov av förändringar i konsekvens-bedömningen.	Utredning av PUA/PUB pågår i staden. Konsekvensbedömningen uppdateras vid behov. Risken är oförändrad eftersom skyddsåtgärden ännu inte är genomförd.	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 riskanalysen.

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 att publicera information i Digitala navet som delas inom Göteborgs Stad bedöms som låga utifrån att det inte är några känsliga personuppgifter som publiceras, förutom facklig tillhörighet för fackligt förtroendevald för de verksamheter som valt att publicera detta. Stadsrevisionen har valt att inte publicera facklig tillhörighet för fackligt förtroendevalda i Digitala navet. Stadsrevisionen har också valt att begränsa tillgången till viss annan verksamhetsinformation (se punkt 2.2.3 ovan).

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 beskrivs 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.

Riskerna har emellertid reducerats avsevärt i och med EU-kommissionens nya adekvansbeslut av den 10 juli 2023. De kan dock komma att öka på nytt om adekvansbeslutet utmanas i domstol och då upphävs, alternativt om leverantören av underliggande IT-system (Microsoft) förlorar sin certifiering under EU-US data privacy framework.

5.3.1 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.

Stadsrevisionens bedömning är att något förhandssamråd inte behöver genomföras i dagsläget givet de förutsättningar som den stadengemensamma tjänsten erbjuds under.

6 Medverkan från berörda parter

6.1 Kommentarer/rekommendationer från dataskyddsombudet

Se separat skrivelse från DSO som bifogas i form av bilaga 4.

6.2 Synpunkter från de registrerade

Intraservice har tagit upp frågan om publicering av känsliga uppgifter i form av facklig tillhörighet och avstämt den med fackförbundens jurister. Man har därvid landat i bedömningen att publicering av information om facklig kontaktperson ska ske i samråd med berörd person. Stadsrevisionen har beaktat detta inför sin planerade användning av Digitala navet och beslutat att inte publicera denna typ av information, då behovet av det bedöms vara begränsat, sett till organisationens storlek. Av denna anledning anses integritetsrisken vara större än kommunikationsbehovet för uppgifterna.

Det Digitala navet kommer vidare att ersätta det befintliga intranätet där motsvarande information för stadsrevisionen lagrats. Det bedöms därmed inte innebära några mer betydande förändringar för de registrerade vid stadsrevisionen att Digitala navet införs som gemensam tjänst i staden och hos stadsrevisionen. Information om det kommande införandet av det Digitala navet har dock ändå lämnats löpande i samband med APT under införandeprocessen där medarbetare haft möjlighet att ställa frågor och framställa synpunkter.

7 Avslut

7.1 Beslut

Revisionsdirektören har efter samråd i ledningsgruppen fattat beslut om att begränsa tillgången till viss information avseende stadsrevisionens verksamhet som publiceras i det Digitala navet.

Den information som omfattas av begränsningen är:

- Lokala styrdokument
- Lokal information som rör säkerhet
- Lokala anställningsförmåner och aktiviteter
- Information om våra revisionella arbetssätt
- Information som innehåller personuppgifter (i den mån det är möjligt)
- Känsliga personuppgifter angående facklig tillhörighet för personer med förtroendeuppdrag inom stadsrevisionens verksamhet.

7.2 Nästa steg

Konsekvensbedömningen ska godkännas och beslutas av revisorskollegiet vid dess sammanträde den 21 november 2023. Lansering/driftsättning av det Digitala navet planeras därefter i december 2023.

8 Bilagor som bifogas

Bilaga 1 – Riskbedömning Digitala navet hos stadsrevisionen

Bilaga 2 – Revisionskontorets riktlinje för kommunikation

Bilaga 3 – Dokumenthanteringsplan för stadsrevisionen

Bilaga 4 – Kommentarer och rekommendationer från dataskyddsombudet för stadsrevisionen

8.1 Underbilagor från intraservices konsekvensbedömning

Underbilaga 1 – Underlag för DPIA - O365 Riskanalys Dataskydd 2022-12-04

Underbilaga 2 – Underlag för DPIA - Digitala navet Riskanalys Dataskydd 2023-01-20

Underbilaga 3 – Underlag för DPIA - Flöden - Digitala navet (O365, Identitet & åtkomst, Lön samt MMD)

Underbilaga 4 – Underlag för DPIA - Tjänstespecifikation - Digitala navet

Underbilaga 5 – Underlag för DPIA - Tjänstespecifikation - O365

Underbilaga 6 – Underlag för DPIA - Tjänstespecifikation - Identitet och Åtkomst

Underbilaga 7 – Underlag för DPIA - Funktionsbeskrivning - Azure AD

Underbilaga 8 – Underlag för DPIA - Funktionsbeskrivning - Sharepoint och Onedrive

Stadsrevisionen
Telefon: 031-365 00 00 (kontaktcenter)
E-post: stadsrevisionen@stadsrevisionen.goteborg.se

9 Bilaga 1 – Riskbedömning Digitala navet hos stadsrevisionen

Senastuppdaterad 2023-11-02

BILAGA 1

Riskbedömning inför driftsättning av Digitala navet hos stadsrevisionen

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

	Behandling	PU-Flöden *PU-aktiviteter där risken finns*	PUA/PUB *Risk bedömd även för tjänsteleverans till andra verksamheter*	Risk *Obehörig åtkomst till personuppgifter, oönskad ändring av personuppgifter, förlust av personuppgifter eller annan form av risk*	Riskbeskrivning	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 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 negativt.	Kan leda till obehag eller hot mot kontakt-personen	3	1	3	Primärt ska funktionsbrevlådor användas som kontakt. Innan kontaktpersoner publiceras ska detta stämmas av. Utbildning av redaktörer säkerställer korrekt hantering.	2	1	2	Arbete som utförs av central (intraservice) och lokal organisation (stadsrevisionen). Dessa organisationer är under uppbyggnad i samband med att tjänsten/systemet ska införas.
2	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.	3	1	3	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 (intraservice) och lokal organisation (stadsrevisionen). Dessa organisationer är under uppbyggnad i samband med att tjänsten/systemet ska införas.
3	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 är aktuell.	1	1	1	Arbete som utförs av central (intraservice) och lokal organisation (stadsrevisionen). Dessa organisationer är under uppbyggnad i samband med att Digitala navet införs.

	Behandling	PU-Flöden *PU-aktiviteter där risken finns*	PUA/PUB *Risk bedömd även för tjänsteleverans till andra verksamheter*	Risk *Obehörig åtkomst till personuppgifter, oönskad ändring av personuppgifter, förlust av personuppgifter eller annan form av risk*	Riskbeskrivning	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
4	Informera och kommunicera i Digitala Navet		PUA	Annan form av risk	Lansering av digitala navet innebär fortsatt användning av Office 365 och dessunderliggande risker. Kommissionens adekvansbeslut från juli 2023 innebär att denna risk reducerats avsevärt. Det förutsätts dock att leverantörerna av underliggande tjänster har giltiga certifieringar.	Risk för tredjelandsöverföring av personuppgifter som visas i Digitala navet.	4	4	16	Digitala navet presenterar information som finns i underliggande tjänster. Gällande adekvansbeslut hanterar riskerna under givna förutsättningar. PUA måste alltid säkerställa att underliggande tjänster levereras av leverantörer med giltig certifiering. www.dataprivacyframework.gov Stadsrevisionen kommer dessutom att aktivt begränsa mängden personuppgifter i systemet enligt beslutad riktlinje för kommunikation.	3	2	6	Om gällande adekvansbeslut ogiltigförklaras av EU-domstolen kommer risken att öka. Stadsrevisionen begränsar dock mängden personuppgifter aktivt.
5	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 personuppgifts-ansvarig (PUA), när intraservices nämnd är PUA samt om stadsledningskont oret 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 skyddsåtgärden ännu inte är genomförd.
6	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 behörig attestant behörigheter innan de godkänner. Acceptera risken.	2	2	4	
7	Informera och kommunicera i Digitala Navet	Aktivitet 8	PUA/PUB	Annan form av risk	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 sociala medier) som även ska gälla för navet. Stadsrevisionen kommer initialt inte att använda kommentarsfunktionen	E/T	E/T	E/T	
8	Informera och kommunicera i Digitala Navet		PUA	Annan form av risk	Risk för otydlig eller otillräcklig information till den registrerade som inte ingår i gruppen anställda medarbetare, exempelvis konsulter.	Avsaknad av eller undermålig information gör att den registrerade inte kan utöva sina fri- och rättigheter.	2	2	4	Rutin för information till konsulter eller andra personer som inte är anställda i verksamheten tas fram.	2	1	2	
9	Informera och kommunicera i Digitala Navet		PUA	Annan form av risk	Risk för otydlig eller otillräcklig information till den registrerade (gäller alla registrerade)	Avsaknad av eller undermålig information gör att den registrerade inte kan utöva sina fri- och rättigheter.	2	2	4	Information lämnas till nyanställda, information lämnas till anställda vid APT om hur personuppgifter behandlas av stadsrevisionen.	2	1	2	

10 Bilaga 2– Revisionskontorets riktlinje för kommunikation

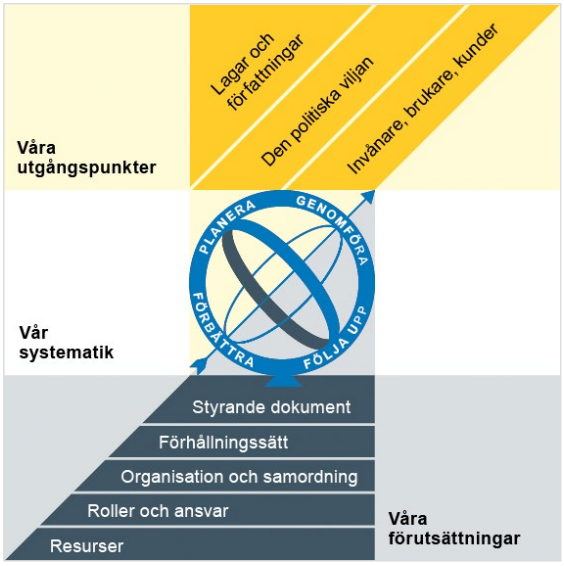
Göteborgs Stad

Revisionskontorets riktlinje för kommunikation

Reglerande styrande dokument

Policy
► **Riktlinje**
Regel
Anvisning
Rutin
Instruktion

Göteborgs Stads styrsystem



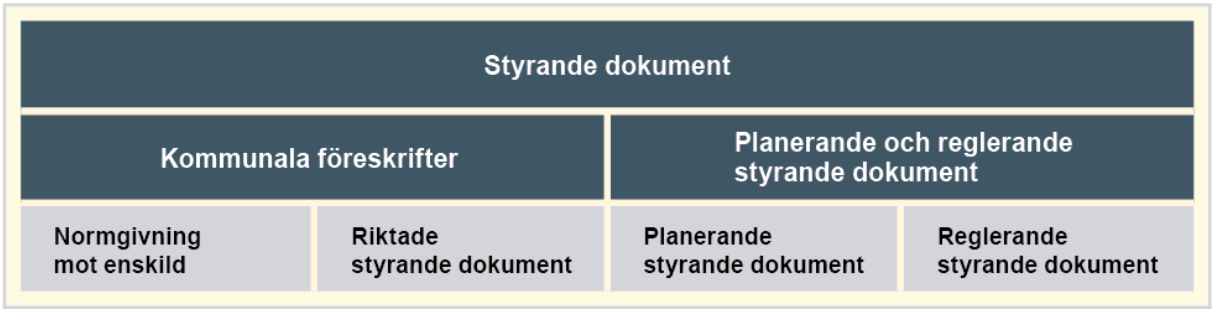
Utgångspunkterna för styrningen av Göteborgs Stad är lagar och författningar, den politiska viljan och stadens invånare, brukare och kunder. För att förverkliga utgångspunkterna behövs förutsättningar av olika slag. Stadens politiker har möjlighet att genom styrande dokument beskriva hur de vill realisera 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.



Beslutad av:	**Gäller för:**	**Diarienummer:**	**Datum och paragraf för beslutet:**
Revisionsdirektören	Revisionskontoret	0253/22	2023-01-09
Dokumentsort:	**Giltighetstid:**	**Senast reviderad:**	**Dokumentansvarig:**
Riktlinje	Tills vidare	2023-11-06	Kommunikationsansvarig

Innehåll

Inledning

Syftet med denna riktlinje

Revisionskontorets riktlinje för kommunikation (hädanefter riktlinjen) gäller för Göteborgs Stads revisionskontor och har tagits fram av ledningsgruppen på revisionskontoret.

I Göteborgs Stads policy för kommunikation står det att kommunikationen i kommunen ska kännetecknas av öppenhet och ett aktivt förhållningssätt samt att den alltid ska vara opartisk och saklig. Utöver detta har stadsrevisionen tre verksamhetsmål:

- Stadsrevisionen ska vara oberoende, publik och tydlig.
- Stadsrevisionen ska ha hög trovärdighet och skapa högt förtroende för revisionens iakttagelser.
- Stadsrevisionen ska arbeta stödjande genom att i sin granskning bidra till en ändamålsenlig verksamhet.

Ett strategiskt kommunikationsarbete är en viktig del för att uppnå verksamhetsmålen och en förutsättning för att kunna följa Göteborgs Stads policy. Genom att alla medarbetare på kontoret har en gemensam plattform att arbeta utifrån kan vi göra detta så effektivt som möjligt. Riktlinjen beskriver hur, varför och när vi ska kommunicera i olika situationer.

Tre huvudsyften med revisionskontorets kommunikation har identifierats:

- Revisionskontoret ska stödja de förtroendevalda revisorerna i att kommunicera granskningsresultaten till alla relevanta målgrupper. Kommunikationen ska ske på ett korrekt, sakligt, lättillgängligt och begripligt sätt.
- Kommunikationsarbetet ska bidra till att skapa en rättvisande och tydlig bild av stadsrevisionens uppdrag.
- Kommunikationsarbetet ska skapa en effektiv internkommunikation med information som når ut till hela revisionskontoret. Verksamhet, roller och förväntningar ska vara tydliga hos kontorets medarbetare.

Vem omfattas av riktlinjen

Denna riktlinje gäller tills vidare och för samtliga medarbetare på revisionskontoret i Göteborgs Stad.

Revisionskontoret består av tjänstepersoner och yrkesrevisorer som bistår de förtroendevalda revisorerna på stadsrevisionen i Göteborgs Stad. I riktlinjen förekommer både benämningen *revisionskontoret* och benämningen *stadsrevisionen*. Revisionskontoret är ett samlingsbegrepp för de tjänstepersoner och yrkesrevisorer som arbetar på revisionskontoret. Stadsrevisionen är ett samlingsbegrepp för tjänstepersoner, yrkesrevisorer och förtroendevalda revisorer. Det är alltså bara tjänstepersoner och yrkesrevisorer som omfattas av riktlinjen. De förtroendevaldas rapportering och kommunikationsarbete styrs inte av riktlinjen, utan av arbetsordningen för revisorsgruppen.

Lagbestämmelser

Stadsrevisionens uppdrag är att granska kommunens verksamhet. Kommunallagen (2017:725) och aktiebolagslagen (2005:551) reglerar revisionsuppdraget och stadsrevisionens granskning av den kommunala verksamheten. Till viss del reglerar de även hur revisionskontoret ska kommunicera.

Koppling till andra styrande dokument

Skriften *God revisionssed i kommunal verksamhet*[1] (hädanefter God sed) reglerar också revisionsuppdraget och stadsrevisionens granskning av den kommunala verksamheten. Skriften är av stor relevans för hur revisionskontoret ska arbeta med kommunikation i anslutning till sitt uppdrag.

Göteborgs Stads styrdokument för kommunikation är också centrala i revisionskontorets kommunikationsarbete. Kontoret är en del av Göteborgs Stad men den särskilda funktion som vi har påverkar hur vi kan och bör arbeta med kommunikation. Vår funktion påverkar också hur vi kan och bör förhålla oss till Göteborgs Stads styrdokument för kommunikation.

Styrande dokument som påverkar denna riktlinje är:

- Arbetsordning för revisorsgruppen (RG) i Göteborgs Stad
- God revisionssed i kommunal verksamhet (SKR)
- Göteborgs Stads policy för kommunikation
- Göteborgs Stads riktlinje för kommunikation
- Göteborgs Stads regler för användande av e-post
- Göteborgs Stads riktlinje för kommunikation
- Krisledningsplan stadsrevisionen
- Revisionens kommunikation (SKR)
- Rutin för flexibel arbetsplats
- Tidplaner för underlag till RG

[1] God revisionssed i kommunal verksamhet. 2022.

Riktlinje

I *Revisionens kommunikation* utgiven av SKR står att:

> En revision som arbetar aktivt med sin kommunikation och dialog blir synlig. Synligheten bidrar till att revisionens iakttagelser och bedömningar tas emot bättre. Detta leder i sin tur till att revisionen kan arbeta främjande, det vill säga hjälpa kommunen eller regionen att utveckla och förbättra verksamheten.[2]

Revisionskontorets medarbetare ska därför alltid ta hänsyn till stadsrevisionens främjande uppdrag i sin kommunikation – det vill säga att vi ska bidra till att förbättra verksamheterna vi granskar. Vår kommunikation kan dock se olika ut beroende på den målgrupp vi kommunicerar med och den kanal vi gör det genom. I det här avsnittet konkretiseras detta.

Målgrupper och kanaler

Revisionskontorets kommunikation har flera målgrupper. Målgrupperna går att dela in i fyra kategorier som vi prioriterar enligt följande:

1. **De granskade och medarbetare i Göteborgs Stad:** bolagsstyrelser, förtroendevalda politiker i kommunfullmäktige, förvaltningschefer, förvaltningsledningar, kommunstyrelsen, nämndledamöter, tjänstepersoner och vd:ar.
2. **Externa målgrupper:** allmänheten, journalister, medborgare i Göteborg.
3. **Förtroendevalda revisorer:** lekmannarevisorer och revisorsgruppen.
4. **Medarbetare på revisionskontoret:** direktionen, verksamhetsstödet och yrkesrevisorerna.

Kanalerna är de vägar som vi använder för att nå våra målgrupper och de vägar som målgrupperna använder för att nå oss. I riktlinjen beskriver vi vilka kanaler som vi ska prioritera i vilka lägen. Valet av kanaler ska alltid möta målgruppens behov, kunskaper och förutsättningar.

För att säkerställa att kommunikationen främjar en hållbar utveckling ska vi undvika kanaler som innebär trycksaker eller pappersutskick.

De granskade och medarbetare i Göteborgs Stad

Digitala navet

Digitala navet är Göteborgs Stads intranät. När den här riktlinjen skrivs är plattformen fortfarande inte lanserad. Funktionaliteten i Digitala navet är däremot känd och utifrån detta planerar vi vår kommunikation i navet.

I Digitala navet finns möjlighet att målgruppsanpassa kommunikationen, både på organisationsnivå och på funktion/roll. Revisionskontoret ska sträva efter att använda de

[2] Revisionens kommunikation (SKR). 2021. s. 10.

möjligheter som navet erbjuder och därigenom utveckla stadsrevisionens interna kommunikation i Göteborgs Stad.

Vi ska alltid överväga Digitala navet som en kanal när de granskade och medarbetare i Göteborgs Stad är målgrupper.

E-post och telefon

Bilden av stadsrevisionen påverkas av varje enskild tjänstepersons kommunikation med verksamheterna. Telefon- och mejlkommunikationen med de granskade ska därför alltid vara saklig och korrekt.

Revisionskontoret ska alltid meddela de granskade verksamheterna när vi har påbörjat och avslutat en granskning. Vi gör bland annat detta genom e-post.

Allmänheten kan begära ut all e-post, såväl extern som intern. Det är därför viktigt att alla medarbetare på revisionskontoret följer *Göteborgs Stads regler för användande av e-post*.

I kontakten med de granskade och medarbetare i Göteborgs Stad ska vi alltid använda Göteborgs Stads aktuella mejlsignatur. Mallen för mejlsignaturen finns på Göteborgs Stads intranät.

Externa webbsidor

Stadsrevisionens externa webbsidor är först och främst relevanta för en extern målgrupp men de är också relevanta för Göteborgs Stads medarbetare och politiker. Revisionskontoret publicerar planer, rapporter, redogörelser och berättelser på de externa webbsidorna. De externa webbsidorna är den enda kanalen för medarbetare i Göteborgs Stad att hitta dessa, bortsett från nämndernas och bolagens egen ärendehantering. Det är därför viktigt att vi tar hänsyn till även denna målgrupp när vi planerar för struktur och innehåll på de externa webbsidorna.

Revisionskontoret ska alltid meddela verksamheter och politiker i Göteborgs Stad när vi har påbörjat och avslutat en granskning. Vi gör bland annat detta på våra webbsidor.

Möten och Microsoft Teams

Möten som en del av granskningen och möten där vi vill kommunicera våra granskningsresultat ska vara sakliga och korrekta. När vi planerar in möten eller deltar i nätverk i Göteborgs Stad för att nå ut med granskningsresultaten ska vi göra det utifrån en strategisk avvägning över vilka målgrupper som vi tjänar mest på att kommunicera med.

Alla medarbetare ska använda den senaste versionen av Göteborgs Stads mall för PowerPoint-presentationer. Varje gång vi tar fram en ny presentation ska vi därför hämta en ny mall från Göteborgs Stads mallsystem – Mallgeneratorn. På detta sätt säkerställer vi att vi alltid använder aktuella mallar.

Vi ska använda oss av digitala möten genom Microsoft Teams när det gagnar verksamheten.

Externa målgrupper

E-post och telefon

De vanligaste kanalerna som allmänheten använder sig av när de vänder sig till stadsrevisionen är e-post och telefon.

När vi får frågor från allmänheten är det viktigt att komma ihåg att varje medarbetare har serviceskyldighet enligt 4§ i förvaltningslagen. Enligt den ska vi lämna upplysningar, vägledning, råd och annan hjälp i enskilda frågor som rör stadsrevisionens verksamhetsområde. Om vi inte kan svara ska vi vidarebefordra frågan till någon som kan. Ärenden som innehåller tips eller förslag på granskningar ska vi om möjligt hänvisa till förvaltningsbrevlådan. Frågor från enskilda ska besvaras så snart som möjligt.

Allmänna handlingar som kommer in till revisionskontoret eller har blivit upprättade på kontoret ska diarieföras. Undantaget är handlingar som hålls ordnade på något annat sätt som gör dem sökbara, exempelvis hålls i kronologisk ordning och att de inte innehåller sekretesskyddade uppgifter. Inte heller handlingar som är av ringa betydelse för myndighetens verksamhet behöver diarieföras. Handlingar som innehåller sekretessbelagda uppgifter måste alltid diarieföras. Reglerna om diarieföring finns i offentlighet- och sekretesslagen.

Allmänheten kan begära ut all e-post, såväl extern som intern. Det är därför viktigt att alla medarbetare på revisionskontoret följer *Göteborgs Stads regler för användande av e-post*.

I kontakten med externa målgrupper ska vi alltid använda Göteborgs Stads aktuella mejlsignatur. Mallen för mejlsignaturen finns på Göteborgs Stads intranät.

Externa webbsidor

Stadsrevisionens externa webbsidor är en del av goteborg.se och ska följa Göteborgs Stads riktlinjer, manualer, instruktioner och tips gällande webb.

De externa webbsidorna är en av de viktigaste kanalerna för att nå ut till allmänheten med våra granskningar och för att beskriva vårt uppdrag. Vi ska därför ständigt arbeta för att synliggöra vår granskning så tydligt som möjligt på våra webbsidor.

Webbsidorna ska ha en tydlig struktur, hög kvalitet och vara tillgänglighetsanpassade. Våra besökare ska lätt hitta vad de letar efter. Innehållet ska ha hög sökbarhet och vi ska arbeta aktivt med sökordsoptimering.

Vi ska meddela att vi har påbörjat en granskning genom att publicera granskningsplanen på våra webbsidor. Alla granskningar ska slutredovisas i rapporter eller redogörelser som också publiceras på våra webbsidor.

Massmedier

Denna kanal skiljer sig från de övriga kanalerna eftersom den ger möjlighet att nå ett stort antal målgrupper på en och samma gång, samtidigt som vi själva inte alltid styr över exakt när eller hur det sker.

Kontakterna med massmedia ska präglas av öppenhet och proaktivitet. Revisionskontoret ska så långt det går säkerställa nyhetsvärdet och sakligheten när det gäller såväl positiva som negativa budskap. Vi ska göra detta genom att själva formulera pressmeddelanden och förbereda de förtroendevalda revisorerna som ska medverka i media.

Massmedia ska snabbt kunna komma i kontakt med presskontakten på stadsrevisionen. I normalfallet är det ordförande eller vice ordförande i revisorsgruppen som är presskontakt och som uttalar sig i media. När ett pressmeddelande rör en bolagsgranskning är det lekmannarevisorerna för det aktuella bolaget som uttalar sig. Kommunikationsansvarig på revisionskontoret ska alltid ge stöd åt den som ska medverka i media. Den yrkesrevisor som har ansvar eller kompetens i en sakfråga för en medial granskning ska finns tillgänglig att svara på frågor.

Stadsrevisionens rapporter och redogörelser innehåller revisionskontorets iakttagelser och bedömningar. De förtroendevalda revisorerna utgår ifrån rapporterna och redogörelserna när de gör sina bedömningar. Det är också de förtroendevalda revisorerna som svarar för sina ställningstaganden och bedömningar i kontakter med massmedia. Yrkesrevisorerna svarar för att förklara iakttagelser och granskningsmetoder för massmedia om det finns ett behov.

Pressmeddelanden

Revisionskontoret ska så långt det är möjligt utforma pressmeddelande enligt Göteborgs Stads manual för pressmeddelanden. Vi ska fokusera på det som är intressant för en journalist att lyfta i sin rapportering. Det är dock viktigt att vi är trogna våra granskningar och använder samma formuleringar som i våra redogörelser och rapporter när det är nödvändigt. Bedömningar och iakttagelser ska vara de samma oavsett om någon läser pressmeddelandet eller redogörelsen/rapporten.

Kommunikationsansvarig, den granskningsansvariga och revisionsdirektören utvärderar nyhetsvärdet i granskningarna och lämnar sin bedömning till revisorsgruppens presidium. Revisorsgruppen beslutar om stadsrevisionen ska gå ut med ett meddelande eller inte. Kommunikationsansvarig skriver ett pressmeddelande när det är aktuellt, exempelvis när en nämnd eller ett bolag får kritik samt i vissa fall när en projektgranskning är klar.

När stadsrevisionens förtroendevalda revisorer medverkar i ett pressmeddelande är det på uppdrag från hela revisorsgruppen. Vid pressmeddelanden som rör bolagen anger vi de aktuella lekmannarevisorerna och kommunikationsansvarig som presskontakter. Vid pressmeddelanden som rör nämnderna anger vi revisorsgruppens ordförande och vice ordföranden samt kommunikationsansvarig som presskontakter.

Pressmeddelanden går ut genom Göteborgs Stads aktuella presstjänst. Förnärvarande Mynewsdesk.

Sociala medier

Stadsrevisionen har inte några egna sociala medie-kanaler. I de fall vi behöver använda sociala medier gör vi det genom Göteborg Stads officiella kanaler.

Förtroendevalda revisorer

Revisorsgruppen och lekmannarevisorerna är revisionskontorets uppdragsgivare. Arbetsformer mellan de förtroendevalda revisorerna och revisionskontoret finns i första hand reglerat i dokumentet *Arbetsordning för revisorsgruppen i Göteborgs Stad*. I arbetsordningen tydliggörs hur revisionskontoret ska förhålla sig kommunikativt till revisorsgruppen och lekmannarevisorerna.

I dokumentet *Tidplaner för underlag till RG* finns en detaljerad beskrivning av hur ansvarsfördelningen, arbetsprocesserna och tidplanerna ser ut när revisionskontoret ska ta fram underlag till de förtroendevalda revisorerna.

Medarbetare på revisionskontoret

Digitala navet

Digitala navet är Göteborgs Stads intranät. När den här riktlinjen skrivs är plattformen fortfarande inte lanserad. Funktionaliteten i Digitala navet är däremot känd och utifrån detta planerar vi vår kommunikation i navet.

Digitala navet är huvudkanalen för intern information som riktar sig till medarbetare på revisionskontoret. Varje medarbetare ansvarar därför för att hålla sig uppdaterad genom att kontinuerligt besöka Digitala navet. Särskilt viktig information – till exempel information som är nödvändig för medarbetarnas dagliga arbete, inbjudningar eller anmälningar – ska däremot gå ut via e-post för att säkerställa att ingen medarbetare missar extra viktig information.

Digitala navet ska innehålla information som är specifik för revisionskontoret, så kallade *specifika tillägg*. Kommunikationsansvarig ansvarar för att alla specifika tillägg som behövs finns på plats. Kommunikationsansvarig ansvarar också för att varje år gå igenom innehållet i alla specifika tillägg, för att säkerställa att de är uppdaterade med aktuell information.

Kommunikationsansvarig publicerar kontinuerligt nyheter som riktar sig till medarbetarna på revisionskontoret. Nyheterna kan vara information om: ledningsbeslut, lagar och riktlinjer, våra granskningar, kurser, föreläsningar, rapporter, uppsatser, it, telefoni och personalfrågor. Information som bara rör några få mejlar vi ut till de berörda.

Ledningsgruppen ska använda Digitala navet för att informera om vad de har behandlat under sina möten.

Vi ska inte publicera lokala styrdokument, lokal information som rör säkerhet eller information om vårt revisionella arbetssätt i Digitala navet.

Vi ska inte heller publicera känsliga personuppgifter, så som facklig tillhörighet, i Digitala navet. Kommunikationsansvarig ansvarar dessutom för att vid varje enskild publicering i Digitala navet minimera antalet personuppgifter så långt det går utan att informationen förlorar sin innebörd. I de fall kommunikationsansvarig behöver publicera personuppgifter i Digitala navet ska alltid ett godkännande inhämtas från den berörda.

E-post

E-post ska alltid värderas, sållas och anpassas efter mottagaren och inte spridas rutinmässigt till alla på revisionskontoret. Vi ska endast använda massutskick av e-post vid undantag, då något är av mycket hög relevans eller behöver nå medarbetare utan dröjsmål. Särskilt viktig information – till exempel information som är nödvändig för medarbetarnas dagliga arbete, inbjudningar eller anmälningar – ska alltid gå ut via e-post för att säkerställa att ingen medarbetare missar extra viktig information. Om du som medarbetare är osäker på hur informationen ska spridas ska du rådfråga kommunikationsansvarig.

Allmänheten kan begära ut all e-post, såväl extern som intern. Det är därför viktigt att alla medarbetare på revisionskontoret följer *Göteborgs Stads regler för användande av e-post*.

Lotus Notes/Visma Ciceron

När den här riktlinjen tas fram använder revisionskontoret Lotus Notes som dokumenthanteringssystem. Alla yrkesrevisorer och kvalitetssäkrare ska arbeta med kontorets rapporter i detta system. Granskningarna som kontoret gör mynnar ut i olika typer av rapporter. Kommunikationen som sker i Lotus Notes/Visma Ciceron i arbetet med rapporterna ska följa ett bestämt arbetssätt.

Under våren 2023 är det tänkt att Visma Ciceron ska ersätta Lotus Notes. Vad detta innebär för revisionskontorets arbete och kommunikation kring kontorets rapporter kommer tydliggöras när det nya dokumenthanteringssystemet är på plats.

Möten, Microsoft Teams och Outlook

Cheferna ska göra verksamhetens mål och fattade beslut begripliga i dialog med medarbetarna. Via regelbundna kontorsmöten har revisionsdirektören och avdelningscheferna möjlighet att informera hela revisionskontoret om senaste nytt inom organisationen. Administrativ chef ger information till verksamhetsstödet vid veckoliga möten. Avdelningscheferna ger information till respektive avdelnings medarbetare vid avdelningsmöten.

Revisionskontoret uppmuntrar digitala möten framför fysiska möten som kräver längre resor. Det är mötesarrangören som avgör om ett möte ska hållas på plats eller digitalt men verksamhetens behov måste dock alltid gå först i valet av mötesform.

Vissa återkommande möten hålls alltid på plats på revisionskontoret. För mer information om vad som gäller se *Rutin för flexibel arbetsplats*.

Revisionskontorets medarbetare ansvarar för att ha en uppdaterad och för revisionskontoret öppen Outlook-kalender. En uppdaterad och öppen kalender gör det lättare för en mötesarrangör att boka in ett möte.

Ansvar och roller

Alla medarbetare på revisionskontoret har ett ansvar att följa *Revisionskontorets riktlinje för kommunikation*. Vissa roller har dock ett särskilt kommunikativt ansvar. Här tydliggörs vilka de är.

Kommunikationsansvarig

Kommunikationsansvarig ingår i ledningsgruppen och har både ett strategiskt och operativt ansvar i det övergripande kommunikationsarbetet på revisionskontoret.

Hen ska vara stödjande i allt arbete som ledningsgruppen bedriver men särskilt när det kommer till kommunikativa frågor.

Kommunikationsansvarig ska hålla sig uppdaterad om vad som händer inom kommunikationsområdet, både i allmänhet och i Göteborgs Stad. På detta sätt kan hen sedan föra in relevanta arbetssätt i revisionskontorets organisation.

Pressarbete, externa webbsidor, intranät, klarspråk, tillgänglighet och mallhantering är områden som kommunikationsansvarig har särskilt ansvar för.

Ledningsgrupp

Inom Göteborgs Stad följer ansvaret för kommunikation med ansvaret för verksamheten. Revisionsdirektören beslutar om strategiska kommunikationsfrågor efter beredning i ledningsgruppen.

Vidare informerar och kommunicerar ledningsgruppen om den egna verksamhetens mål och uppdrag. När de gör det ska kommunikationen från ledningsgruppen vara enhetlig och gemensam.

Ledningsgruppen ska även fånga upp synpunkter från medarbetare och visa att de har övervägts eller tagits om hand. Det ska därför finns en struktur för återkoppling mellan revisionskontorets medarbetare och ledningsgruppen, vid de tillfällen när det behövs.

Ledningsgruppen utgör revisionskontorets krisledningsgrupp. Ansvaret för kriskommunikationen följer linjeorganisationen och går att läsa mer om i *Krisledningsplan stadsrevisionen*.

Nämndsekreterare och registrator

Nämndsekreterare och registrator innefattas i en och samma roll (hädanefter ”nämndsekreteraren”). Rollen innebär en central funktion i det operativa kommunikationsarbetet.

Nämndsekreteraren ansvarar särskilt för diariet, arkivet, förvaltningsbrevlådan, medborgarärenden, protokollföring och alla former av expediering.

I sitt protokoll- och dokumentationsarbete ska nämndsekreteraren alltid använda sig av de mallar som Göteborgs Stad förordar.

I sin kommunikation med allmänheten ska nämndsekreteraren alltid använda ett vårdat, enkelt och begripligt språk.

Yrkesrevisorer

Yrkesrevisorerna kommunicerar i alla delar av revisionsprocessen och har därför ett särskilt ansvar för relationen stadsrevisionen har till förvaltningar, bolag och nämnder. All kontakt med granskade verksamheter ska därför präglas av ett sakligt och korrekt

förhållningssätt. Yrkesrevisorerna ska också ta hänsyn till stadsrevisionens främjande uppdrag i sin kommunikation – det vill säga att vi ska bidra till att förbättra verksamheterna.

Varje yrkesrevisor ansvarar för att revisionskontorets rapportering sker i uppdaterade mallar. I alla texter de skriver ska de använda ett vårdat, enkelt och begripligt språk.

Genomförande

Budskap

Vid de flesta tillfällen kommunicerar revisionskontoret kring granskningsresultat. Vad vi väljer att lyfta fram skiljer sig åt beroende på målgrupp och kommunikationsform. Vi ska därför vid varje granskning tänka igenom vilka iakttagelser som är viktigast att lyfta fram och på vilket sätt för respektive målgrupp.

Revisionskontoret ska alltid förhålla sig till stadsrevisionens mål när vi formulerar våra budskap:

- Vi ska vara oberoende, publika och tydliga.
- Vi ska ha hög trovärdighet och skapa högt förtroende för revisionens iakttagelser.
- Vi ska arbeta stödjande genom att granskning bidrar till en ändamålsenlig verksamhet.

Utöver detta har revisionskontorets medarbetare ett gemensamt ansvar att kommunicera och förklara stadsrevisionens uppdrag och arbetssätt.

Så benämner vi olika delar av vår verksamhet

Det finns flera olika benämningar inom ramen för organisationen stadsrevisionen. Vi använder olika benämningar beroende på vilken del av verksamheten vi vill hänvisa till. Här följer en uppställning över vid vilka tillfällen som respektive benämning är lämplig att använda:

- **Stadsrevisionen** använder vi när vi pratar om hela organisationen som innefattar förtroendevalda revisorer, lekmannarevisorer och tjänstepersoner på revisionskontoret.
- **Revisionskontoret** använder vi när vi enbart pratar om tjänstepersoner på revisionskontoret.
- **Revisorsgruppen** använder vi när vi pratar om de 22 förtroendevalda revisorerna som grupp.
- **Revisorskollegiet** är vår motsvarighet till en nämnd. Revisorskollegiet består av 7 ledamöter och 4 ersättare. Samtliga är hämtade ur revisorsgruppen.
- **Presidiet** är benämningen på ordförande och vice ordförande i revisorskollegiet. De är också ordförande och vice ordförande i revisorsgruppen.
- **Lekmannarevisorer** använder vi när vi pratar om de förtroendevalda revisorer som är utsedda lekmannarevisorer i Göteborgs Stads bolag.

Dialog och förtroendeskapande

I *Revisionens kommunikation* utgiven av SKR står att:

> En revision som arbetar aktivt med sin kommunikation och dialog blir synlig. Synligheten bidrar till att revisionens iakttagelser och bedömningar tas emot bättre. Detta leder i sin tur till att revisionen kan arbeta främjande, det vill säga hjälpa kommunen eller regionen att utveckla och förbättra verksamheten.[3]

Revisionskontorets medarbetare ska därför alltid ta hänsyn till stadsrevisionens främjande uppdrag i sin kommunikation – det vill säga att vi ska bidra till att förbättra verksamheterna vi granskar.

Kommunikation vid kris

Enligt *Göteborgs Stads riktlinje för krisberedskap och kriskommunikation* ska bolag och förvaltningar ha en plan för krisberedskap och kriskommunikation. Revisionskontoret har tagit fram en krisledningsplan för hela stadsrevisionen – *Krisledningsplan stadsrevisionen*. I den finns ansvar och tillvägagångssätt när det kommer till kommunikationsarbetet i händelse av kris.

Omvärldsbevakning

Ledningsgruppen har beslutat att tills vidare inte använda något av de omvärldsbevakningsverktyg som Göteborgs Stad har ramavtal med. Revisionskontoret har dock möjlighet till omvärldsbevakning genom prenumeration på Göteborgs-Posten och Mynewsdesk.

Kommunikationsansvarig ansvarar för att omvärldsbevakningen när det kommer till kommunikation- och pressarbete.

Språk och klarspråk

I enhetlighet med Språklagen (2009:600) är revisionskontorets officiella kommunikationsspråk svenska. Av språklagen framgår vidare att språket i offentlig verksamhet ska vara vårdat, enkelt och begripligt. Det är därför väsentligt att revisionskontorets medarbetare strävar efter att uttrycka sig klart och begripligt i sin kommunikation.

Som ett led i detta arbete ska revisionskontoret arbeta aktivt med klarspråk för att göra våra texter vårdade, enkla och begripliga. Arbetet ska ske genom att revisionskontoret tar fram stödmaterial, erbjuder utbildningar och kontinuerligt följer upp arbetet. Medarbetare ansvarar för att aktivt ta del av underlag och utbildningar.

Tillgänglighet och mallar

2018 blev webbtillgänglighetsdirektivet lag. Detta innebär att alla offentliga myndigheter ska kommunicera enligt direktivet.

Kommunikationsansvarig på revisionskontoret ansvarar för att vi följer webbdirektivet när det gäller text, bild och rörlig bild på stadsrevisionens externa webbsidor. Detta innebär även att kommunikationsansvarig ska säkerställa att alla PDF-dokument som vi

[3] Revisionens kommunikation (SKR). 2021. s. 10.

publicerar på våra webbsidor är tillgänglighetsanpassade. Dokument som inte är tillgänglighetsanpassade får inte publiceras på de externa webbsidorna.

Mallar

I Göteborgs Stads mallsystem – Mallgeneratorn – finns både Göteborgs Stads mallar och revisionskontorets mallar. Kommunikationsansvarig ansvarar för att revisionskontorets mallar följer tillgänglighetsdirektivet och är uppdaterade.

Alla medarbetare ska underlätta arbetet med tillgänglighet genom att använda uppdaterade mallar. Vi ska därför alltid börja skriva i en ny mall från Mallgeneratorn varje gång vi tar fram en ny plan, rapport, redogörelse, berättelse eller ett tjänsteutlåtande.

Allt material som revisionskontoret offentliggör på stadsrevisionens webbsidor ska vara skrivet i uppdaterade mallar. Mallarna ska vara ett stöd för revisionskontorets revisorer och ska säkerställa att vi skriver på ett tillgängligt och enhetligt sätt.

Prioriteringar

Revisionskontorets kommunikationsarbete ska följa en prioriteringsordning, i de fall när det behövs. Prioriteringen är främst till för att kommunikationsansvarig ska kunna avgöra var fokus behöver ligga när arbetsbördan är extra stor. I det dagliga arbetet och bland medarbetare generellt är alla delar att betrakta som lika viktiga.

1. **Kommunikation i samband med rapportering och planering av granskningar**
   Granskningen av Göteborgs Stads verksamheter är revisionskontorets kärnverksamhet. Därför ska detta arbete alltid prioriteras.

2. **Centrala projekt från Göteborgs Stad**
   Göteborgs Stad genomför kontinuerligt förändringsprojekt inom kommunikation. När revisionskontoret är en del av sådana projekt är de viktiga att prioritera i det dagliga arbetet.

3. **Klarspråksarbete och mottagaranpassning**
   Det finns flera anledningar för revisionskontoret att arbeta aktivt med klarspråk och mottagaranpassning. Som myndighet har vi enligt lag skyldighet till detta, det är en demokratisk fråga och dessutom har enkätundersökningar med kommunfullmäktige under flera mandatperioder i rad visat på att vi måste göra våra rapporter mer lättillgängliga. På grund av detta är klarspråk ett prioriterat område.

4. **Internkommunikation på revisionskontoret och i Göteborgs Stad**
   Möjligheterna till internkommunikation utvecklas just nu mycket inom Göteborgs Stad. Främst genom att kommunen inför Digitala navet som nytt intranät. Revisionskontoret ska prioritera att utveckla internkommunikationen med hjälp av Digitala navet och de möjligheter som det erbjuder.

Uppföljning

Revisionskontoret ska löpande följa upp kommunikationsinsatser, interna såväl som externa. Detta ska ske i den utsträckning det är nödvändigt i förhållande till insatsens storlek och med de verktyg som Göteborgs Stad erbjuder.

Kommunikationsansvarig ska följa upp statistik kring stadsrevisionens externa webbsidor och rapporter. Kommunikationsansvarig ska även följa den rapportering som sker om stadsrevisionen i media och i sociala medier. Vid behov ska kommunikationsansvarig rapportera om detta till ledningsgruppen. I särskilda fall kan ledningsgruppen välja att lyfta ett enskilt fall till alla medarbetare på kontoret genom exempelvis revisionsforum.

11 Bilaga 3 – Dokumenthanteringsplan för stadsrevisionen

Göteborgs Stad
Stadsrevisionen

Dokumenthanteringsplan

Dnr 0314/17

Antagen av Stadsrevisionen – Göteborgs stad 2017-11-28

Gäller handlingar upprättade från 2017-01-01

Inledning

Stadsrevisionen beslutade den 2017-11-28 att anta denna dokumenthanteringsplan som gäller handlingar upprättade från och med 2017-01-01 och i och med detta upphör den tidigare dokumenthanteringsplanen med diarienummer 0279/15 att gälla. För att inte dela på handlingar som inkommit under 2017 så tillämpas dokumenthanteringsplanen från 2017-01-01.

Stadsrevisionen utgörs dels av revisionskontoret med yrkesrevisorer och administratörer, dels av förtroendevalda revisorer och upphandlade revisionsbyråer. Myndigheten bildades 1961 och samtidigt delades Göteborgs styrelser, nämnder och stiftelser in i nio olika grupper. Ordföranden för varje revisorsgrupp bildade stadens revisorskollegium. Kollegiets beredande och verkställande organ var revisionskontoret. Sedan 1989 utgör samtliga stadens styrelser och nämnder ett revisionsområde. När Västra Götalandsregionen bildades 1998 lyftes revisionen av bland annat sjukvårdsnämnderna från stadsrevisionen.

Arkiv som myndigheten förvarar

Handlingar från 1813 till 1960 från Drätselkammaren finns på Stadsarkivet, arkivnummer 661. Handlingar från stadsrevisionen mellan åren 1961 till 1995 har arkivnummer 97. Leveranser har skett med några års intervaller. Handlingar från 1995 och framåt förvaras i stadsrevisionens arkiv.

För mer information om arkivets innehåll för handlingar inkomna eller upprättade till och med den 31 januari 2017 se dokumenthanteringsplan, arkivbeskrivning och arkivförteckning (dnr 0279/15). För handlingar i ärenden öppna efter 1 februari 2017 se klassificeringsstruktur, arkivbeskrivning, arkivförteckning och denna dokumenthanteringsplan (dnr 0105/17)

Dokumenthanteringsplanens syfte och uppbyggnad

Syftet med dokumenthanteringsplanen är att säkerställa att handlingar i processerna hanteras på samma sätt varje gång och för att öka sökbarheten i arkivet. Den ger anvisningar om hur handlingar som tas emot eller upprättas ska hanteras och huruvida de ska diarieföras. Var handlingar ska förvaras och om de ska bevaras eller gallras.

Dokumenthanteringsplanen och diarieplanen är utformade efter Stadsrevisionens gällande klassificeringsstruktur som är antagen sedan 2017-02-01. Detta innebär att handlingarna redovisas utifrån myndighetens verksamhetsområden och processer. Handlingar av tillfällig eller ringa betydelse samt handlingar i projekt redovisas inte i planen utan redovisas sist i inledningen.

Dokumenthanteringsplanen är indelad i kolumner som beskriver vilket verksamhetsområde (VO), projektgrupp (PG) eller projekt (P) som handlingarna tillhör samt vilken beteckning (punktnotation). Vidare framgår om handlingen ska bevaras eller gallras samt vilket gallringsbeslut som stöder gallring. Tidigare utgjorde dokumenthanteringsplanen gallringsbeslut men i och med att Stadsrevisionen gick över till verksamhetsbaserad arkivredovisning den 1 februari 2017 så efter detta datum måste det finnas generella gallringsbeslut eller myndighetsspecifika gallringsbeslutfattade av regionsarkivet som stöder gallring, utan detta får handlingar inte gallras.

I kolumnen förvaring/sortering och arkivmedium anges var handlingen förvaras samt i vilket format. I kolumnen registreras anges om handlingen ska registreras i diariet. Observera att handlingar som ska lämnas ut alltid ska sekretessprövas eftersom det kan finnas uppgifter i alla handlingar som innehåller sekretess. Se vidare stadsrevisionens anvisning om "Utlämnande av allmän handling" som finns på intranätet under våra styrande dokument.

För mer information om stadsrevisionens arkiv se klassificeringsstruktur, arkivbeskrivning samt arkivförteckning

Handlingstyper som kan förekomma i alla processer: (Besluten tillämpas på handlingar som inkommit efter 2016-01-01, undantag för handlingar som inkommit i ärenden påbörjade innan 2015-12-31)

* Handlingar av tillfällig eller ringa betydelse gallras enligt arkivmyndigheterns gallringsbeslut AN 2016:1 (Stadsrevisionens tillämpningsbeslut dnr 0105/16 samt Hanteringsanvisning till beslutet dnr 0105/16)
* Gallring av pappershandlingar efter skanning sker enligt arkivmyndighetens gallringsbeslut AN 2016:3 (Stadsrevisionens tillämpningsbeslut dnr 0105/16 samt Hanteringsanvisning till beslutet dnr 0105/16)

Årsmapp - en mapp läggs upp varje år för handlingarna i den kategorin

VO, PG, P	Punkt-notation	Handlingstyp	Bevaras/ gallras	Gallringsbeslut	Registrering/ sortering	Arkiv-medium	Förvaring	Sekretess	Anmärkning
VO	**1.**	**Styra/Planera och följa upp**							
P	**1.1**	**Utföra politiskt ledningsarbete:**							
P	1.1	Delegationsbeslut	Bevaras		Registreras i diariet	Digitalt/ papper	LIS diariet		
P	1.1	Förteckning över inkomna skrivelser, revisorskollegiet	se anmärkning				Förvaras ej		Inbands med protokollet fram till 2004-09-30, senare förteckningar gallras efter respektive möte genomförts.
P	1.1	Revisorskollegiets protokoll	Bevaras		Kronologisk ordning	Papper	Kassaskåp plan 7	Nej	Inbindes per mandatperiod. Protokollen publiceras på hemsidan efter justering.
P	1.1	Anslagsbevis	Bevaras		Sorteras efter mötesdatum	Digitalt	I:mapp: Gemensam/ revisorskollegiet	Nej	
P	1.1	Revisorskollegiets föredragningslista	Bevaras		Kronologisk ordning	Digitalt	Lotus Notes databas		
P	**1.2**	**Planera, förvalta och följa upp verksamheten**							
P	1.2	Bokslut inklusive bilagor	Bevaras	Arkivnämnden AN 0194/16	Årsvis i arkivbox	Papper	Arkivet plan 8		Bevaras enligt Arkivnämndens gallringsbeslut AN 0194/16, se Stadsrevisionens tillämpningsbeslut dnr 0105/16
P	1.2	Delårsbokslut, delårsrapporter inkl bilagor	Bevaras	Arkivnämnden AN 0194/16	Årsvis i arkivbox	Papper	Arkivet plan 8		Bevaras enligt Arkivnämndens gallringsbeslut AN 0194/16, se Stadsrevisionens tillämpningsbeslut dnr 0105/16.
P	1.2	Mål och budget dokument	Bevaras		Registreras i diariet	Digitalt	LIS diariet		
P	1.2	Årsredogörelse	Bevaras		Registreras i diariet	Digitalt	LIS diariet	Nej	Sammanfattar årets granskning
P	1.2	Årsrapport/årsredovisning	Bevaras	Arkivnämnden AN 0194/16	Registreras i diariet	Digitalt / papper	LIS diariet		Bevaras enligt Arkivnämndens gallringsbeslut AN 0194/16, se Stadsrevisionens tillämpningsbeslut dnr 0105/16.
P	**1.3**	**Utföra internt ledningsarbete**							
P	1.3	Attestanter och utanordningsrättigheter, beslut	Bevaras		Registreras i diariet	Papper/ digitalt	LIS diariet		
P	1.3	Dokumenthanteringsplan	Bevaras		Registreras i diariet	Digitalt	LIS diariet	Nej	
P	1.3	Handlingsplaner och anvisningar	Bevaras		Intranätet under Revisionen internt	Digitalt	Intranätet		
P	1.3	Kallelser ledningsgruppen	Vid inaktualitet		Databas i Lotus Notes samt appen Handlingar	Digitalt	Lotus Notes		
P	1.3	Kontorsmöten mötesanteckningar	2 år efter aktuellt år är slut		Kronologisk ordning	Digitalt	Lotus Notes databas		

VO, PG, P	Punkt-notation	Handlingstyp	Bevaras/ gallras	Gallringsbeslut	Registrering/ sortering	Arkiv-medium	Förvaring	Sekretess	Anmärkning
P	1.3	Ledningsgruppens mötesanteckningar	Bevaras		Kronologisk ordning	Digitalt	Lotus Notes databas		Mötesanteckningar från och med 2010 finns i databasen, innan dess gallrades mötesanteckningarna.
P	1.3	Styrande dokument	Bevaras		Intranätet under Revisionen internt	Digitalt	Intranätet		Låg tidigare i Verksamhetshandboken i Lotus Notes, men har flyttats över till intranätet. Regler, anvisningar, rutiner och handlingsplaner etc.
P	**1.4**	**Utveckla verksamheten**							
P	1.4	Handlingar som rör verksamhetsutveckling	Bevaras		Registreras i diariet	Digitalt	LIS diariet		
P	**1.5**	**Hantera revision och granskning**							
P	1.5	Inspektionsprotokoll	Bevaras		Registreras i diariet	Digitalt/ papper	LIS diariet		T.ex. Brandskyddsprotokoll, Arbetsmiljöverket etc.
P	1.5	Internkontrollplaner/Anvisning för intern kontroll	Bevaras		Registreras i diariet	Digitalt/ papper	LIS diariet		
P	**1.6**	**Samverka och förhandla som arbetsgivare**							
P	1.6	Kallelser förvaltningens samverkansgrupp (FSG), kontorsmöten	Vid inaktualitet		Kronologisk ordning	Digitalt	Lotus Notes databas		
P	1.6	Protokoll, Förvaltningens samverkansgrupp (FSG)	Bevaras		Kronologisk ordning	Digitalt	Lotus Notes databas		1977-2006 i pärm, kassaskåpet pl 7. From 2006-08-29 förvaras protokollen enbart digitalt.
P	1.6	Protokoll från löneöversyn	Bevaras		Registreras i diariet	Digitalt/ papper	LIS diariet		
P	**1.7**	**Bedriva systematiskt arbetsmijöarbete**							
P	1.7	Skyddsrondsprotokoll	Bevaras		Kronologisk ordning		Hos skydds-ombudet		
P	**1.8**	**Besvara remisser och enkäter**							
P	1.8	Enkäter, svar, sammanställning och resultat	Bevaras		Registreras i diariet	Digitalt	LIS diariet		
P	**1.9**	**Hantera externa synpunkter och klagomål**							
P	1.9	Synpunkter från medborgare	Bevaras		Registreras i diariet	Digitalt/ papper	LIS diariet		
P	**1.10**	**Samverka med andra organisationer**							

VO, PG, P	Punkt-notation	Handlingstyp	Bevaras/ gallras	Gallringsbeslut	Registrering/ sortering	Arkiv-medium	Förvaring	Sekretess	Anmärkning
P	1.10	STAREV, styrelsehandlingar	Bevaras		Kronologisk ordning	Papper	Pärmar i arkivet plan 8		Starev är ett samarbetsorgan för förtroendevalda revisorer i kommuner, landsting och regioner. Under vissa år innehar Stadsrevisionen i Göteborg ordförandeskapet och upprättar protokoll m.m. som bevaras.
VO	**2**	**GE VERKSAMHESTSSTÖD**							
PG	**2.1**	**Administrera anställning och löner**							
P	**2.1.1**	**Rekrytera**							
P	2.1.1	Platsannons	Bevaras		Registreras i diariet	Digitalt	LIS diariet		Ett ärende öppnas per rekrytering. Annons och sammanställning över sökande registreras.
P	2.1.1	Anställningsbevis/avtal/förordnande	Bevaras		I personens personalakt	Papper	Personalakt		
P	2.1.1	Ansökning- och tillsättningshandlingar, erhållen tjänst	Bevaras		I personens personalakt	Papper	Personalakt		
P	2.1.1	Ansökning- och tillsättningshandlingar, ej erhållen tjänst	2 år efter anställnings-beslut		Sorteras efter inkomst datum	Papper	Pärm i arkivet plan 8		Ansökningarna finns även i Visma recruit, skrivs ut och bevaras i 2 år.
P	2.1.1	Sammanställning av sökande samt beslut om tillsättande av tjänst	Bevaras		Registreras i diariet	Digitalt	LIS diariet	Nej	Händelseregistreras i diariet
P	2.1.1	Spontanansökningar, ej utlyst eller ledigförklarad tjänst	Bevaras		Registreras i diariet	Digitalt	LIS diariet		Spontanansökningar och praktikförfrågningar samlas under ett diarienummer varje år.
P	**2.1.2**	**Hantera anställning**							
P	2.1.2	Anmälan om dödsfall	Bevaras		I personens personalakt	Papper	Personalakt		
P	2.1.2	Arbetsgivarintyg	Bevaras		I personens personalakt	Papper	Personalakt		
P	2.1.2	Begäran om avgång	Bevaras		I personens personalakt	Papper	Personalakt		
P	2.1.2	Disciplinära åtgärder	Bevaras		Registreras i diariet	Papper/ digitalt	LIS diariet		Diarieförs och kopia läggs i personalakt.
P	2.1.2	Fritidsstudier	Bevaras		I personens personalakt	Papper	Personalakt		
P	2.1.2	Gratifikationer	Bevaras		I personens personalakt	Papper	Personalakt		
P	2.1.2	Korttidsvikariat	Bevaras		I personens personalakt	Papper	Personalakt		
P	2.1.2	Las-handlingar	Bevaras		I personens personalakt	Papper	Personalakt		Anmälan om företrädelserätt, besked till arbetstagare och facklig organisation, erbjudande om ny anställning, svar från arbetstagare.

VO, PG, P	Punkt-notation	Handlingstyp	Bevaras/ gallras	Gallringsbeslut	Registrering/ sortering	Arkiv-medium	Förvaring	Sekretess	Anmärkning
P	2.1.2	Lista på anhörigkontaktperson för personal	Uppdateras ständigt		Registreras i Personec	Digitalt	Hos administratör		Namn, telefonnummer m.m.
P	2.1.2	Personalakt	Bevaras		I personnummers-ordning	Papper	Aktskåp plan 8	Ja (21 kap OSL)	Sekretesspröva alltid innan utlämning. Avslutade personalakter förvaras i arkivboxar i arkivet på plan 8 i personnummerordning.
P	2.1.2	Pensionsunderlag	Bevaras		I personens personalakt	Papper	Personalakt		
P	2.1.2	Tystnadsplikt/sekretessförbindelse	Bevaras		I personens personalakt	Papper	Personalakt		
P	2.1.2	Telefonlistor tex. anställda och förtroendevalda	Uppdateras ständigt		Intranätet under Revisionen internt	Digitalt	Intranätet	Nej	Uppdateras regelbundet och den tidigare versionen gallras.
P	2.1.2	Tystnadsplikt/sekretessförbindelse tillfällig personal	Bevaras		Personnummerordning	Papper	Pärm i kassa-skåp		
P	**2.1.3**	**Beräkna och betala ut löner, arvoden och pension**							
P	2.1.3	Arvodesunderlag och reseräkningar, förtroendevalda	10 år efter inkomstårets slut		Pärm i arkivet plan 8	Papper	Förtroende-mannarutinen		
P	2.1.3	Löneunderlag och underlag till arvoden som tidkort, friskvårdsbidrag, rättelser, rikskuponger, kvittenser m m.	2 år efter inkomstårets slut		Pärm/ Personec	Papper/ digitalt	I Personec		Gäller personal, registreras i Personec
P	2.1.3	Läkarintyg, övriga	2 år efter inkomstårets slut		Registreras ej	Papper	Hos administatör	Ja	Läkarintyg som gäller arbetsskada diarieförs och bevaras. I 21 kap 1§ OSL regleras sekretess till skydd för uppgift om enskilds personliga förhållanden.
P	2.1.3	Facklig tid, rapporter och sammanställningar	2 år efter inkomstårets slut			Digitalt	Personec		
P	2.1.3	Reseräkningar och andra ersättningar till tjänstemän	2 år efter inkomstårets slut			Digitalt	Personec		
P	**2.2**	**Hantera bemanning**							
P	2.2	Ledighetsanmälan ledighet längre än 6 månader	Bevaras		I personens personalakt	Papper	Personalakt		Administratör registrerar i Personec och lägger anmälan i personalakten.
PG	**2.3**	**Hantera personalsocialafrågor**							
P	**2.3.1**	**Kompetensutveckla**							
P	2.3.1	Kurser och konferenser	5 år efter avslutad kurs/ konferens		Pärm	Papper	Arkivet plan 8	Nej	Innehåller deltagarförteckning, material etc till kurser/konferenser i egen regi samt anmälningar, kursplaner och inbjudningar till externa kurser och konferenser för anställd personal.

VO, PG, P	Punkt-notation	Handlingstyp	Bevaras/ gallras	Gallringsbeslut	Registrering/ sortering	Arkiv-medium	Förvaring	Sekretess	Anmärkning
P	**2.3.2**	**Tillhandahålla friskvård**							
P	2.3.2	Kvitto på utlägg för friskvård	2 år efter inkomstårets slut		Registreras av administratör	Papper/ digitalt	Personec		
P	2.3.2	Riktlinjer för friskvård	Vid inaktualitet		Intranätet under Revisionen internt	Digitalt			
P	2.3.2	Avtal angående friskvårdstjänster	Bevaras		Registreras i diariet	Papper/ digitalt	LIS diariet		
P	**2.3.3**	**Hantera tillbud, arbetsskada och otillåten påverkan**							
P	2.3.3	Anmälan om arbetsskada	Bevaras		Personalakt/Lisa	Papper/ digitalt			Rapporteras i Lisa
P	2.3.3	Läkarintyg arbetsskada	Bevaras		I personens personalakt	Papper	Personalakt	Ja	I 21 kap 1§ OSL regleras sekretess till skydd för uppgift om enskilds personliga förhållanden.
P	**2.3.4**	**Rehabilitera**							
P	2.3.4	Rehabiliteringsutredningar	Bevaras		I personens personalakt och registreras i Personec	Papper	Personec	Ja	Processkartläggningar förvaras i Personec. I 21 kap 1§ OSL regleras sekretess till skydd för uppgift om enskilds personliga förhållanden.
PG	**2.4**	**Administrera ekonomi**							
P	**2.4.1**	**Utforma och följa upp ekonomi**							
P	2.4.1	Budget	Bevaras	Arkivnämnden AN 0194/16	Registreras i diariet	Papper/ digitalt	LIS diariet	Nej	Bevaras enligt Arkivnämndens gallringsbeslut AN 0194/16, se Stadsrevisionens tillämpningsbeslut dnr 0105/16.
P	**2.4.2**	**Hantera intäkter från kund**							
P	2.4.2	Kundfakturor/kundinbetalningar	10 år efter räkenskaps-årets slut	Arkivnämnden AN 0194/16	Ekonomen administrerar dessa.	Digitalt	Agresso (Centralt)	Nej	Utgående fakturor (Tidigare kundfakturor från programmet Horisont finns på Cd-skivor i kassaskåpet). Gallras enligt Arkivnämndens gallringsbeslut AN 0194/16, se Stadsrevisionens tillämpningsbeslut dnr 0105/17.
P	**2.4.3**	**Hantera kostnader från leverantör**							
P	2.4.3	Leverantörsfakturor	10 år efter räkenskaps-årets slut	Arkivnämnden AN 0194/16	Skannas in av Intraservice	Digitalt	Gasell/Winst (centralt)	Nej	Hanteras av GAS/Intraservice från 2001 (Gasell och senare Winst). Fakturorna skannas in av Intraservice.Gallras enligt Arkivnämndens gallringsbeslut AN 0194/16, se Stadsrevisionens tillämpningsbeslut dnr 0105/17.

VO, PG, P	Punkt-notation	Handlingstyp	Bevaras/ gallras	Gallringsbeslut	Registrering/ sortering	Arkiv-medium	Förvaring	Sekretess	Anmärkning
P	2.4.3	Utbetalningsorder med underlag	10 år efter räkenskaps-årets slut	Arkivnämnden AN 0194/16		Digitalt/ papper	Agresso / pärm i arkivet på plan 8	Nej	Utbetalningsunderlag förvaras tillsammans med bokföring/dagrapporten i en verifikationspärm. Gallras enligt Arkivnämndens gallringsbeslut AN 0194/16, se Stadsrevisionens tillämpningsbeslut dnr 0105/17.
P	**2.4.4**	**Hantera löpande ekonomiredovisning**							
P	2.4.4	Bokföringsorder med underlag	10 år efter räkenskaps-årets slut	Arkivnämnden AN 0194/16	Underlag skrivs ut och förvaras kronologist i pärm	Digitalt/ papper	UBW (centralt)/pärm i arkivet plan 8		Gallras enligt Regionarkivets gallringsbeslut AN 0194/16, se Stadsrevisionens tillämpningsbeslut dnr 0105/17.
P	**2.4.5**	**Hantera skatteredovisning**							
P	2.4.5	Momsredovisning	10 år efter räkenskaps-årets slut	Arkivnämnden AN 0194/16		Digitalt	GAS (centralt)	Nej	Sammanställning månatligen av momsen förvaras i pärm. Momsen rapporteras till gemensam funktion i staden. Gallras enligt Arkivnämndens gallringsbeslut AN 0194/16, se Stadsrevisionens tillämpningsbeslut dnr 0105/17.
P	**2.4.6**	**Hantera försäkringar**							
P	2.4.6	Försäkringsinformation	Bevaras		Registreras i diariet	Digitalt	LIS diariet		
PG	**2.5**	**Köpa in och upphandla**							
P	**2.5.1**	**Köpa in, beställa och avtala (direktupphandling)**							
P	2.5.1	Beställningar, rekvisitioner	10 år efter räkenskaps-årets slut	Arkivnämnden AN 0194/16	Pärm i arkivet plan 8. Egen nummerserie	Papper	Nej	Nej	Gallras enligt Arkivnämndens gallringsbeslut AN 0194/16, se Stadsrevisionens tillämpningsbeslut dnr 0105/17.
P	2.5.1	Avtal som rör inköp och upphandling	Bevaras		Registreras i diariet	Papper/ digitalt	LIS diariet		
P	2.5.1	Förnyad konkurrensutsättning eller avrop mot ramavtal	Bevaras		Registreras i diariet	Digitalt	LIS diariet		Underlag, anbud, protokoll, tilldelningsbeslut, avtal diarieförs. För upphandlingar inom revision se VO 4.
P	2.5.1	Följesedlar om fakturan är komplett	2 år efter räkenskaps-årets slut	Arkivnämnden AN 0194/16	Kronologisk ordning. Efter datum för beställning.	Papper	Pärm i arkivet plan 8	Nej	Förvaras med beställningar i Beställningspärmen. Gallras enligt Arkivnämndens gallringsbeslut AN 0194/16, se Stadsrevisionens tillämpningsbeslut dnr 0105/17.
P	2.5.1	Följesedlar - hänvisning på fakturan	10 år efter räkenskaps-årets slut	Arkivnämnden AN 0194/16	Kronologisk ordning. Efter datum för beställning.	Papper	Pärm i arkivet plan 8	Nej	Förvaras med beställningar i Beställningspärmen. Gallras enligt Arkivnämndens gallringsbeslut AN 0194/16, se Stadsrevisionens tillämpningsbeslut dnr 0105/17
P	**2.5.2**	**Hantera upphandling enligt lagen om offentlig upphandling (LOU)**							
P	2.5.2	Upphandlingar enligt LOU	Bevaras		Registreras i diariet	Papper/ digitalt	LIS diariet		Underlag, anbud, protokoll, tilldelningsbeslut, avtal diarieförs. För upphandlingar inom revision se VO 4.

VO, PG, P	Punkt-notation	Handlingstyp	Bevaras/ gallras	Gallringsbeslut	Registrering/ sortering	Arkiv-medium	Förvaring	Sekretess	Anmärkning
P	2.5.3	Tilläggsavtal/avrop	Bevaras		Registreras i diariet	Papper/ digitalt	LIS diariet		
P	2.5.3	Uppsägningar av avtal	Bevaras		Registreras i diariet	Papper/ digitalt	LIS diariet		
PG	**2.6**	**Administrera allmänna handlingar**							
P	**2.6.1**	**Registrera handlingar och hantera post**							
P	2.6.1	Diarieplan	Bevaras		Registreras i diariet	Digitalt	LIS diariet	Nej	Diarieförs och arkiveras vid förändring.
P	2.6.1	Diarium, databas	Bevaras		Lotus Notes	Digitalt	Databas i Lotus Notes		
P	2.6.1	Diarieförda handlingar	Bevaras		Registrerade i diariet	Digitalt	LIS diariet		Från och med 2016-01-01 bevaras handlingarna enbart digitalt, se beslut om gallring efter skanning dnr 0105/16.
P	2.6.1	Fullmakt för öppning av direktställd post	Bevaras		I personens personalakt	Papper	Personalakt	Nej	
P	2.6.1	E-postloggar	Gallras efter 30 dagar	Arkivnämnden AN-5371/17	Förvaras hos Intraservice	Digitalt	Outlook	Nej	Se arkivnämndens beslut Dnr AN-5371/17 samt stadsrevisionens tillämpningsbeslut dnr 0105/17.
P	**2.6.2**	**Redovisa, styra och hantera handlingar och arkiv**							
P	2.6.2	Arkivbeskrivning	Bevaras	Arkivlagen (1990:782 §6)	Registreras i diariet	Digitalt	LIS diariet	Nej	
P	2.6.2	Arkivförteckning	Bevaras	Arkivlagen (1990:782 §6)	Registreras i diariet	Digitalt	LIS diariet	Nej	
P	2.6.2	Diariets innehåll i diarienummerordning	Bevaras			Papper/ digitalt	LIS diariet	Nej	Skrivs ut en gång per år och förvaras i arkivbox i kassaskåpet.
P	2.6.2	Saknummerregister (utskrift av diariet enligt diarieplansbeteckning)	Bevaras			Papper/ digitalt	LIS diariet	Nej	Skrivs ut en gång per år och förvaras i arkivbox i kassaskåpet.
P	**2.6.3**	**Ta emot arkiv**							
P	2.6.3								Stadsrevisionen saknar i nuläget sådana handlingar.
P	**2.6.4**	**Överlämna arkiv**							
P	2.6.4	Leveransreversal	Bevaras		Registreras i diariet	Digitalt	LIS diariet	Nej	
P	**2.6.5**	**Hantera utlämnande av allmänna handlingar**							
P	2.6.5	Beslut på vägran att lämna ut allmän handling	Bevaras		Registreras i diariet	Digitalt/ papper	LIS diariet		
P	2.6.5	Överklagande av beslut om vägran att lämna ut allmän handling	Bevaras		Registreras i diariet	Digitalt	LIS diariet		
P	**2.7**	**Kontrollera personuppgiftsbehandlingar**							

VO, PG, P	Punkt-notation	Handlingstyp	Bevaras/ gallras	Gallringsbeslut	Registrering/ sortering	Arkiv-medium	Förvaring	Sekretess	Anmärkning
P	2.7	Förteckning personuppgifter	Bevaras	Personuppgifts-lagen (1998:204)	Central databas per förvaltning	Digitalt	Lotus Notes		Personuppgiftsombudets lista över personregister. Gemensam databas för Göteborgs Stad.
P	**2.8**	**Hantera och förvalta IS/IT**							
P	2.8.1	Förstudie med kravspecifikation	Bevaras		Registreras i diariet	Digitalt	LIS diariet		
P	2.8.1	Beställning av nytt system samt leveransgodkännande	Bevaras		Registreras i diariet	Digitalt	LIS diariet		
P	2.8.2	Lathundar och användarmanualer för it-system	Vid inaktualitet		I:mappen	Digitalt	Nej		
P	2.8.2	Beställningar och bekräftelser på it-behörigheter	Vid inaktualitet		I:mappen (Gemensam/it och telefoni/behörigheter)	Digitalt	Nej		Sammanställs i lista av administratör som uppdateras vid förändringar av behörigheter.
P	2.8.3	Beställningar och bekräftelser på It-behörigheter	Vid inaktualitet		Gemensamt system i staden	Digitalt	Serviceportalen (centralt)		Görs genom elektronisk ansökan på stadens serviceportal, vi förvaras ej ansökan utan registrerar behörigheterna i en separat lista se 2.8.2
P	2.8.4	Incidentrapporter vid svagheter inom informationssäkerheten	Bevaras		Registreras i diarium	Digitalt	LIS diariet		
	2.8.4	Sårbarhetsanalyser	Bevaras		Registreras i diarium	Digitalt	LIS diariet		
P	2.8.5	Beslut och plan för avveckling av it-system	Bevaras		Registreras i diariet	Digitalt	LIS diariet		
PG	**2.9**	**Förvalta fastighet och inventarier**							
P	**2.9.1**	**Förvalta fastigheter och fysisk säkerhet**							
P	2.9.1	Inventarieförteckning	10 år efter avskrivning		Gemensamt system i staden	Digitalt	Webblisa		Förteckning finns i stadens leasingverktyg WebbLisa.
P	2.9.1	Hyresavtal	Bevaras		Registreras i diariet	Digitalt	LIS diariet		
P	**2.9.2**	**Hantera fysisk säkerhet och skalskydd**							
P	2.9.2	Polisanmälningar rörande stöld/hot/olaga intrång	Bevaras		Registreras i diariet	Digitalt	LIS diariet		
P	2.9.2	Inpasseringskoder/larmkoder/taggar	2 år efter inaktualitet		Lista förvaras hos säkerhetsansvarig	Papper/ digitalt			Lista över utlämnande och återlämnade nycklar/taggar.
P	**2.10**	**Informera, kommunicera och omvärldsbevaka**							
P	2.10	Egenproducerat informationsmaterial och trycksaker	Bevaras		Registreras i diariet	Papper/ digitalt	LIS diariet		
P	2.10	Prenumerationstjänst	Vid inaktualitet		Hanteras av kommunikatör	Distributionslista	Lotus Notes databas		Förteckning över e-postadresser till prenumeranter på Stadsrevisionens protokoll och rapporter. Uppdateras regelbundet.
P	2.10	Power Point-presentationer och andra presentationer	Vid inaktualitet		mapp I:/gemensam	Digitalt			

VO, PG, P	Punkt-notation	Handlingstyp	Bevaras/ gallras	Gallringsbeslut	Registrering/ sortering	Arkiv-medium	Förvaring	Sekretess	Anmärkning
VO	**3**	**Revision**							
P	**3.1.1**	**Planera granskning**							
P	3.1.1	Förstudier/arbetsmaterial	10 år efter året som granskningen utfördes	Arkivnämndens beslut AN-5296/17			Pärmar i arkivet plan 6 samt databasen Revy		Gallras enligt Arkivnämndens gallringsbeslut AN-5296/17, se Stadsrevisionens tillämpningsbeslut dnr 0105/17.
P	3.1.1	Revisionsplan	Bevaras		Registreras i diariet	Digitalt	LIS diariet		Upprättas en gång per år
P	**3.1.2**	**Granska årligen (ÅG)**							
P	3.1.2	Granskningsplan för bolag och nämnder	Bevaras		Registreras i diariet	Digitalt	LIS diariet		Finns även digitalt i ReVy
P	3.1.2	Följebrev till bolag och nämnder	Bevaras		Registreras i diariet	Digitalt	LIS diariet		Finns även digitalt i ReVy
P	3.1.2	Revisionsredogörelse och revisionsberättelse/sammanfattning för	Bevaras		Registreras i diariet	Digitalt	LIS diariet		Finns även digitalt i ReVy
P	3.1.2	Granskningsrapport och granskningsredogörelse för bolag	Bevaras		Registreras i diariet	Digitalt	LIS diariet		Finns även digitalt i ReVy
P	3.1.2	Lägesrapporter, bokslut, rapporter etc från konsulter	Bevaras		Registreras i diariet	Digitalt	LIS diariet		
P	3.1.2	Yttranden/svar från granskade nämnder/bolag	Bevaras		Registreras i diariet	Digitalt	LIS diariet		
P	3.1.2	Pressmeddelanden/information om granskningar	Bevaras		Registreras i diariet	Digitalt	LIS diariet		Diarieförs i mappen media som har en mapp för varje år.
P	3.1.2	Underlag till grund för revision (arbetsmaterial)	10 år efter året som granskningen utfördes		Pärm och/eller ReVy	Digitalt	Se anmärkning		Årsakter på granskad verksamhet finns digitalt i ReVy, en del handlingar förvaras i pärm i arkivet plan 6. Gallras enligt arkivnämndens beslut AN-5296/17, se stadsrevisionens tillämpningsbeslut 0105/17.
P	3.1.2	Handlingar från granskade nämnder av tillfällig och ringa betydelse	Vid inaktualitet		Förvaras hos handläggaren	Papper/ digitalt			Material som mottagits för kännedom och som inte ligger som grund till granskning, ex kallelse till nämndsammanträde, protokoll m.m.
P	**3.1.3**	**Granska fördjupat/i projekt (FG)**							
P	3.1.3	Revisionsrapporter/sammandrag	Bevaras		Registreras i diariet	Digitalt	LIS diariet		Fördjupade granskningar, finns även digitalt i ReVy.
P	3.1.3	Information till granskade enheter/Pressmeddelanden	Bevaras		Registreras i diariet	Digitalt	LIS diariet		
P	3.1.3	Projektplan	Bevaras		Registreras i diariet	Digitalt	LIS diariet		
P	**3.1.4**	**Granska för gemensam kvalitetssäkring**							
P	3.1.4	Rapport	Bevaras		Registreras i diariet	Digitalt	LIS diariet		Från och med 2016 års granskning diarieförs rapporten.

VO, PG, P	Punkt-notation	Handlingstyp	Bevaras/ gallras	Gallringsbeslut	Registrering/ sortering	Arkiv-medium	Förvaring	Sekretess	Anmärkning
PG	**3.2**	**Utbilda och informera**							
P	3.2	Utbildnings- och informationsmaterial	Vid inaktualitet			Digitalt	I:gemensam		Gäller förtroendevalda.
PG	**3.3**	**Hantera Revisorgruppens sammanträden**							
p	3.3	Revisorsgruppens anteckningar	Bevaras		Kronologisk ordning	Papper	Kassaskåp plan 7	Ja	Inbindes per mandatperiod. Sekretessen hävs då anteckningarna lämnas över till Revisorkollegiet, vilket görs i början av följande år.
p	3.3	Revisorsgruppens föredragningslista	Vid inaktualitet		Kronologisk ordning	Digitalt	Lotus Notes		
p	3.3	Förteckning över inkomna skrivelser revisorsgruppen	se anmärkning		Förvaras ej		Nej		Inbands med protokollet fram till 2004-09-30, senare förteckningar gallras efter respektive möte genomförts.
PG	**3.4**	**Ta emot rapportering från stadsdelsnämnder**							
P	3.4	Rapportering från SDN till Stadsrevisionen om ej verkställda biståndsbeslut	3 år efter det år som rapporten avser	Arkivnämndens beslut AN-6423/17	Per stadsdelsnämnd och kvartal	Papper	Pärmar i arkivet plan 6 samt databasen Revy		Gallras enligt arkivnämndens beslut AN-66423/17, se stadsrevisionens tillämpningsbeslut dnr 0105/17.
VO	**4**	**Upphandling**							
PG	**4.1**	**Hantera upphandling av revisionstjänster enligt lagen om upphandling LOU**							
P	4.1	Förfrågningsunderlag	Bevaras		Registreras i diariet	Digitalt	LIS diariet		
P	4.1	Tjänsteutlåtande och protokollsutdrag	Bevaras		Registreras i diariet	Digitalt	LIS diariet		
P	4.1	Frågor och svar under pågående upphandling	Bevaras		Registreras i diariet	Digitalt	LIS diariet		
P	4.1	Anbud, antagna	Bevaras		Registreras i diariet	Digitalt	LIS diariet	Ja	Anbuden omfattas av sekretess för det allmännas ekonomiska intresse (19 kap. 3 § 1 st OSL) t.ex. timpriser, sekretessprövas alltid innan utlämning.
P	4.1	Anbud, ej antagna	10 år efter tilldelnings-beslutet togs		Registreras i diariet	Papper/ digitalt	LIS diariet	Ja	Anbuden omfattas av sekretess för det allmännas ekonomiska intresse (19 kap. 3 § 1 st OSL) t.ex. timpriser, sekretessprövas alltid innan utlämning.
P	4.1	Anbudskvitto	Bevaras		Registreras i diariet	Digitalt	LIS diariet		
P	4.1	Annonsunderlag, beställningar, beställningsbekräftelser	5 år efter tilldelnings-beslutet togs		Registreras i diariet	Digitalt	LIS diariet		I förekommande fall när annonsering är lagstadgad.

VO, PG, P	Punkt-notation	Handlingstyp	Bevaras/ gallras	Gallringsbeslut	Registrering/ sortering	Arkiv-medium	Förvaring	Sekretess	Anmärkning
P	4.1	Öppningsprotokoll	Bevaras		Registreras i diariet	Papper och digitalt	LIS diariet	Ja	Förekommer det uppgifter om kostnader omfattas av öppningsprotokollen av sekretess för det allmännas ekonomiska intresse (19 kap. 3 § 1 st OSL) t.ex. timpriser, sekretessprövas alltid innan utlämning.
P	4.1	Utvärdering	Bevaras		Registreras i diariet	Papper och digitalt	LIS diariet	Ja	Förekommer det uppgifter om kostnader omfattas av utvärderingen av sekretess för det allmännas ekonomiska intresse (19 kap. 3 § 1 st OSL) t.ex. timpriser, sekretessprövas alltid innan utlämning.
P	4.1	Tilldelningsbeslut	Bevaras		Registreras i diariet	Papper och digitalt	LIS diariet	Nej	
P	4.1	Avtal/Kontrakt	Bevaras		Registreras i diariet	Papper och digitalt	LIS diariet		
P	4.1	Sekretessprövade anbudshandlingar	5 år efter tilldelnings-beslutet togs		Per upphandling och anbudsgivare	Papper	Pärm i arkivet plan 8	Nej	Kopior i pärm som kan lämnas ut efter avslutad upphandling.
P	4.1	Informationsmaterial som inte tillför sakuppgift till lämnat anbud	Vid inaktualitet		Förvaras hos upphandlingsansvarig	Papper/ digitalt	-		
PG	**4.2**	**Tillämpa förnyad konkurrensutsättning**							
P	4.2	Tilläggsuppdrag årlig granskning	Bevaras		Registreras i diariet	Digitalt	LIS diariet		

12 Bilaga 4 – Kommentarer och rekommendationer från dataskyddsombudet för stadsrevisionen

Kommentarer och rekommendationer från dataskyddsombudet

Konsekvensbedömning angående personuppgiftsbehandling - att informera och kommunicera i Digitala navet

1. Inledning och bakgrund

Stadsrevisionen i Göteborgs Stad granskar årligen all verksamhet i Göteborgs Stad i enlighet med lag och god sed. Ytterst ansvariga för denna verksamhet är de 22 förtroendevalda revisorerna i Staden. Revisorernas gemensamma förvaltning hanteras i enlighet med revisorernas reglemente av revisorskollegiet. Kollegiet består av 7 ordinarie ledamöter och 4 ersättare som utsetts av kommunfullmäktige bland revisorerna och kan i många stycken jämställas med en kommunal nämnd. Kollegiet företräder revisorerna i förvaltningsfrågor och utgör därigenom anställningsmyndighet, arkivansvarig och personuppgiftsansvarig för stadsrevisionens verksamhet.

Innan ett nytt IT-system ska tas i bruk så åligger det en personuppgiftsansvarig att pröva om användningen av det kommer att innebära behandling av personuppgifter som sannolikt leder till en hög risk för fysiska personers rättigheter enligt GDPR[1]. Om prövningen visar att så är fallet ska den personuppgiftsansvarige göra en konsekvens-bedömning i enlighet med artikel 35 i GDPR. En sådan konsekvensbedömning syftar till att klargöra vilka risker som finns för integritetsskyddet, hur den personuppgiftsansvarige hanterat dessa risker samt dokumentera den personuppgiftsansvariges arbete kopplat till detta. Om konsekvensbedömningen slutligen visar att där finns särskilt höga kvarstående risker som inte hanterats på ett tillfredställande sätt ska den personuppgiftsansvarige även rådgöra särskilt med tillsynsmyndigheten (IMY[2] i Sverige) i enlighet med artikel 36 i GDPR innan systemet tas i bruk och några personuppgiftsbehandlingar därmed utförs.

Enligt artikel 35.2 GDPR ska den personuppgiftsansvarige rådfråga dataskyddsombudet (om sådant utsetts) vid genomförande av en konsekvensbedömning avseende dataskydd. I Göteborgs Stad finns stadsgemensamma dataskyddsombud för stadens verksamheter som

[1] 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)./ (GDPR/Dataskyddsförordningen)

[2] Integritetsskyddsmyndigheten, tidigare benämnd Datainspektionen,

utses av kommunstyrelsen och är placerade vid Dataskyddsenheten. Organisatoriskt tillhör denna enhet nämnden för intraservice.

I samband med att GDPR infördes 2018 fattade revisorskollegiet beslut om att revisorernas förvaltning av oberoende- och granskningsskäl inte skulle anlita/låta utse dataskyddsombud via kommunstyrelsen/Dataskyddsenheten. Som en konsekvens av detta ställningstagande utsågs jag till dataskyddsombud för stadsrevisionen från och med 2018-05-25 och har innehaft detta uppdrag sedan dess. I rollen som dataskyddsombud förutsätts jag bland annat att understödja den personuppgiftsansvariges egen organisation för dataskydd genom råd och vägledning. Ett dataskyddsombud har dock inte något eget ansvar för den personuppgiftsansvariges följsamhet mot GDPR.

Arbetet med att ta fram föreliggande konsekvensbedömning har letts av stadsrevisionens dataskyddsansvariga tjänsteperson, tillika administrativa chef. Arbetet har bedrivits i en arbetsgrupp bestående av administrativ chef, kommunikationsansvarig samt registrator. Jag har i egenskap av dataskyddsombud också ingått som stödfunktion i arbetsgruppen.

2. Kommentarer avseende upprättad konsekvensbedömning

En konsekvensbedömning ska enligt GDPR[3] minst 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 förordningen efterlevs, med hänsyn till de registrerades och andra berörda personers rättigheter och berättigade intressen.

Vid iakttagande av dessa grundkrav för en konsekvensbedömning bör en personuppgiftsansvarig beakta relevanta rådgivande dokument från europeiska dataskyddsstyrelsen (EDPB), från europeiska datatillsynsmannen (European Data Protection Supervisor) samt från Sveriges nationella tillsynsmyndighet – integritetsmyndigheten (IMY).[4]

[3] Jfr GDPR artikel 35 p. 7

[4] Aktuella rådgivande dokument är: 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 (godkänd av EDPB 2018-05-25) 2 European Data Protection Supervisor, Accountability on the ground part II: Data Protection Impact Assessment & Prior Consultation, februari 2018. Webblänk till IMY:s informationssida är: Konsekvensbedömningar och förhandssamråd | IMY

2.1. Ansvar kopplat till användning av IT-system i den kommungemensamma miljön

Det är alltid den personuppgiftsansvarige som är ansvarig för att föreskrivna krav för personuppgiftsbehandling enligt GDPR följs och upprätthålls för en verksamhet. Detta kan innebära särskilda utmaningar i en kommun där drifts- och utvecklingsansvar för gemensamma IT-system ligger utanför den personuppgiftsansvariges kontroll. Detta är fallet i Göteborgs Stad där detta ansvar vilar på nämnden för intraservice medan personuppgiftsansvaret primärt vilar på den verksamhet som använder ett kommungemensamt system.

Det är då – ur dataskyddssynpunkt – mycket viktigt att den personuppgiftsansvarige så långt det är möjligt eftersträvar att tillförsäkra sig kontroll över och insikt i hur personuppgiftsbehandlingar görs i de system som tillhandahålls av nämnden för intraservice. Detta arbete behöver också dokumenteras så det framgår att det gjorts, för att den personuppgiftsansvariges ansvarsskyldighet att kunna uppvisa följsamhet mot GDPR:s regelverk ska mötas. En konsekvensbedömning ska också i sig själv redogöra för vilka risker som identifierats och hur de bedömts och hanterats i de system som utför behandlingarna.

Annorlunda uttryckt ska en registrerad med ledning av en konsekvensbedömning kunna ta del av all information som krävs för att själv förstå vilka behandlingar som sker och att den personuppgiftsansvarige vidtagit nödvändiga åtgärder för att begränsa de risker som finns. Stadsrevisionen har därför valt att – mot bakgrund av att det Digitala navet utgörs av en SharePoint baserad applikation som fungerar i Office 365-miljö - innefatta en omfattande teknisk redovisning för hur de underliggande systemen för tjänsten fungerar ur dataskyddssynpunkt. Denna redovisning bygger på underlag som framtagits av nämnden för intraservice och även använts vid denna nämnds egen konsekvensbedömning för det Digitala navet.

Jag bedömer det som nödvändigt att Stadsrevisionen hanterar den aktuella konsekvensbedömningen i enlighet med detta angreppsätt för att uppfylla sina skyldigheter i förhållande till gällande regelverk. Det har också funnits en samsyn runt detta ställningstagande i arbetsgruppen som tagit fram konsekvensbedömningen.

2.2. Kvarstående osäkerhet runt fördelning av personuppgiftsansvar i Staden

Nämnden för intraservice arbetar med att anpassa sin verksamhet till ”Göteborgs Stads /nya/ riktlinje för styrning, samordning och finansiering av digital utveckling och förvaltning”. Ett led i detta arbete innefattar en förändring av det tidigare gällande synsättet i Staden att nämnden med stöd av sitt uppdrag - som beslutats av fullmäktige - fungerar som personuppgiftsbiträde i förhållande till övriga verksamheter i Staden.

Det har då i sin tur inneburit att detta beslut medgett ett undantag från det normala kravet enligt GDPR som innebär att en personuppgiftsansvarig som anlitar ett personuppgiftsbiträde, också ska sluta ett särskilt avtal med instruktioner för hur personuppgifter ska hanteras av biträdet.

Den nya inriktningen via riktlinjen enligt ovan är att personuppgiftsansvaret efter utredning ska fördelas på ett tydligare sätt i staden vid användning av olika system och applikationer och att separata personuppgiftsbiträdesavtal ska slutas mellan verksamheter

i Staden och nämnden för intraservice. Då arbetet inte är färdigställt innebär det en otillfredsställande situation för stadsrevisionen. Utvecklingen i denna del behöver därför följas noga så att korrekt utformade personuppgiftsbiträdesavtal kan slutas med nämnden för intraservice snart det kan ske.[5] Utkast till personuppgiftsbiträdesavtal som hittills presenterats av nämnden har inte varit utformade i enlighet med GDPR:s krav då de saknat instruktioner respektive tydliga hänvisningar till vilka underbiträden nämnden använder sig av.

2.3. Överföring av personuppgifter till tredje land

Som stadsrevisionen redogjort för i sin konsekvensbedömning krävs det vid överföring av personuppgifter till land utanför EU/EES (tredje land) att det mottagande landet har en skyddsnivå för personuppgifterna och de registrerades intressen som motsvarar vad som gäller för där GDPR är direkt tillämplig. Om det finns ett så kallat ”adekvansbeslut” det vill säga ett beslut av EU-kommissionen att mottagarlandet har en sådan adekvat skyddsnivå så kan den personuppgiftsansvarige stödja sig på det och göra överföringen utan risk att bryta mot GDPR. Under framtagningen av det Digitala navet har det saknats ett giltigt adekvansbeslut för Förenta staterna (USA), vilket i sig varit problematiskt då viss överföring sker vid användning av underliggande system i Office 365-miljön.[6]

Från och med den 10 juli 2023 gäller dock ett nytt adekvansbeslut. Beslutet gäller inte generellt för alla typer av överföringar av personuppgifter till USA utan att är begränsat till att gälla överföringar som sker till organisationer etablerade där och som omfattas av det nya ramverket ”EU-US data privacy framework.” Ramverket är en mekanism för självcertifiering där de organisationer som vill delta får genomgå en särskild process för att godkännas. Certifieringen gäller för ett år i taget och kan därefter förnyas via ytterligare en process. Microsoft, som ansvarar för Office 365-miljön är certifierade och omfattas därmed av adekvansbeslutet.

Det är dock inte självklart att adekvansbeslutet kommer att gälla om EU-domstolen prövar det. Det finns tydliga signaler att det kommer att utmanas i framtiden, vilken innebär en risk för att det i likhet med tidigare liknande (föregående beslut) avseende USA kan komma att upphävas av domstolen.

Det finns också en risk att Microsoft inte alltid kommer att vara certifierade under EU-US data privacy framework.

Sammantaget är det därför av stor vikt att stadsrevisionen, liksom övriga personuppgiftsansvariga som arbetar i/med Office 365-baserade system/applikationer – noga bevakar utvecklingen runt tillåtligheten att överföra personuppgifter till USA.

2.4. Begränsning av information i det Digitala navet

Användning av det Digitala navet kan innebära många fördelar ur kommunikationssynpunkt då det ger stadens verksamheter och medarbetare enkel tillgång till stora informationsmängder. Detta innebär samtidigt vissa risker ur integritets- och

[5] Jfr 3.4.5 i aktuell konsekvensbedömning.
[6] Jfr 4.2 i aktuell konsekvensbedömning.

dataskyddssynpunkt. Stadsrevisionen har valt att – med hänvisning till det senare – begränsa informationsmängden i det Digitala navet i fråga om den egna verksamheten.

Funktioner som kommentarsfält och liknande i systemet kommer inte heller att aktiveras av samma skäl. Min uppfattning är att detta är en riktig och rimlig begränsning av informationsmängden där integritetsskyddsrisker tillåtits väga tyngre än behovet av kommunikation via det Digitala navet.

Det noteras vidare att den som tilldelas redaktörsbehörighet i det Digitala navet ytterst kommer att vara ansvarig för att publicering av material inte innebär några betydande integritetsrisker. Det är därför viktigt att den som har sådan behörighet dels har rätt kompetens och dels även har tillgång till relevant stöd för sina arbetsuppgifter i form av skriftliga rutiner eller motsvarande. Min uppfattning är att stadsrevisionen har en medvetenhet om betydelsen av detta.

3. Rekommendationer kopplat till användning av Digitala navet

Jag lämnar mot bakgrund av vad som diskuterats ovan följande rekommendationer till stadsrevisionen inför driftsättning och användning av det Digitala navet:

- Stadsrevisionen bör ställa förnyade krav på nämnden för intraservice att ta fram korrekta underlag för att upprätta personuppgiftsbiträdesavtal avseende Digitala navet och underliggande system (Office 365) så snart det går att genomföra.
- Stadsrevisionen bör *generellt* ha en beredskap för att göra en förnyad konsekvens-analys för det Digitala navet kan om förutsättningarna som behandlats i aktuell analys för användning av systemet förändras i framtiden.
    - Stadsrevisionen behöver i detta särskilt bevaka rättsutvecklingen runt adekvansbeslutet avseende EU-US data privacy framework och dess framtida giltighet.
    - Detsamma gäller i fråga giltigheten för underliggande systemleverantörs certifiering inom ramen för EU-US data privacy framework (Microsoft).
- Stadsrevisionen bör slutligen säkerställa att den som tilldelas redaktörsbehörighet i det Digitala navet alltid har rätt kompetens och tillgång till relevant stöd för arbete som innebär publicering av personuppgifter i systemet.

Göteborg den 30 oktober 2023

Anders Landkvist
Dataskyddsombud för stadsrevisionen i Göteborg

13 Underbilagor från intraservices konsekvensbedömning

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

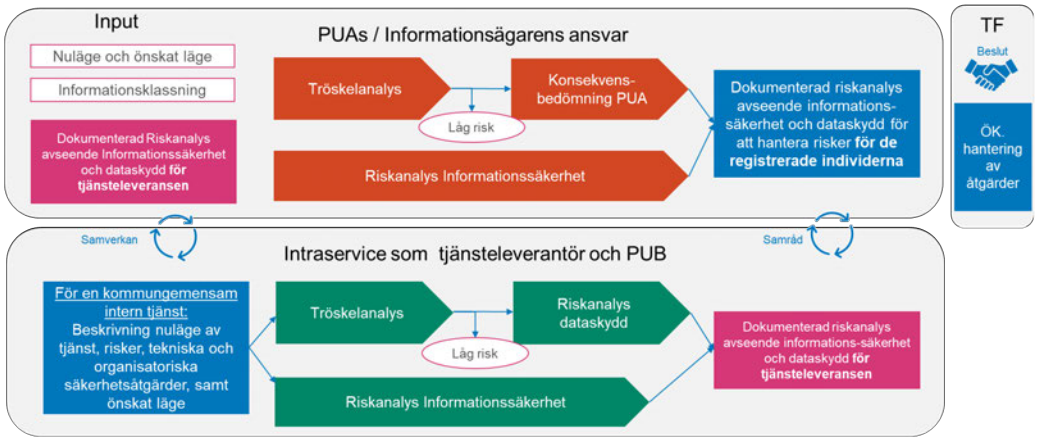
Innehållsförteckning

1 Bakgrund och Metod

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

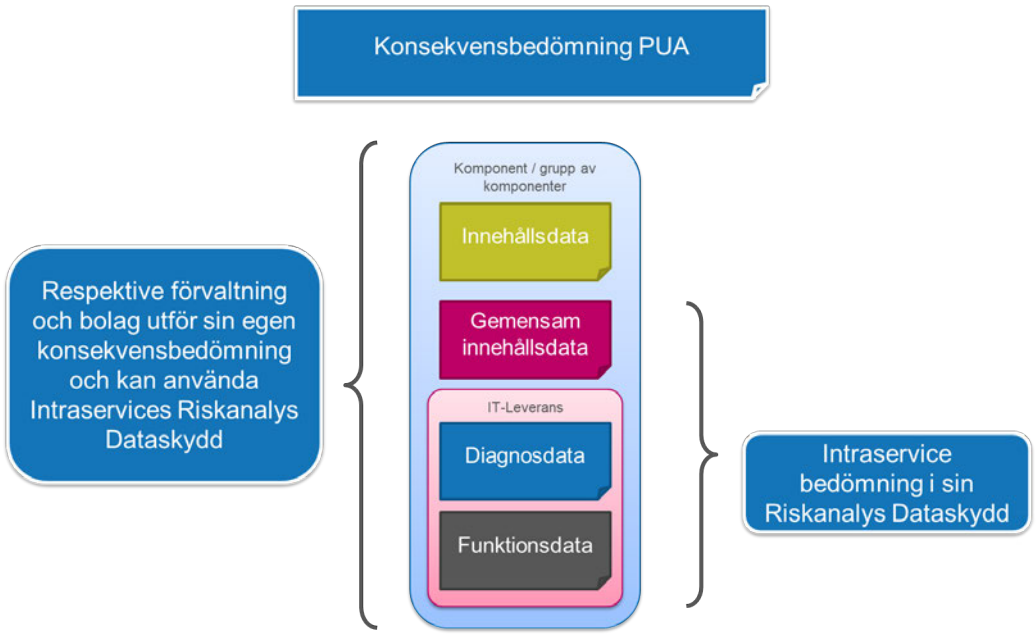
Riskanalys dataskydd för Microsoft Office 365 utförs av tjänsteleverantören Intraservice för kommungemensamma interna tjänster i egenskap av personuppgiftsbiträde. Riskanalys dataskydd är en beskrivning av tjänsten som levereras samt riskanalys med fokus på personuppgifter utifrån tjänsteleverans och 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).

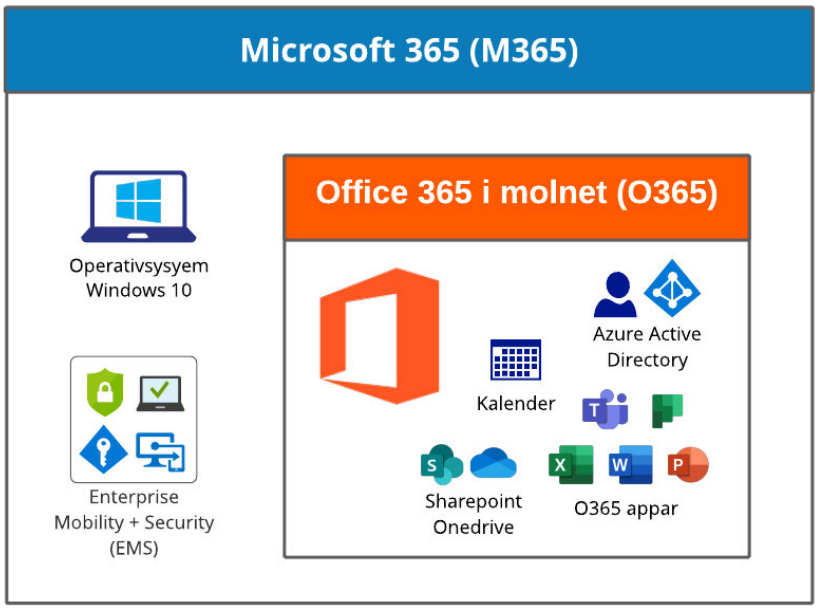
> *The observed telemetry data do not contain any content from documents, emails or conversations, and no directly identifying data such as user names or e-mail addresses. The events related to the use of the processor Connected Experiences such as the spelling checker and Translator also do not contain 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

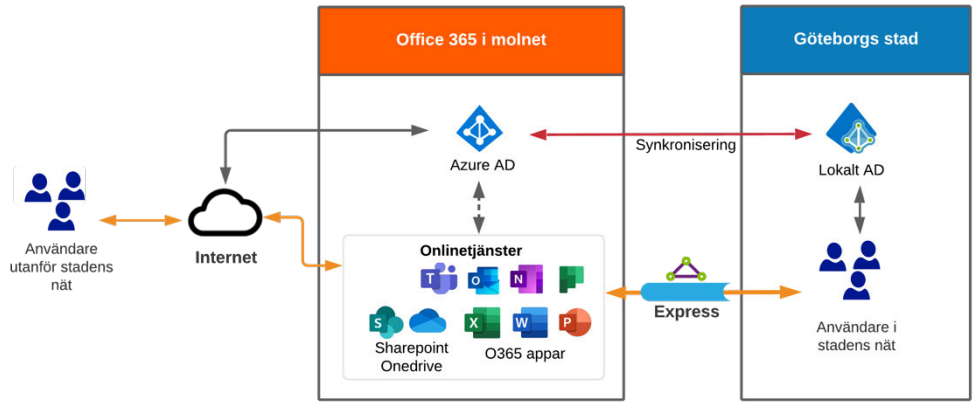
För mobila enheter och operativsystem finns även Word, Excel och Powerpoint samt andra appar där kommunens användare kan skapa, kommunicera och samarbeta. Microsoft Office mobile apps motsvarar Microsoft 365 Apps for enterprise men körs på Android eller iOS mobila enheter.

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)



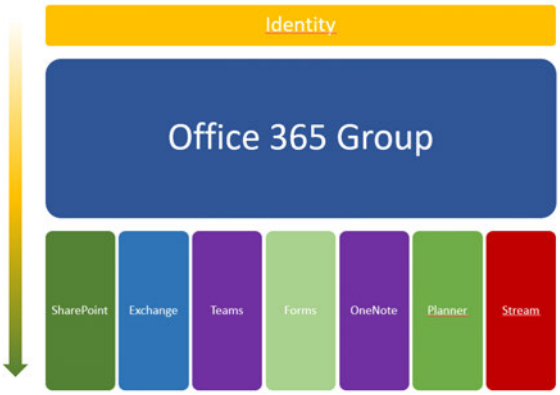
Figur 3- Microsoft molntjänster för att visualisera att O365 är en Saas tjänst hos Microsoft

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.

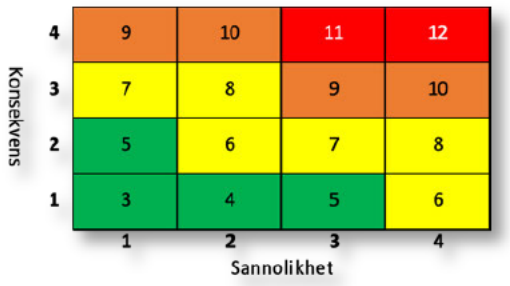
Själva riskvärderingen har dokumenterats i excelformat och återfinns i bilagan *O365 Riskanalys Dataskydd v3.0* och omfattar riskerna R1–R30. Riskerna 16 och 17 har är ej bedömds och ersätts i aktuell riskhantering av riskerna 18–30, som mer precist visar förekomst av risker för tredjelandsöverföring.

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.	

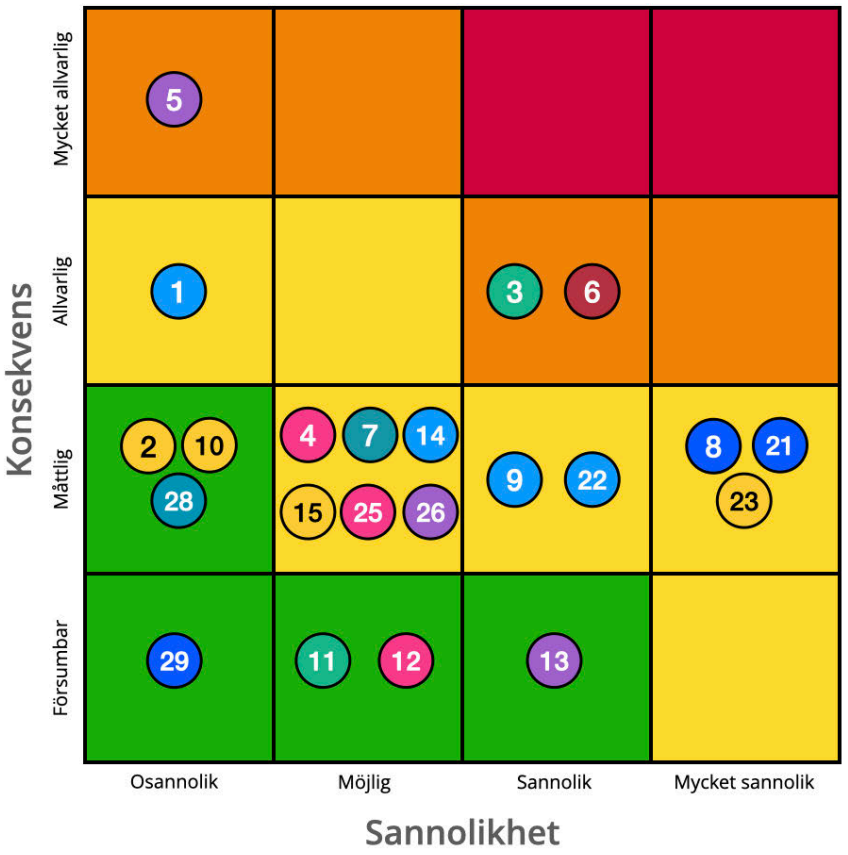
#	Beskrivning	Påverkar	Kommentar och åtgärder för riskhantering	Riskvärde
R31	**Övervakning av anställda (Teams analytics och Viva Insights)** Risk för… Möjlighet för kommunen få tillgång till medarbetares arbetsmönster genom Microsofts tjänster Teams Analytics och Viva Insights På grund av… Diagnosdata 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.

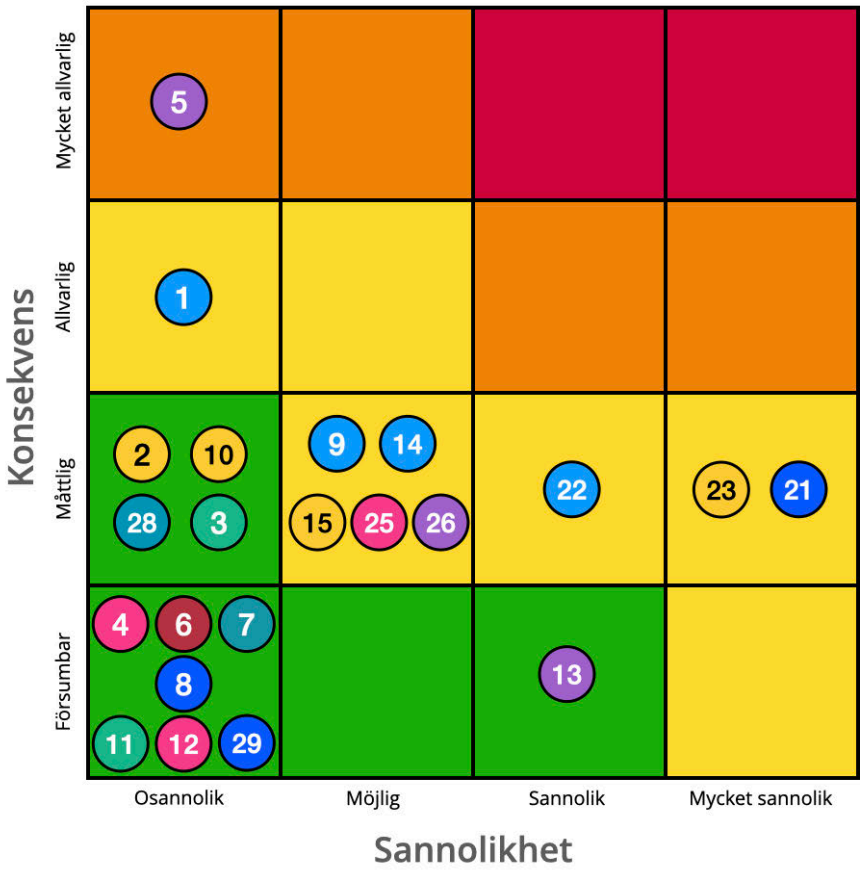
1. Värderade risker före åtgärder
2. Värderade risker efter åtgärder
3. Riskvärdering före och efter åtgärder (jämförelse)
4. Öppna risker

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

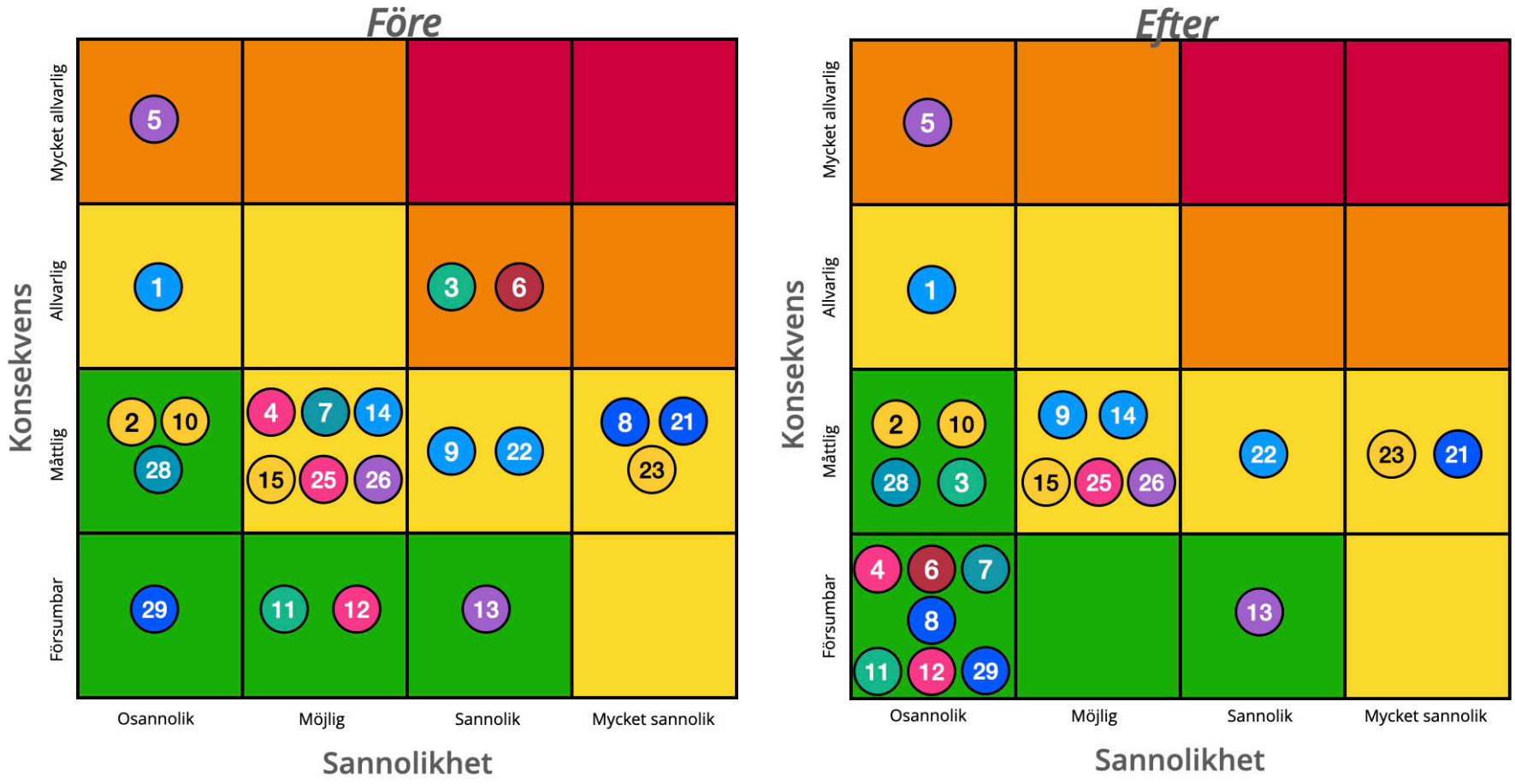
25 Samtal i Teams inkluderar vilka konton/ användare som samtalar och när.

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

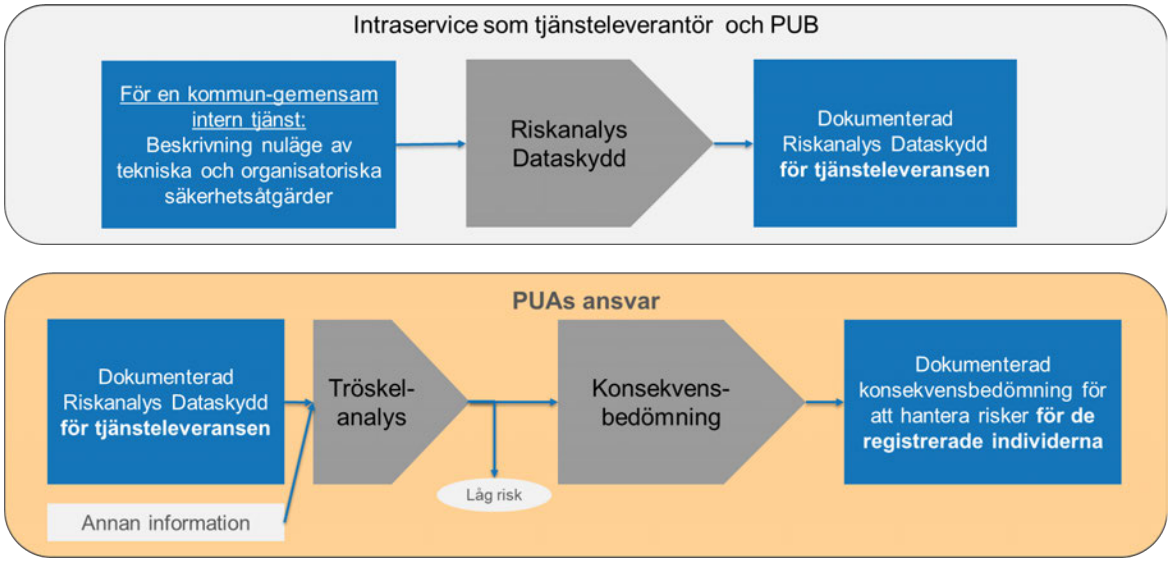
Innehållsförteckning

1 Bakgrund och metod

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.



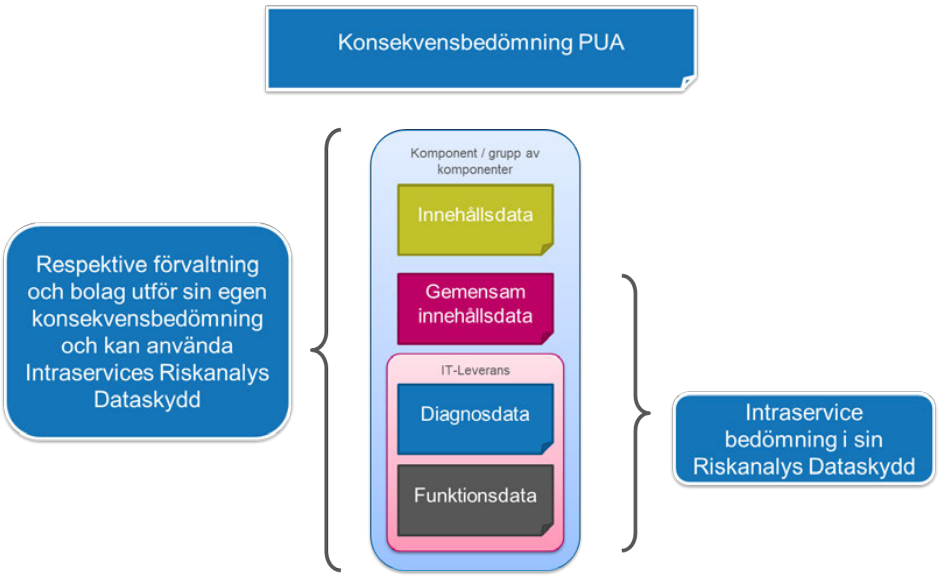
1.2 Metod

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.

Loggar på sig på sin dator	Användaren loggar på sig med sitt M365-konto på sin dator.
Går till Digitala navet	Användaren är redan inloggad på SharePoint som en del av M365
Startsidan visas	Användarinformation för Digitala navet så som roll och organisation hämtas från SQL-databas med hjälp av användarid
Användaren ändras sina användar-inställningar	Nytt val av organisation(-er) och/eller roll(-er) sparas som id:n till SQL-databasen
Startsidan visas igen	Informationen på startsidan uppdateras baserat på valen gjorda i steget innan
Besöker en sida i ämnesstrukturen	Informationen på sidan visas baserat på vilken organisation(-er) som valts.

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 personuppgiftskategorie***r 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

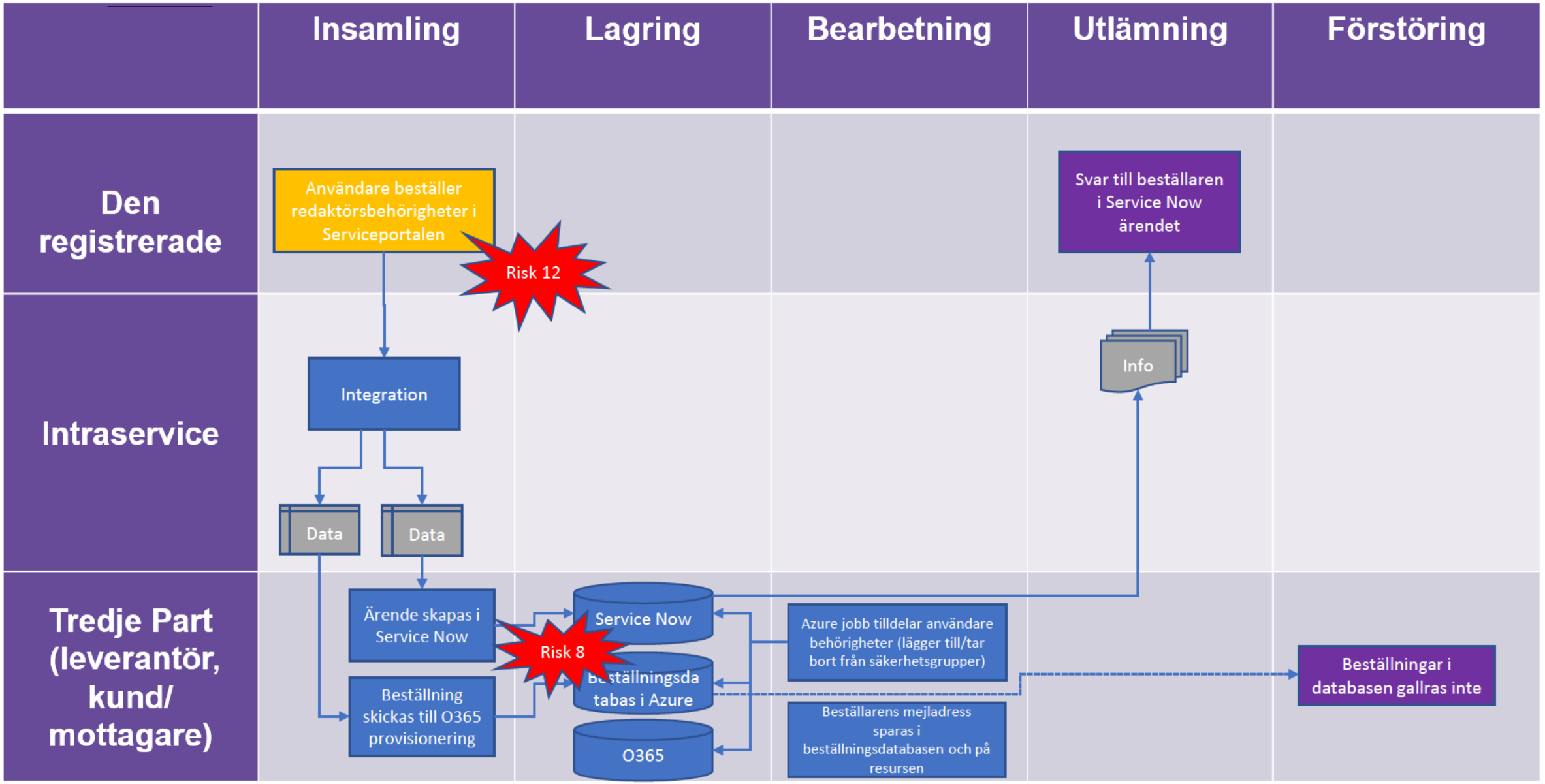
- Uppgifterna är inlagda i ett system och överförs via systemet, eller läggs in i ett system 

- 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. 

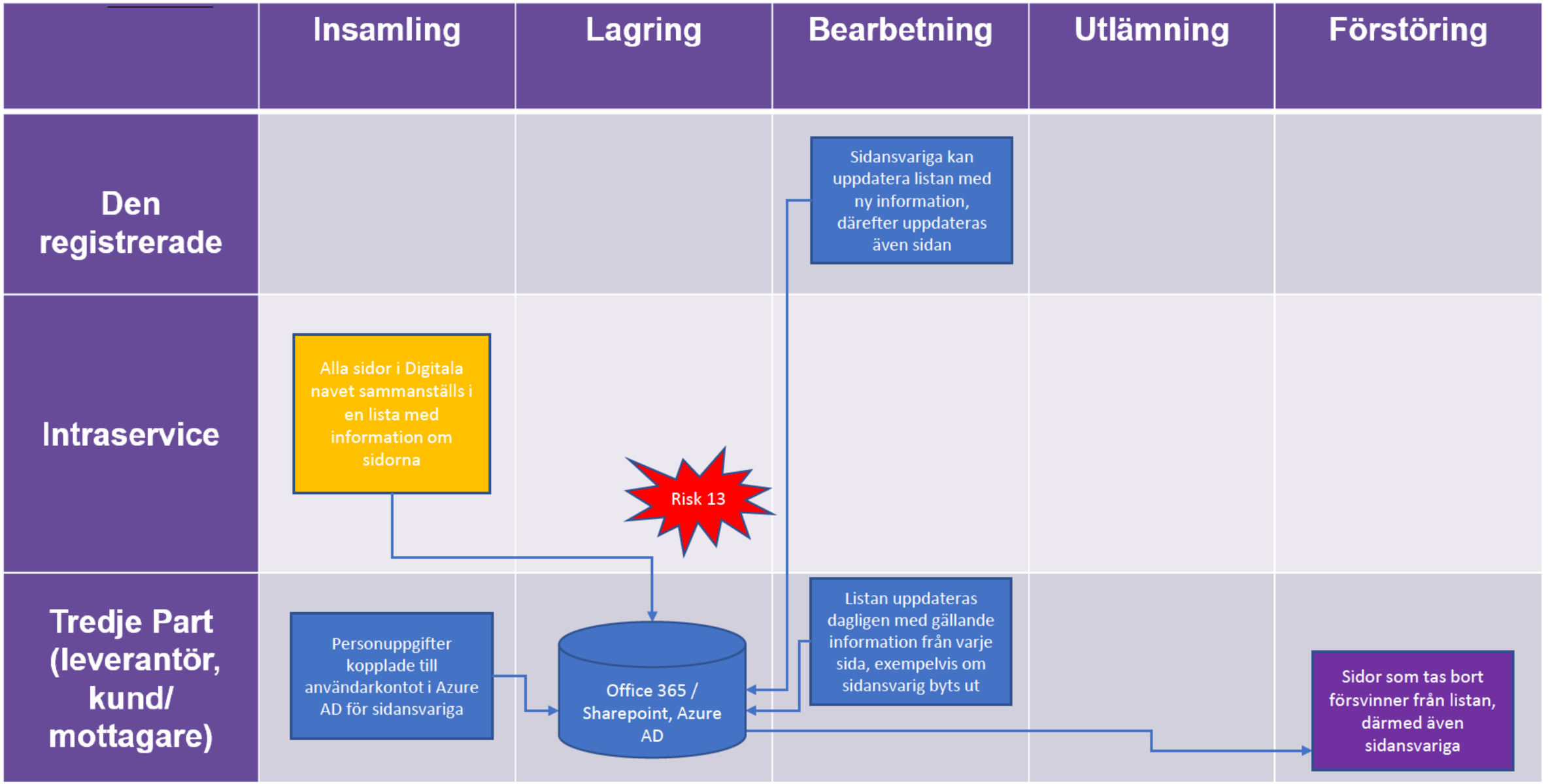
M365/Navet

2- Beställningar av redaktörsbehörigheter i Digitala navet via Serviceportalen



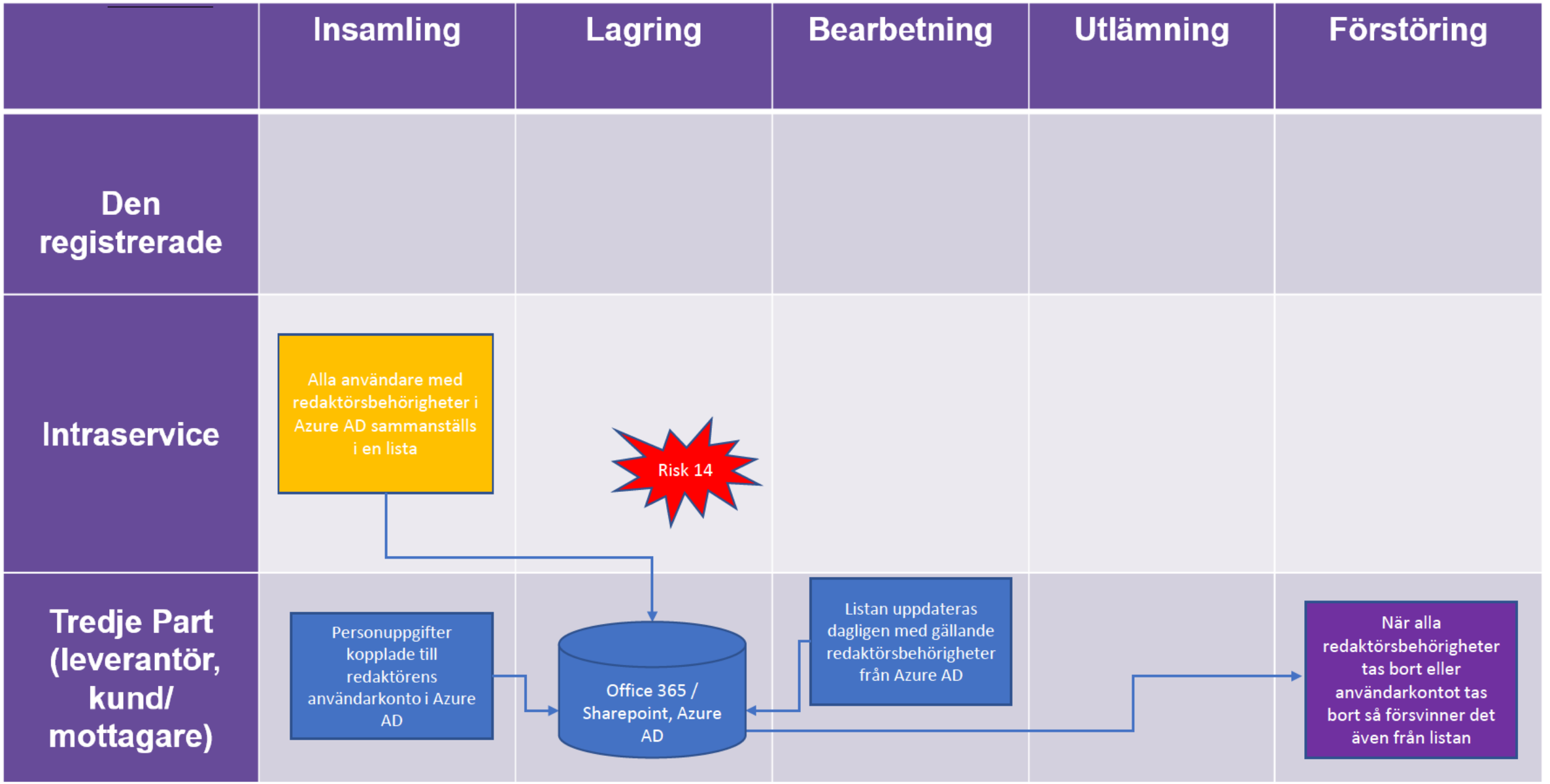
M365/Navet

3- Lista över alla sidor i Digitala navet



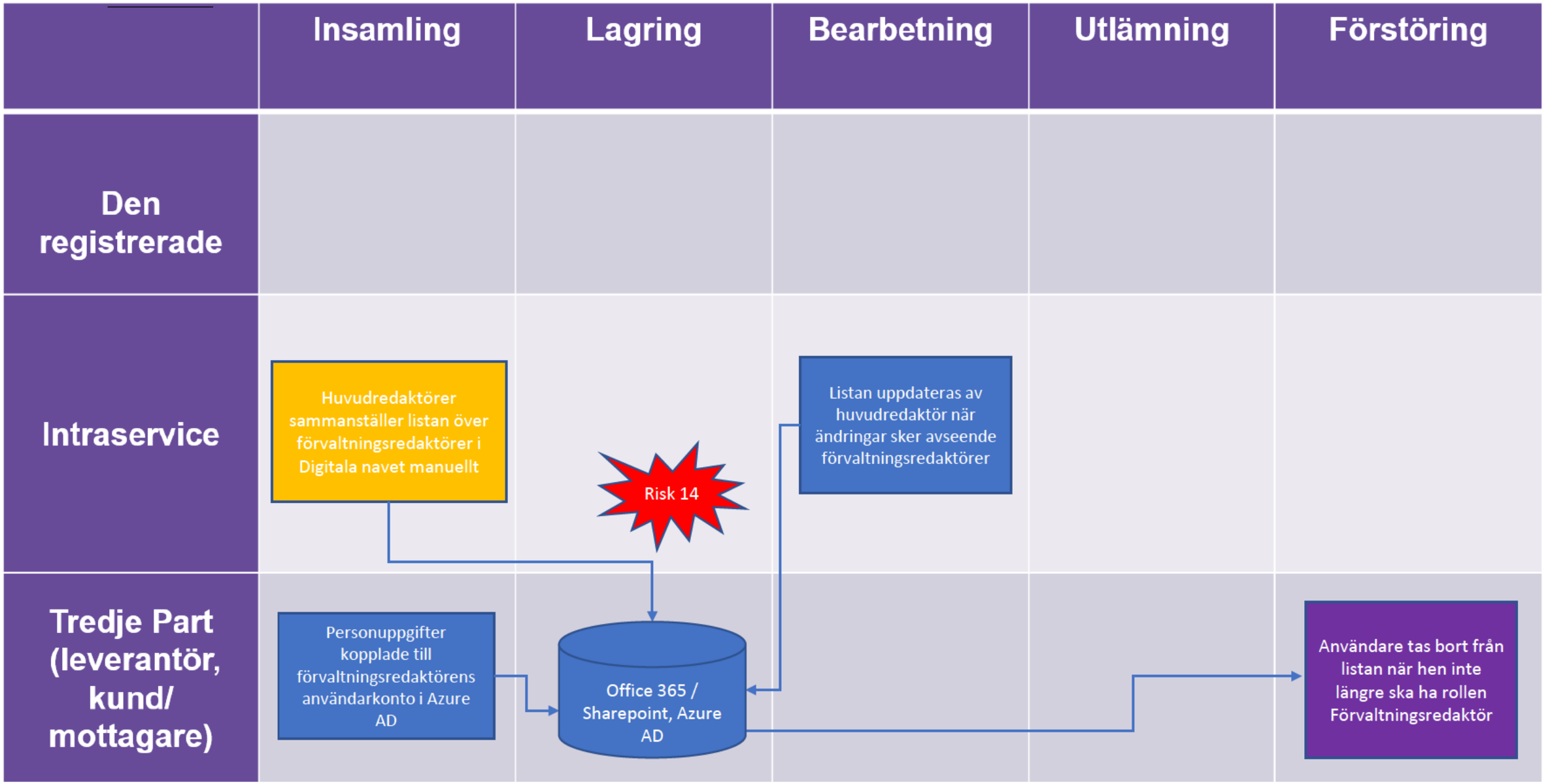
M365/Navet

4 - Lista över redaktörsbehörigheter



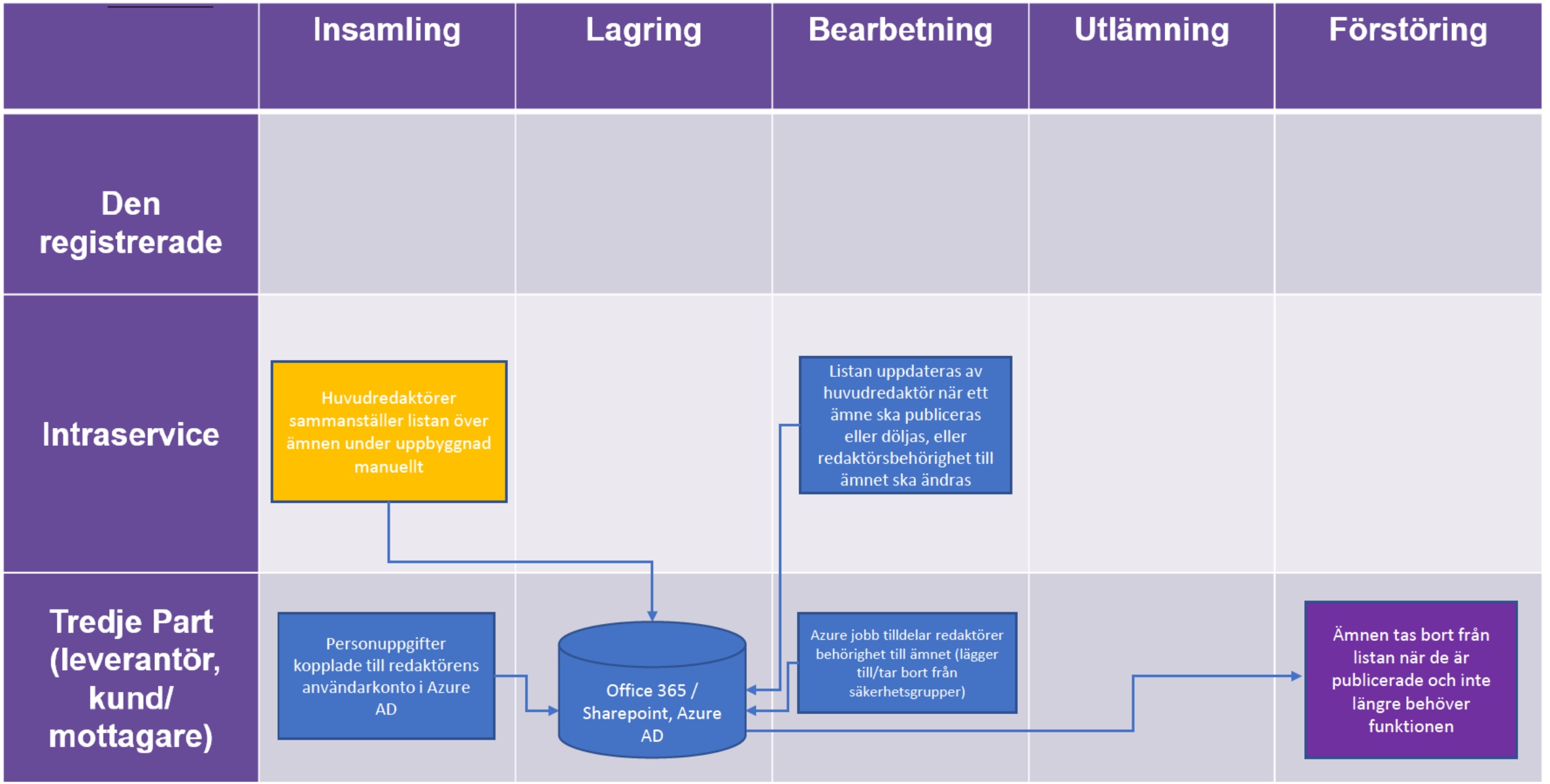
M365/Navet

5- Lista över förvaltningsredaktörer

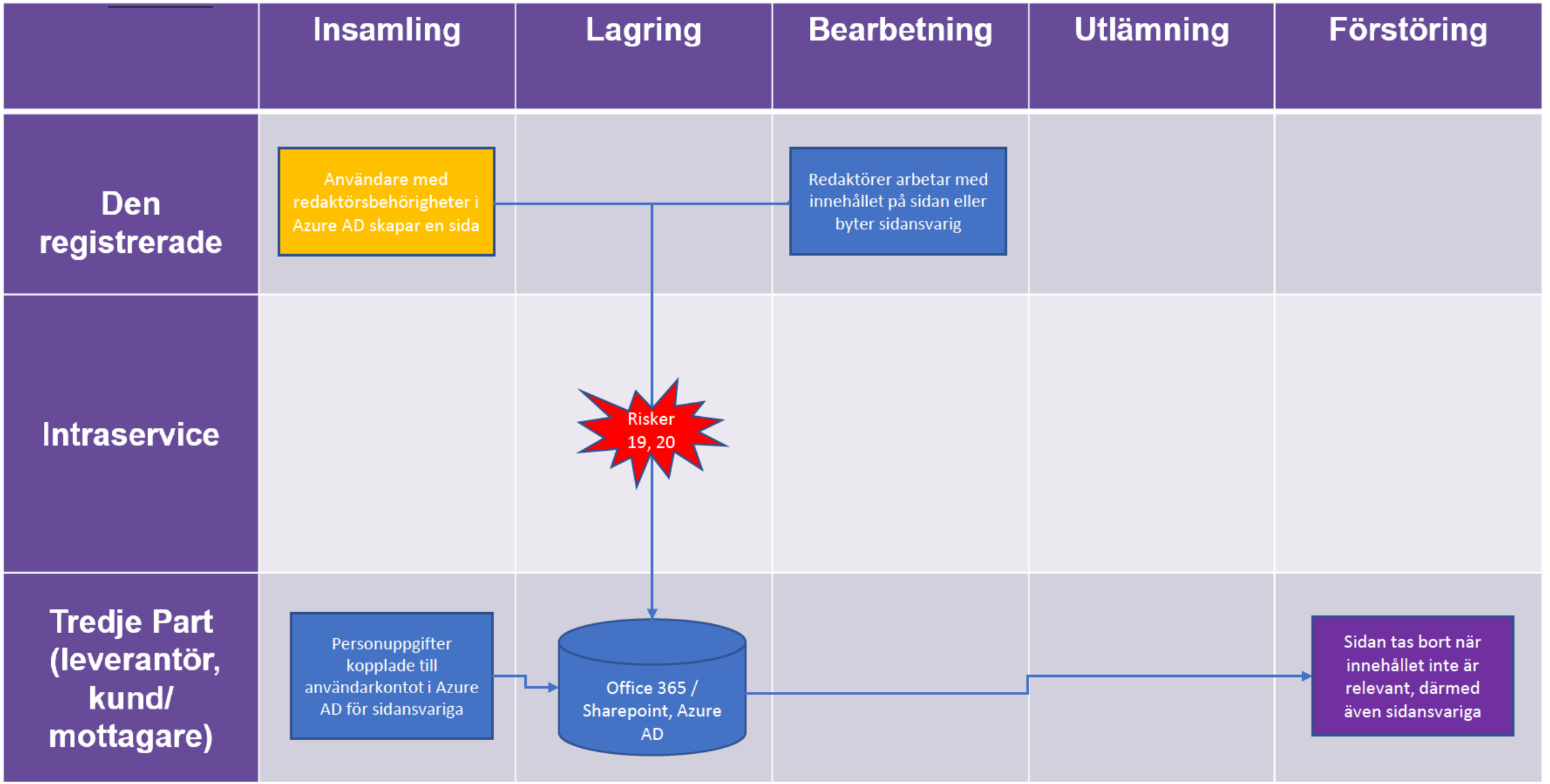


M365/Navet

6 - Lista för ämnen under uppbyggnad

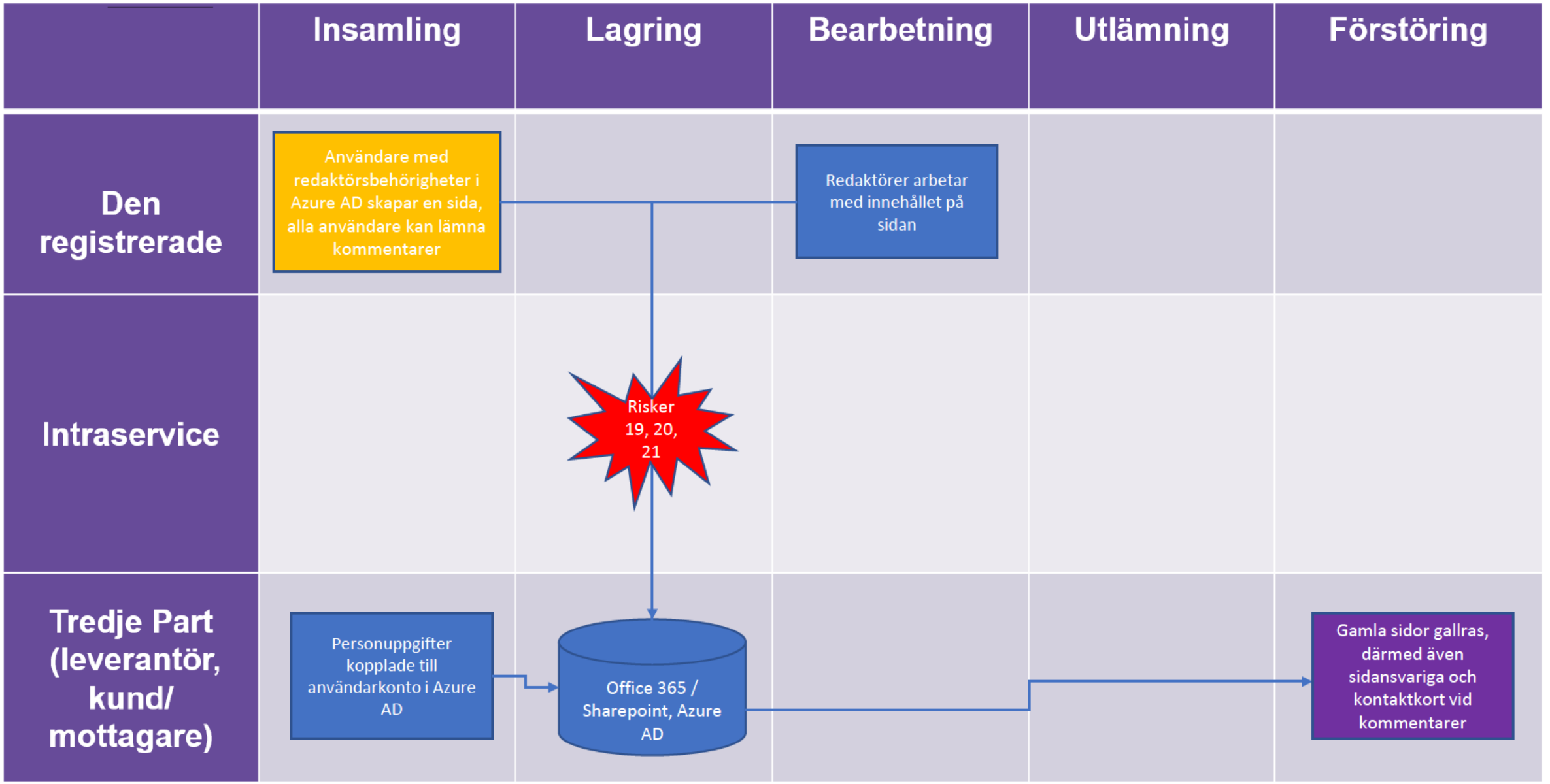


7 - Artikelsidor och specifika tillägg



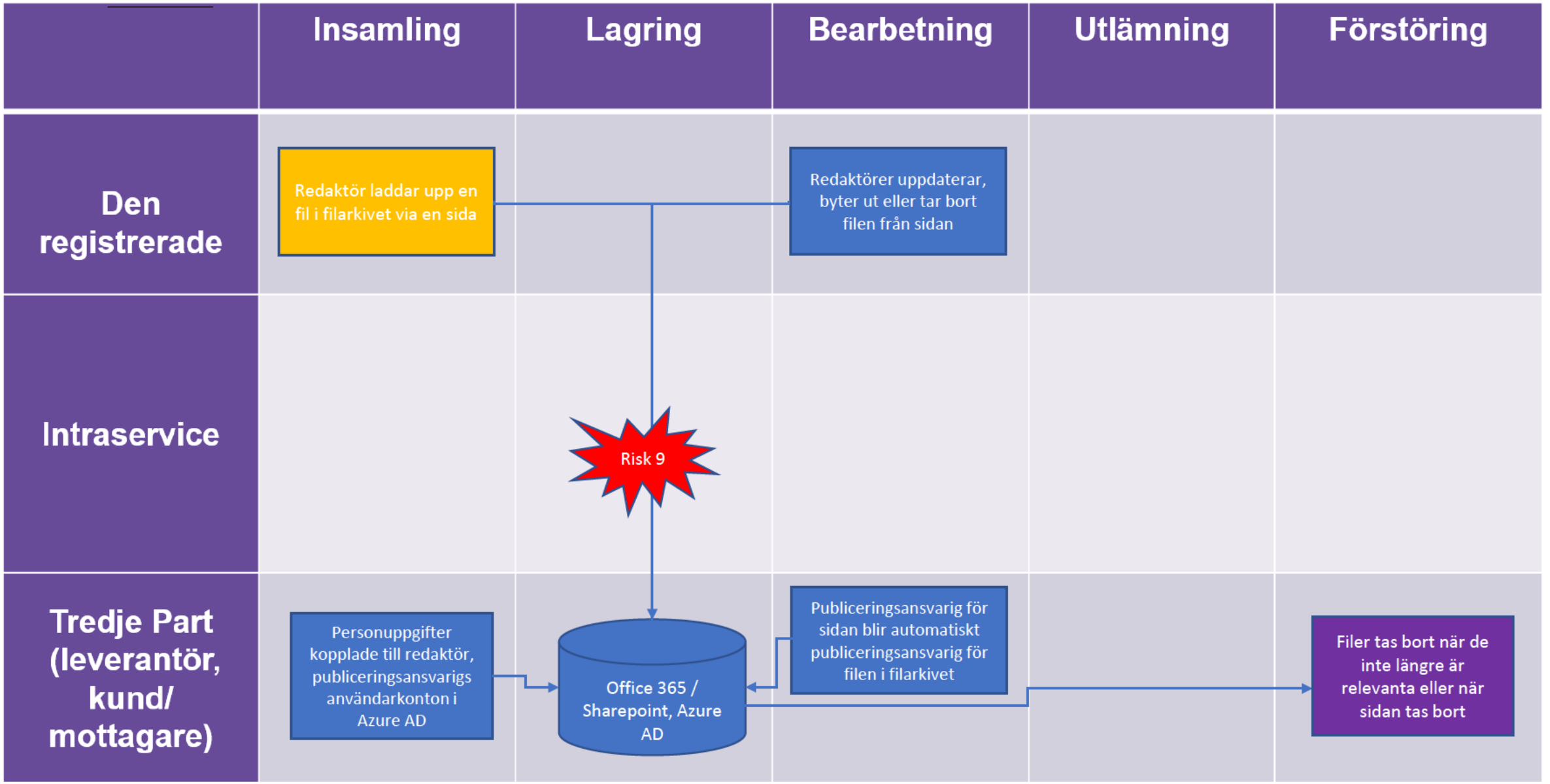
M365/Navet

8 - Inlägg i kommunikativa kanaler

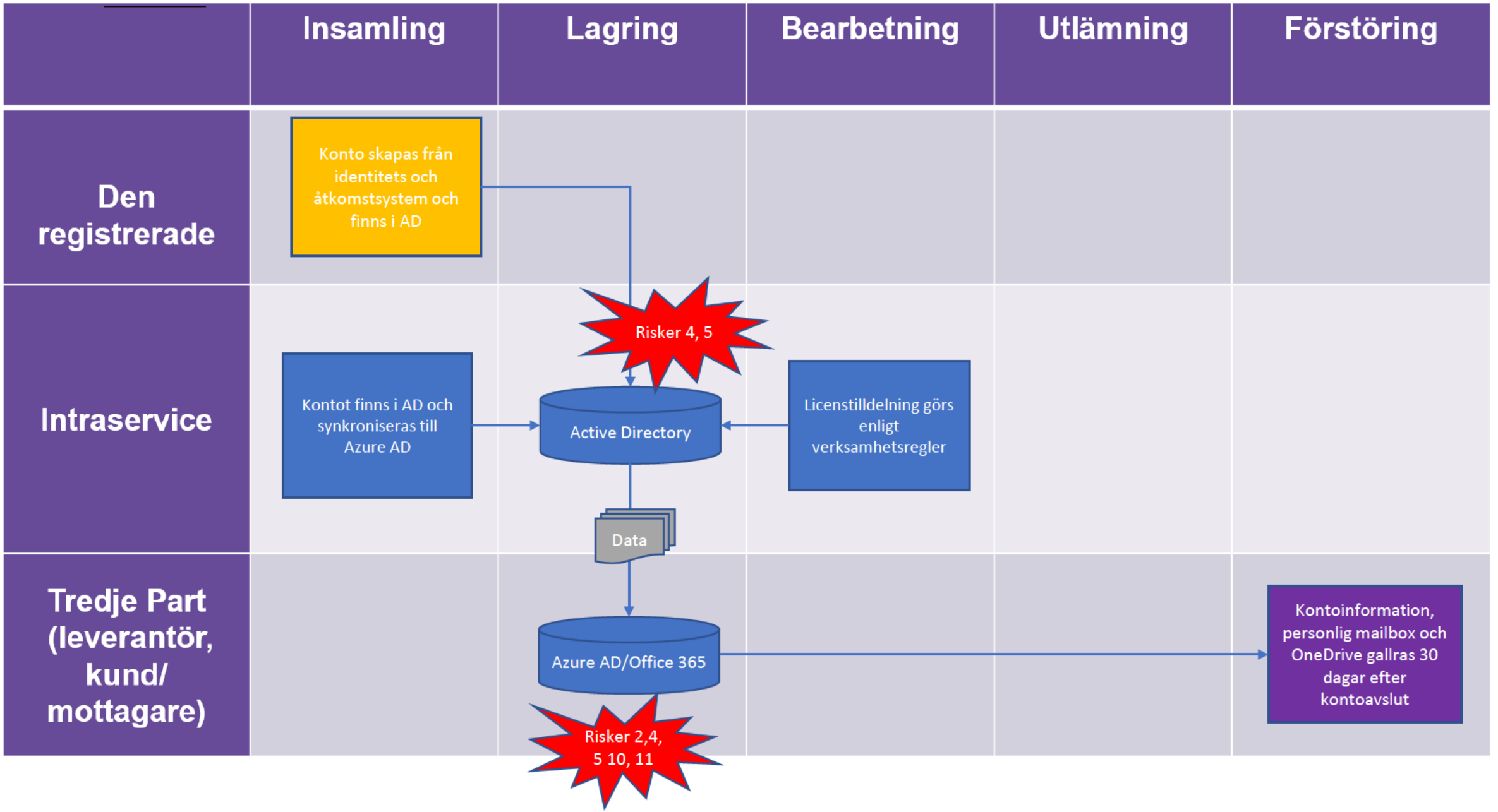


M365/Navet

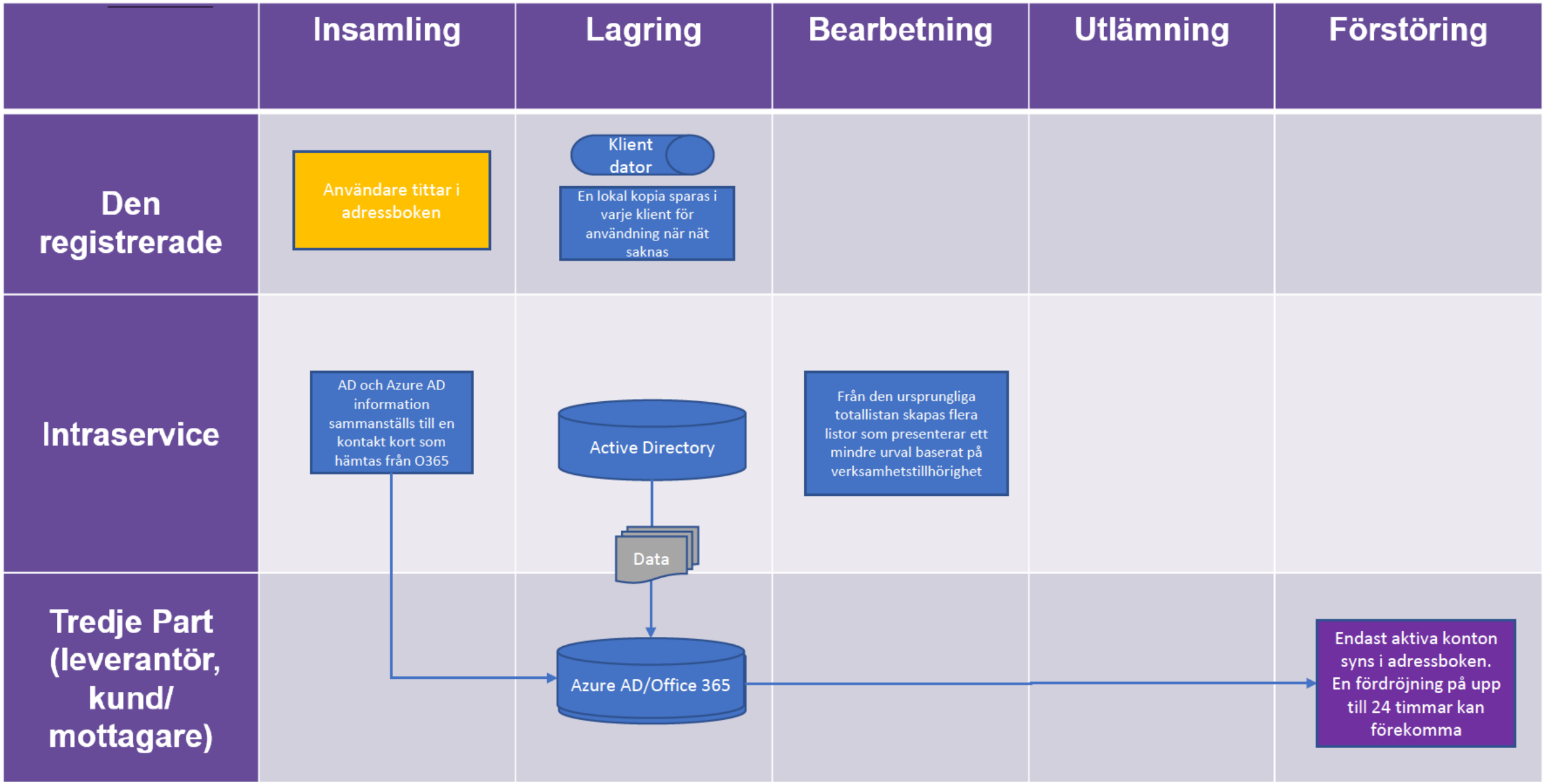
9 - Filer i Digitala navets filarkiv



10 - Kontoskapande



11- Adressboken i Outlook



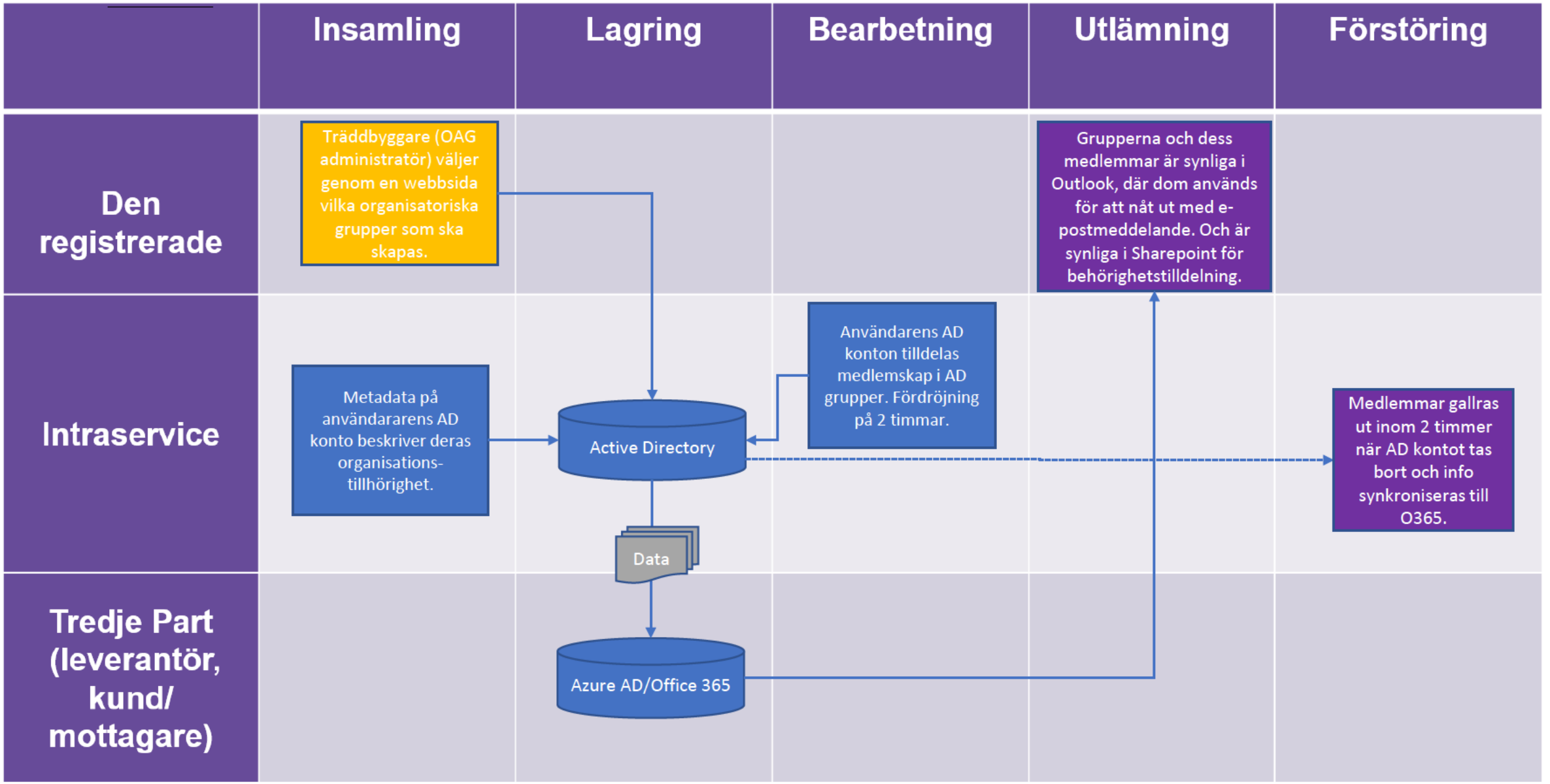
M365/Navet

Kontakt korten

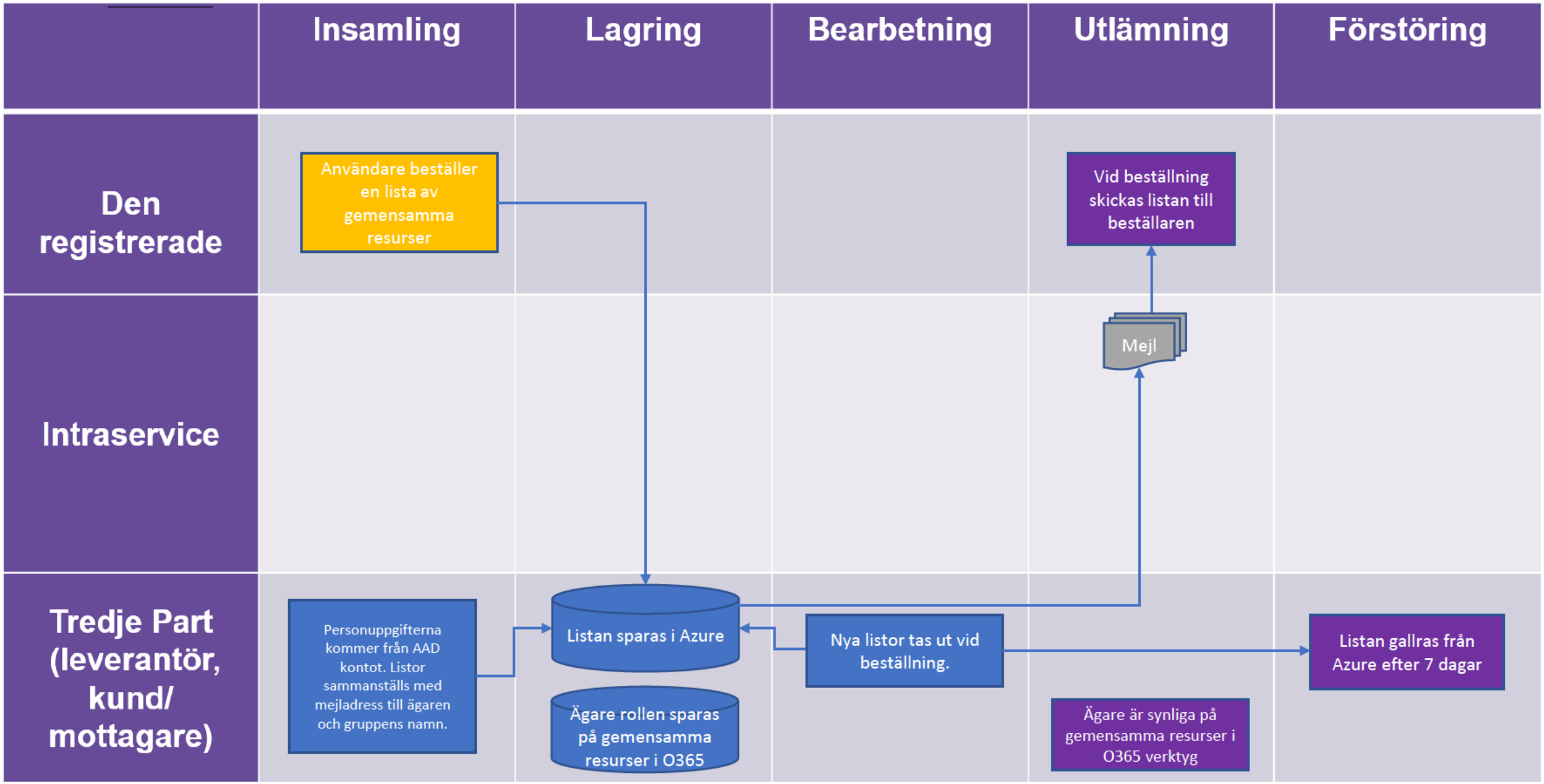
	Insamling	Lagring	Bearbetning	Utlämning	Förstöring
Den registrerade	Användare söker information om en kollega.				
Intraservice	Azure AD information sammanställs till en kontakt kort som hämtas från O365				
Tredje Part (leverantör, kund/ mottagare)		Azure AD/Office 365			Endast aktiva konton har ett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

M365/Navet

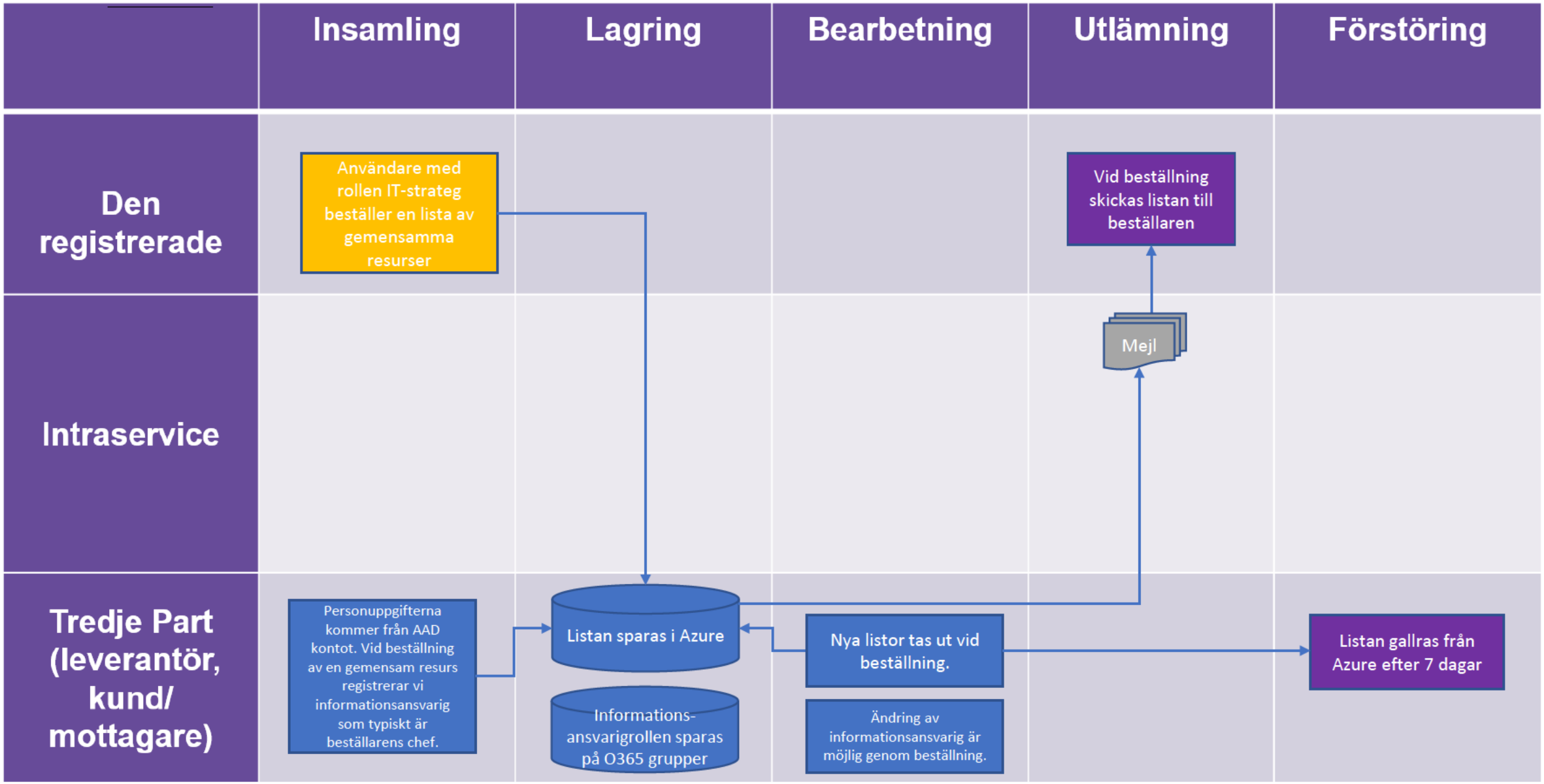
13 - Skapade av organisatoriska AD grupper (OAG)



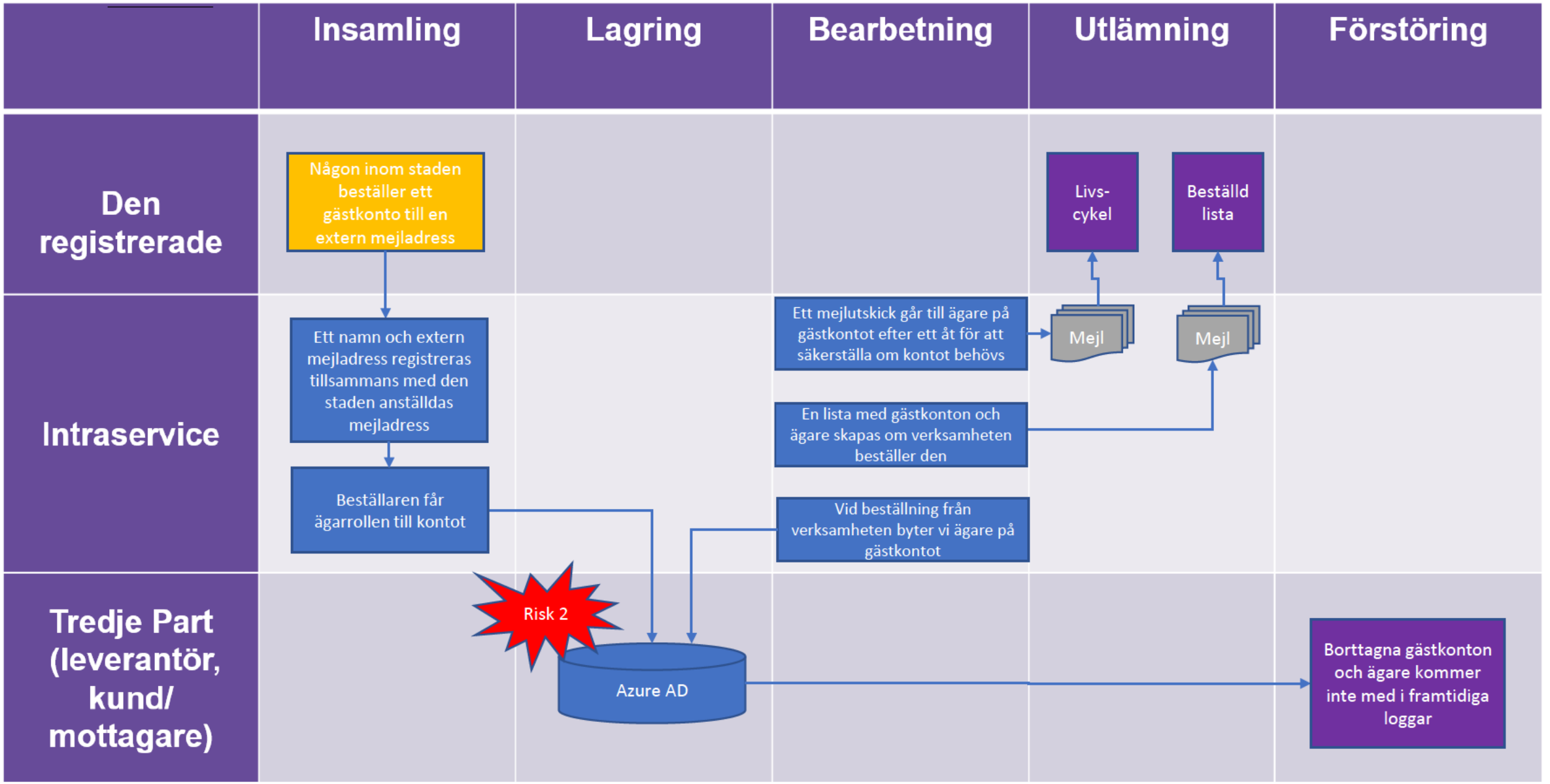
14 - Ägare rollen



15- Informationsansvarig rollen

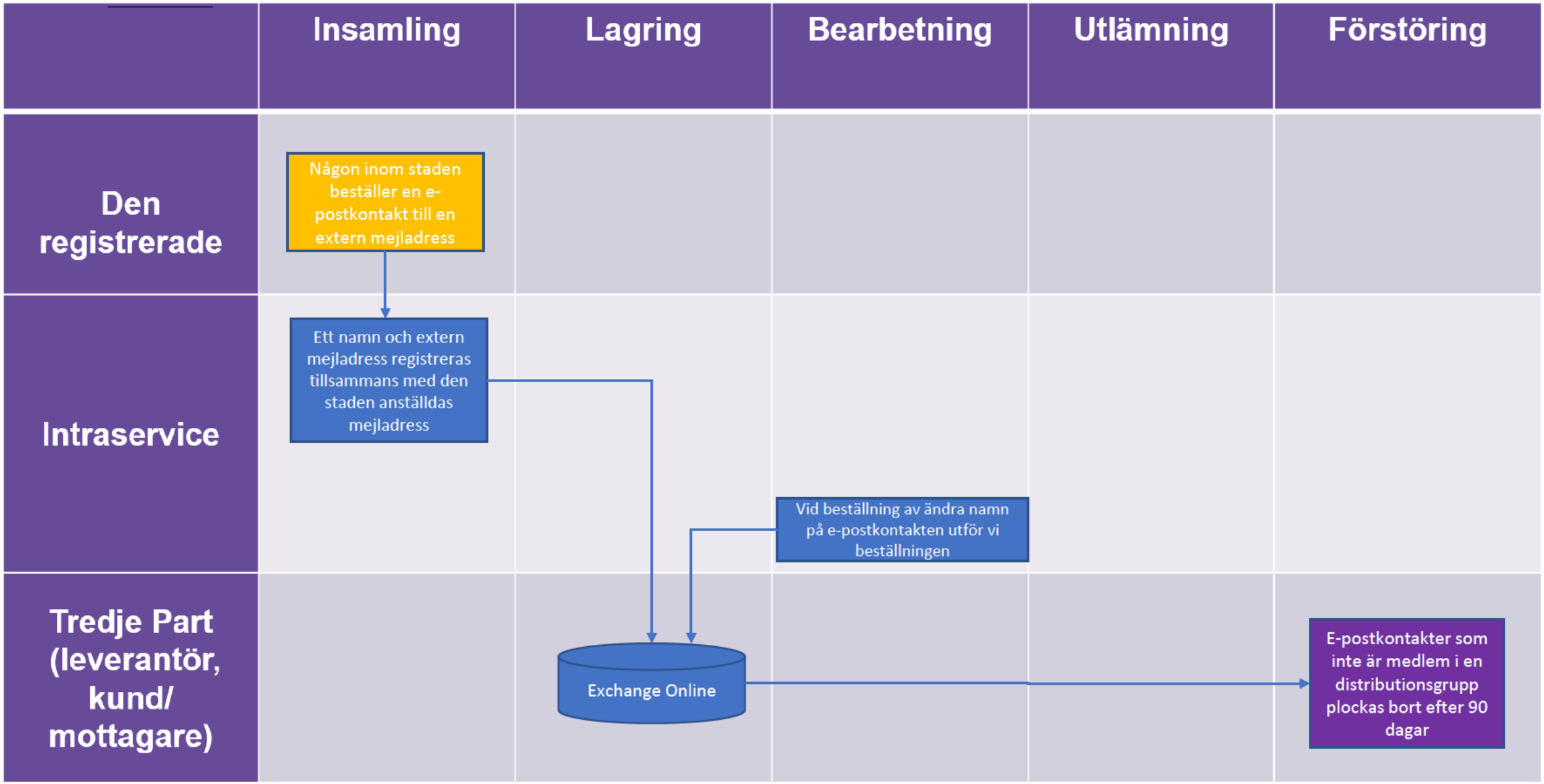


16 - Gästkonton

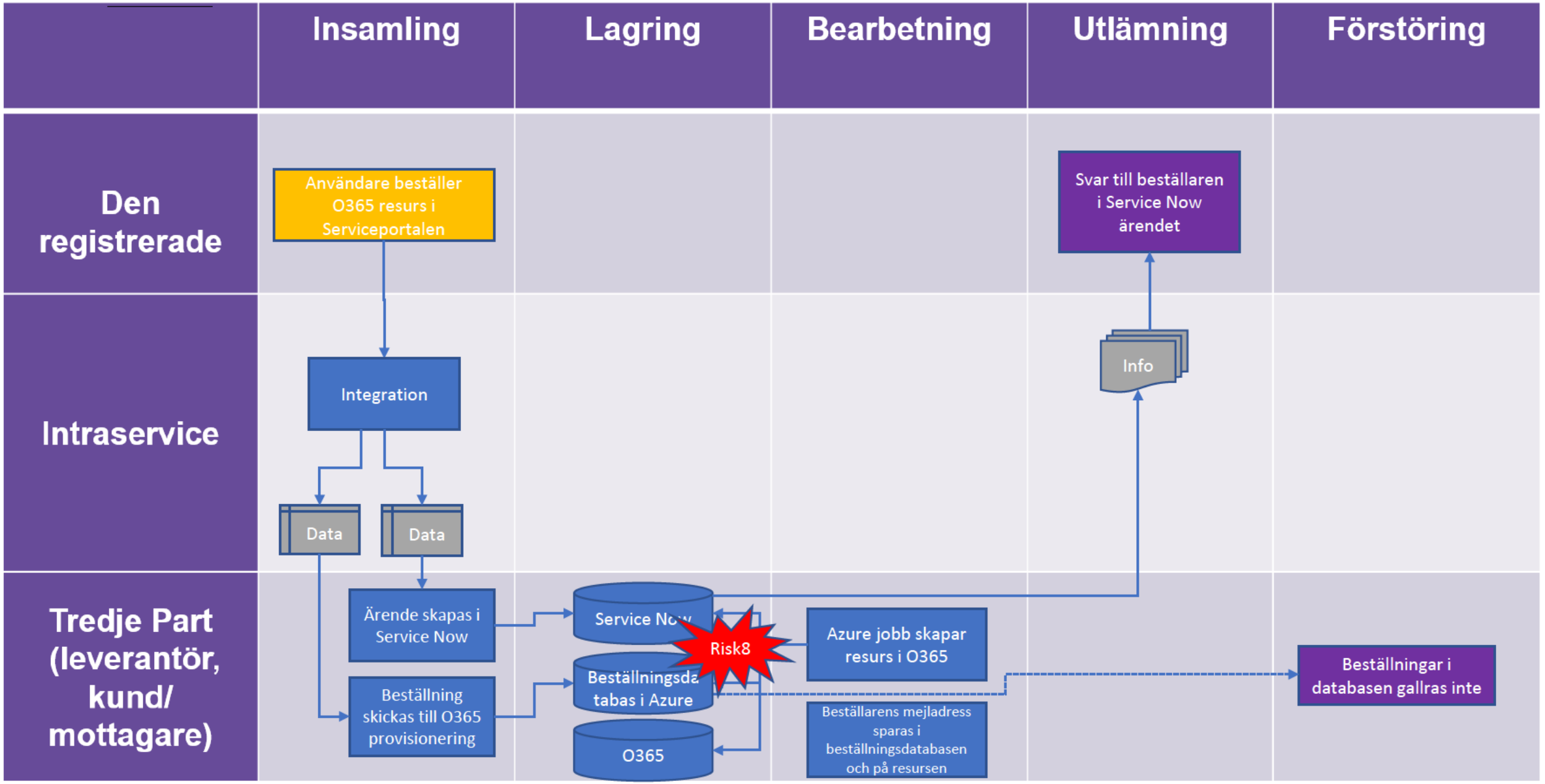


M365/Navet

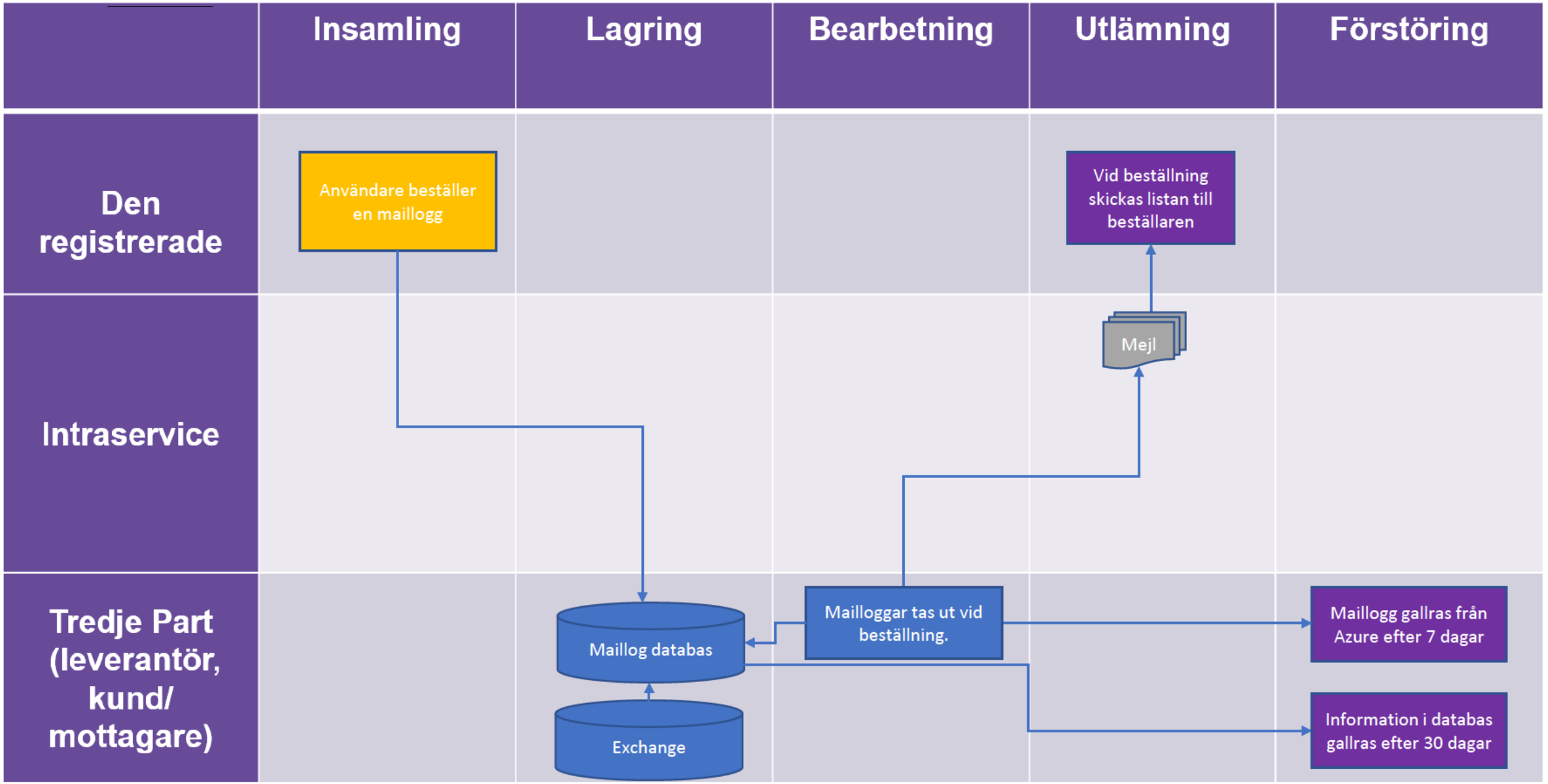
E-postkontakter



18 - Beställningar av Office 365 resurser i Serviceportalen

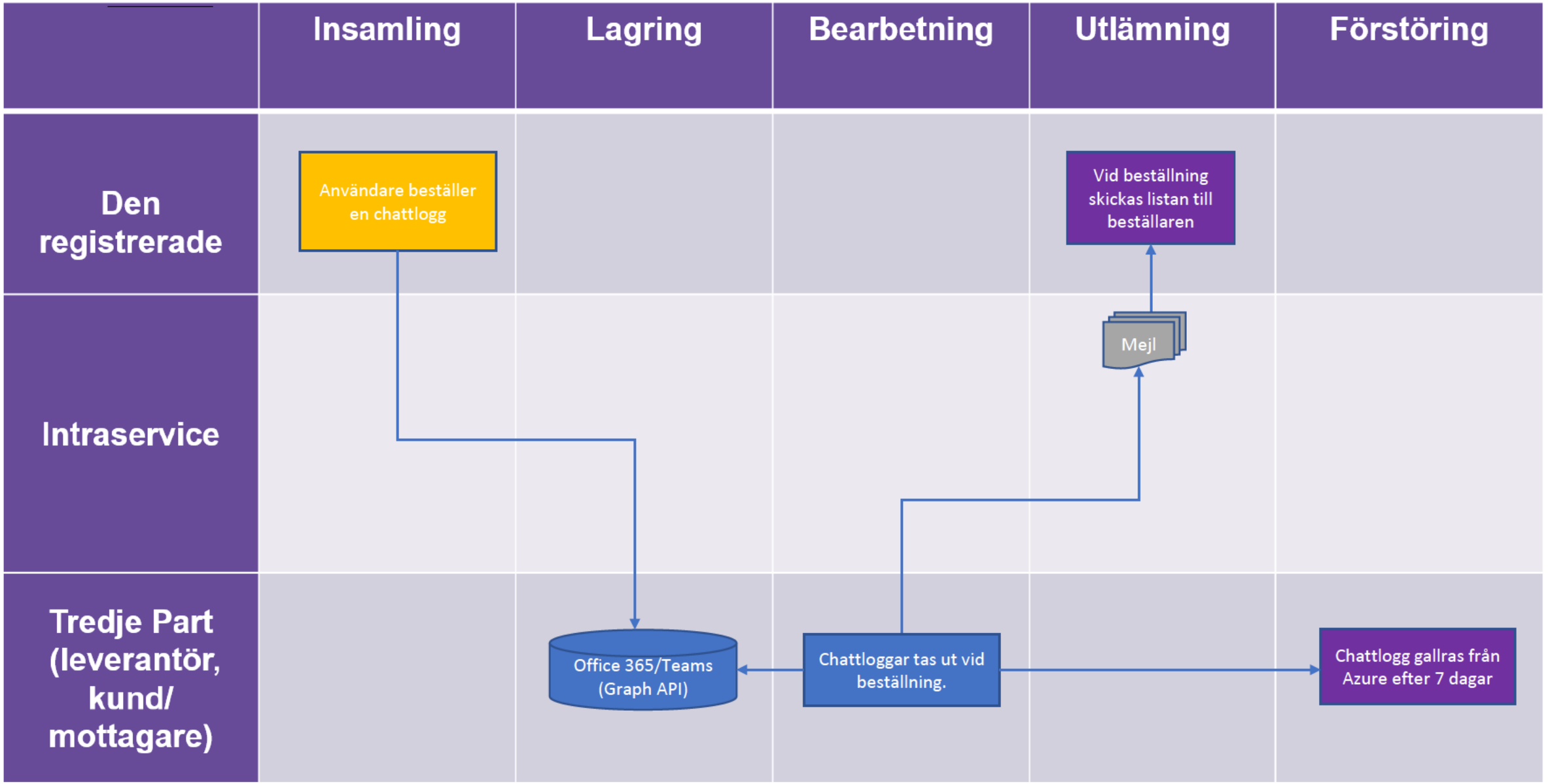


19 - Mailbox loggning

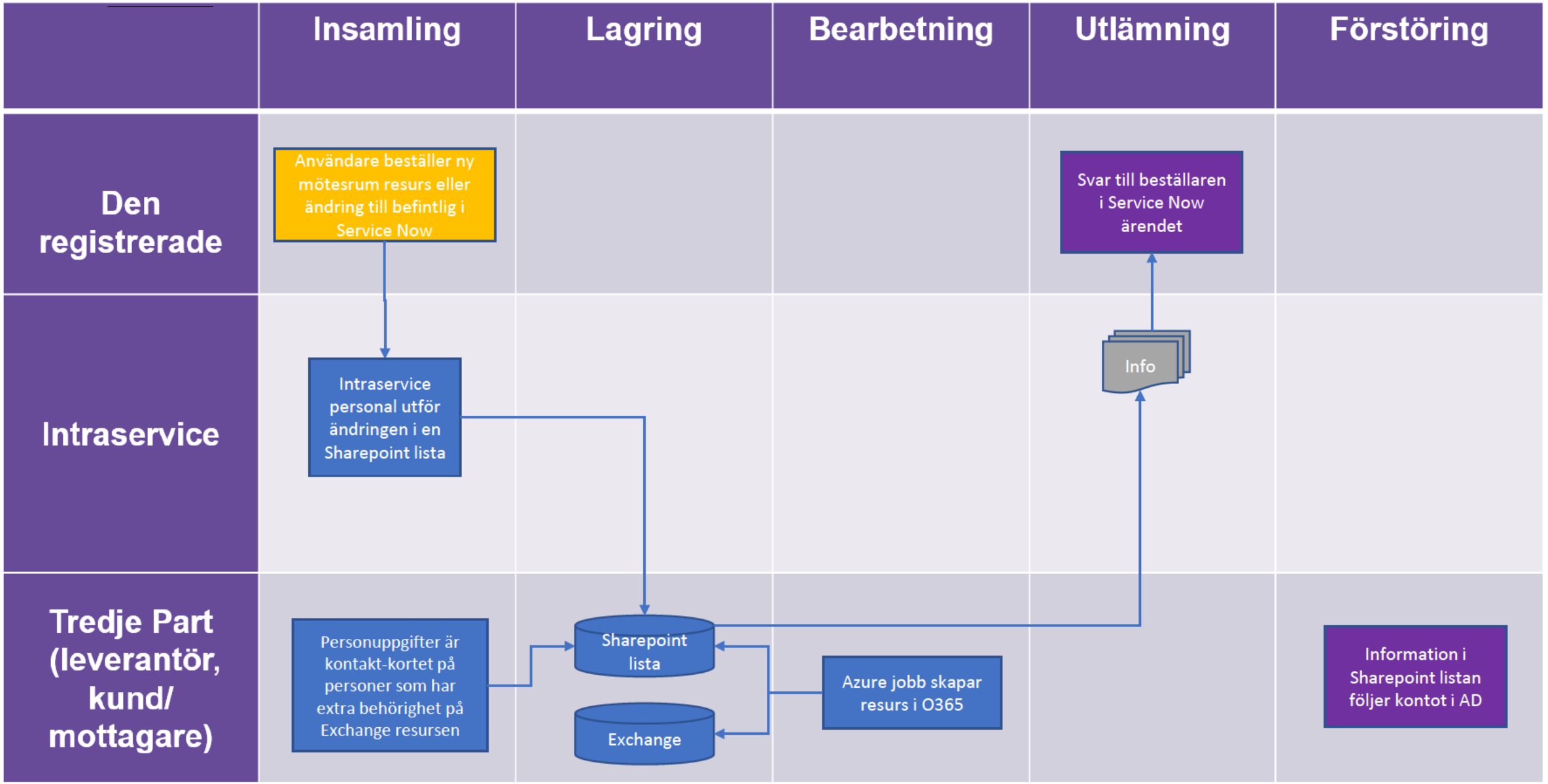


M365/Navet

Chatt loggning

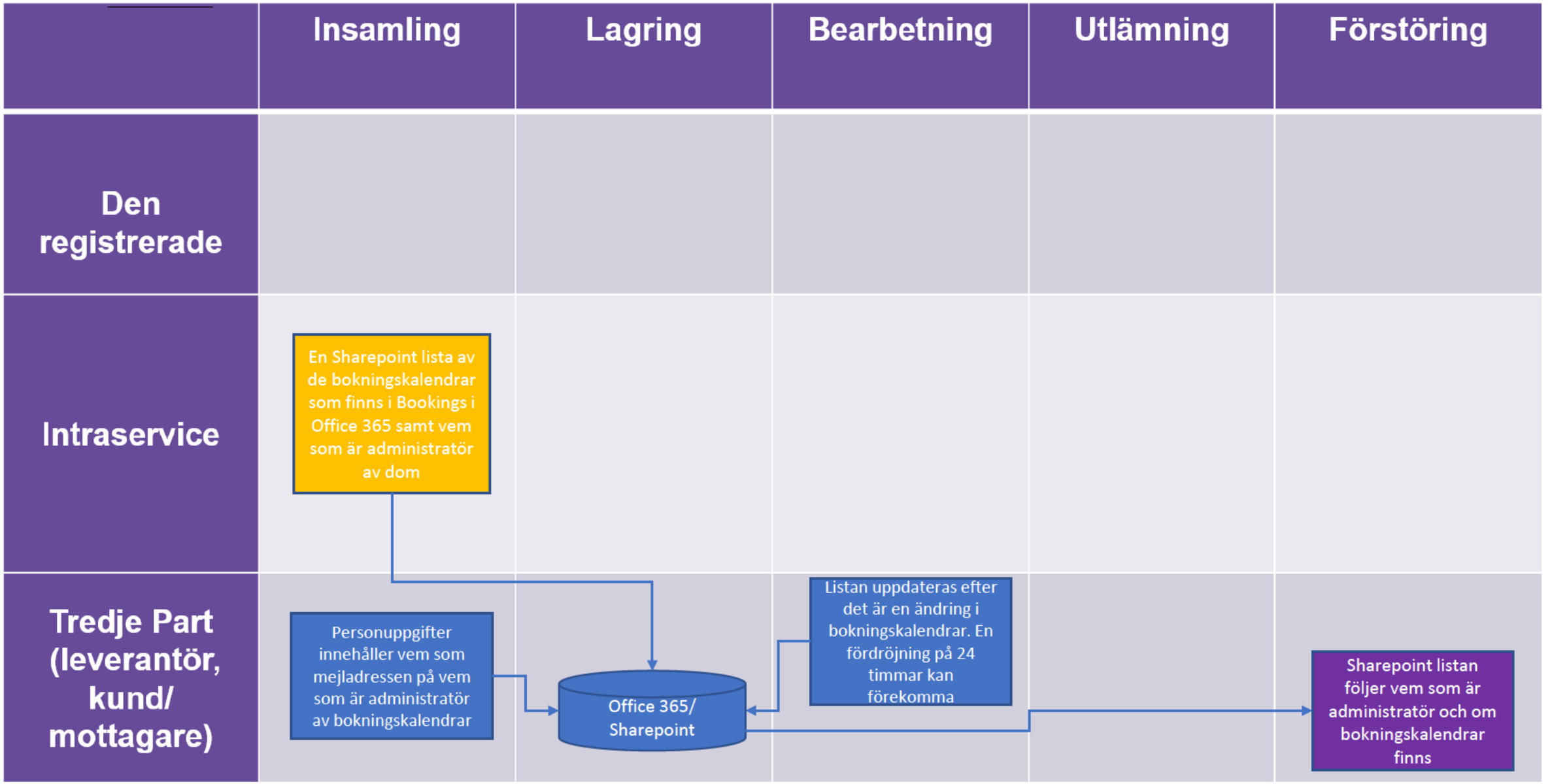


21 - Exchange resursadministration



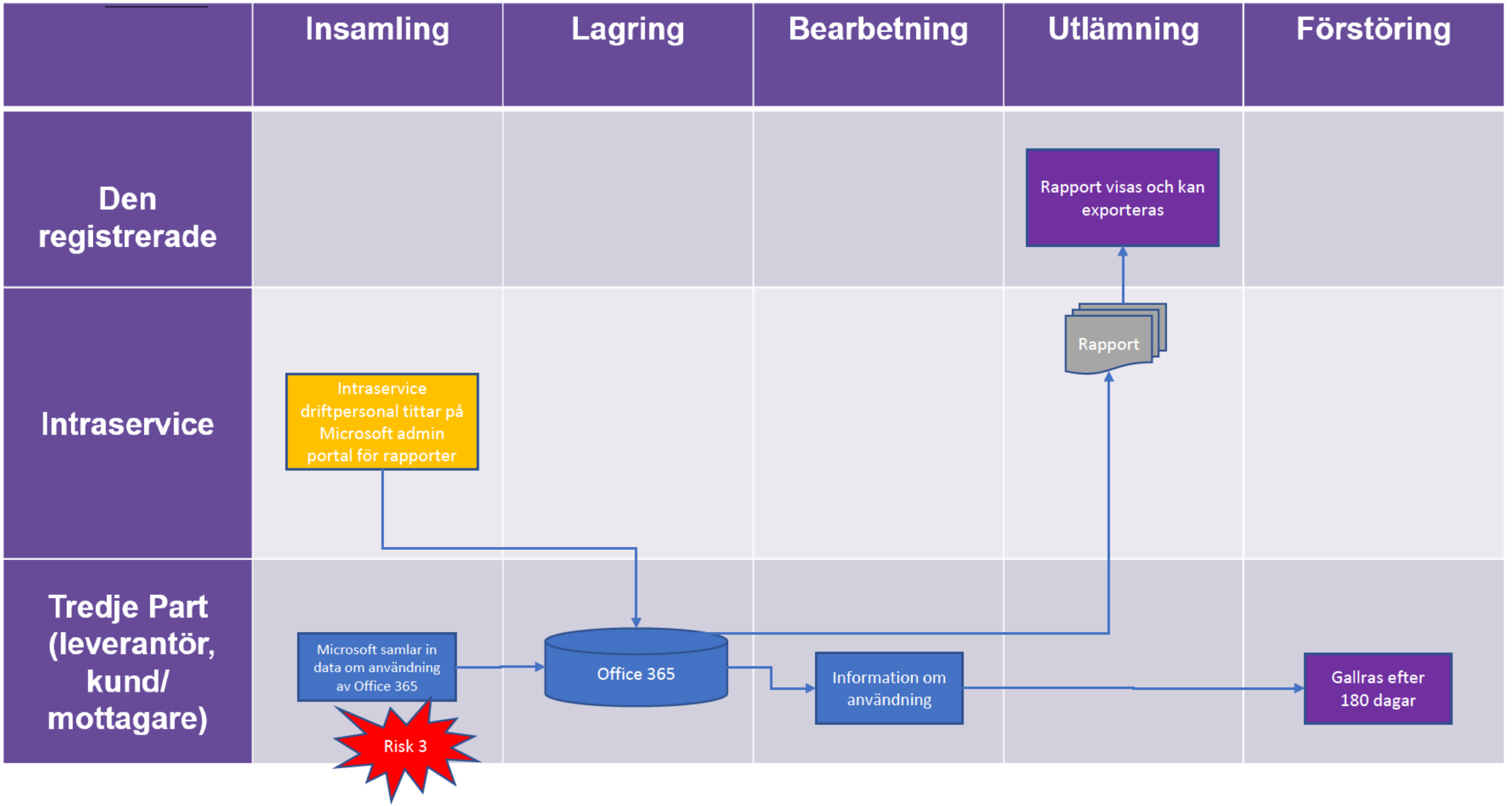
M365/Navet

22 - Microsoft Bookings



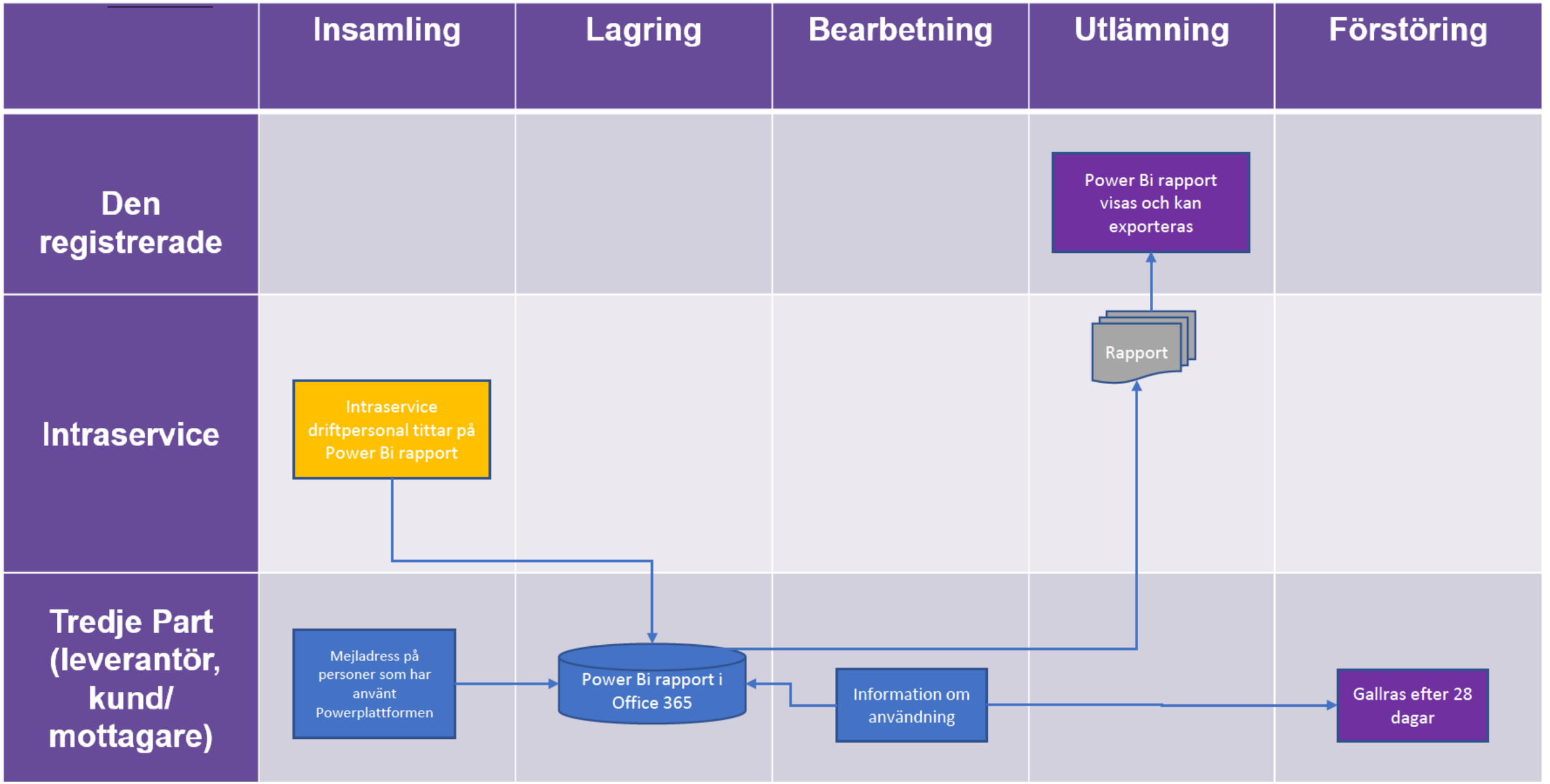
M365/Navet

23 - Rapporter och statistik leveranser



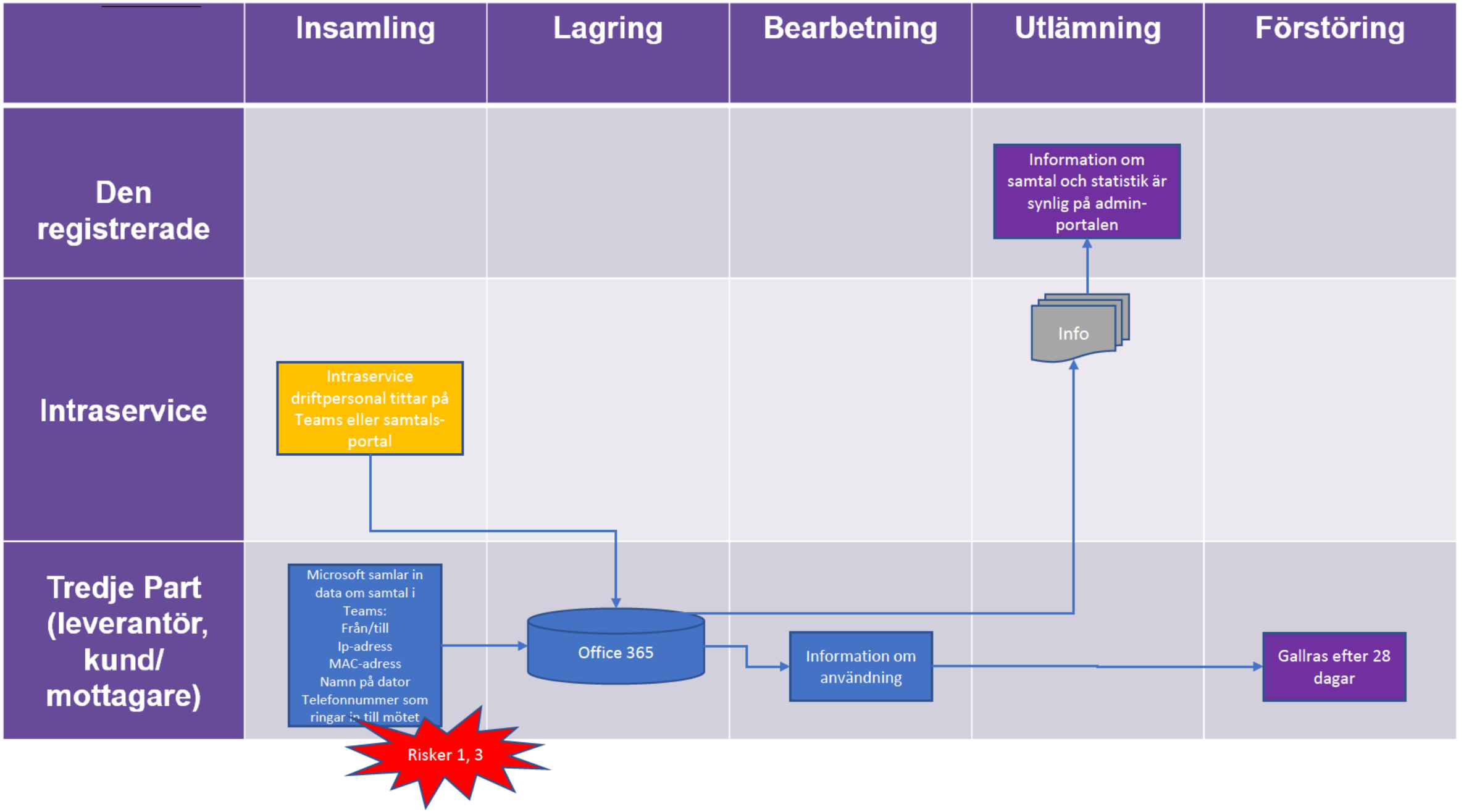
M365/Navet

24 - Center of Excellence (CoE)



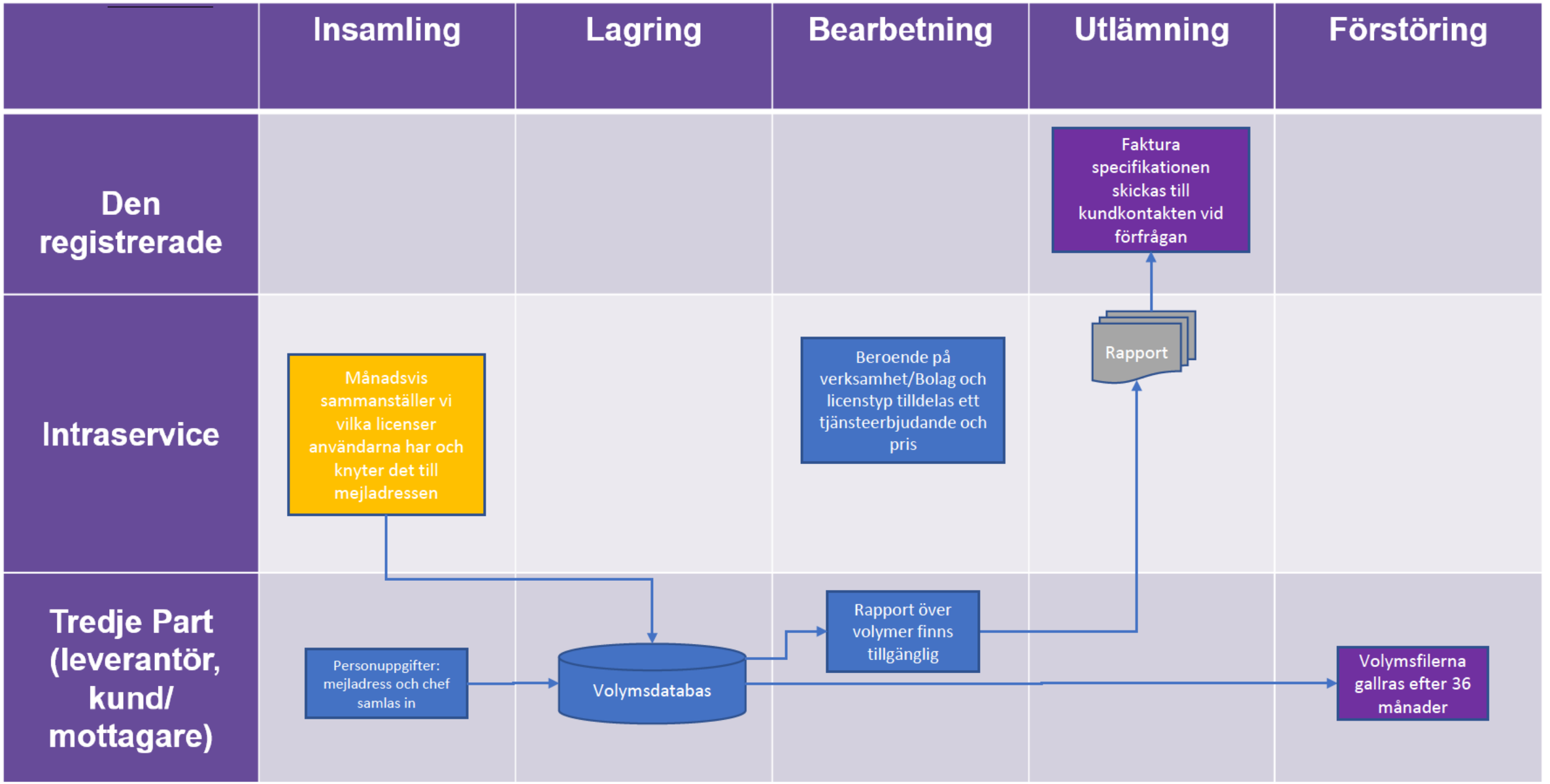
M365/Navet

25 Teams samtalsstatistik/analys



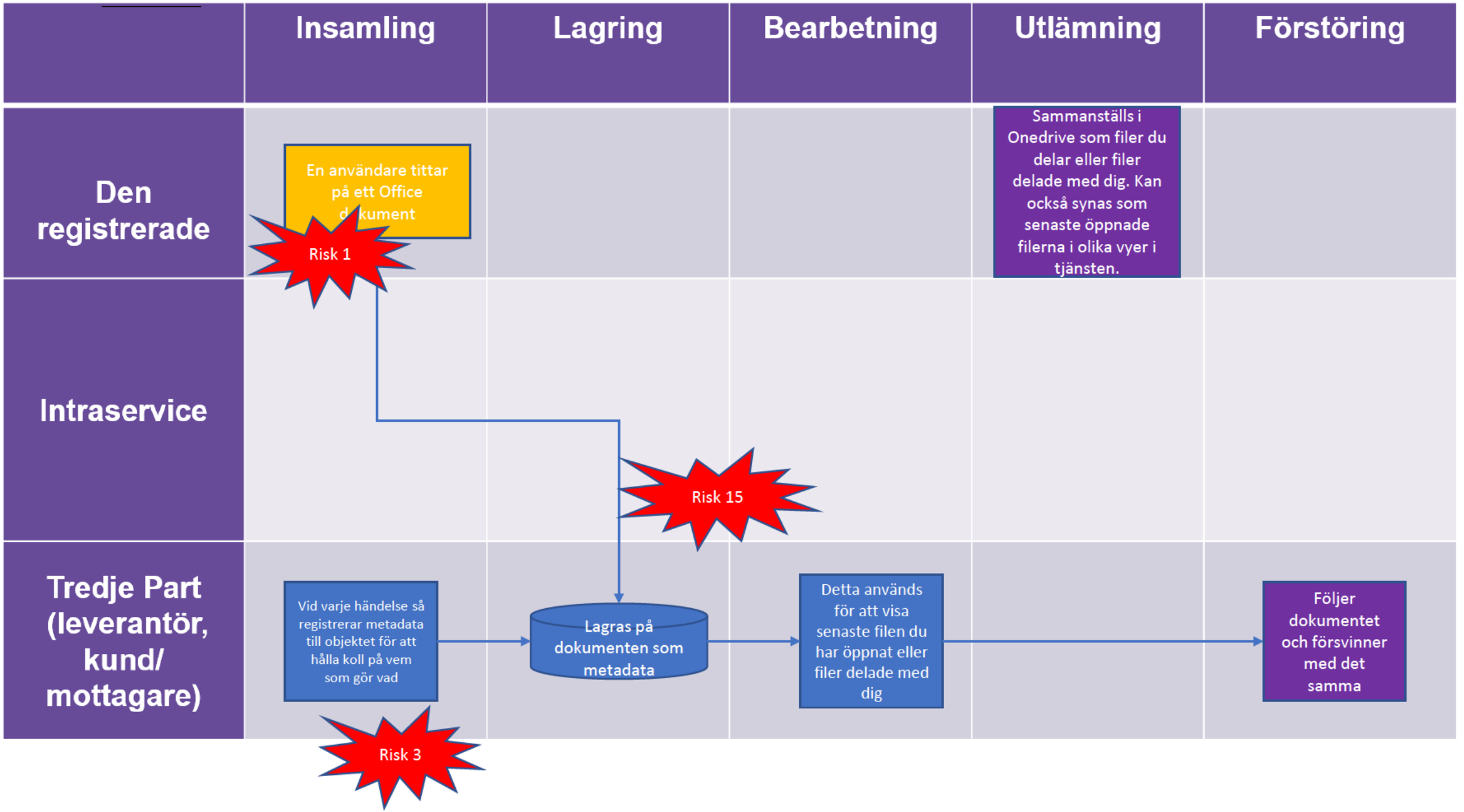
M365/Navet

26 - Volymsrapportering

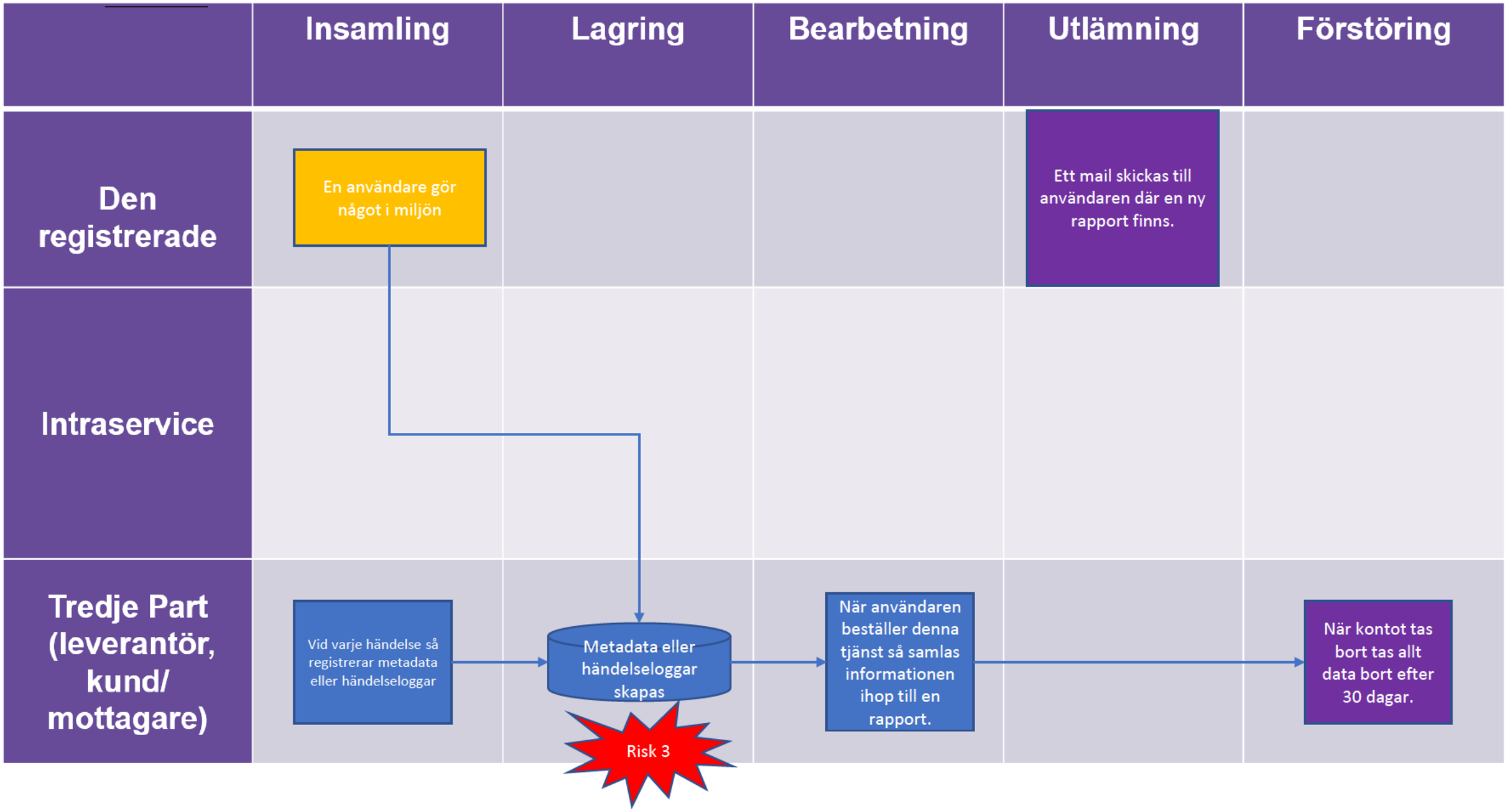


M365/Navet

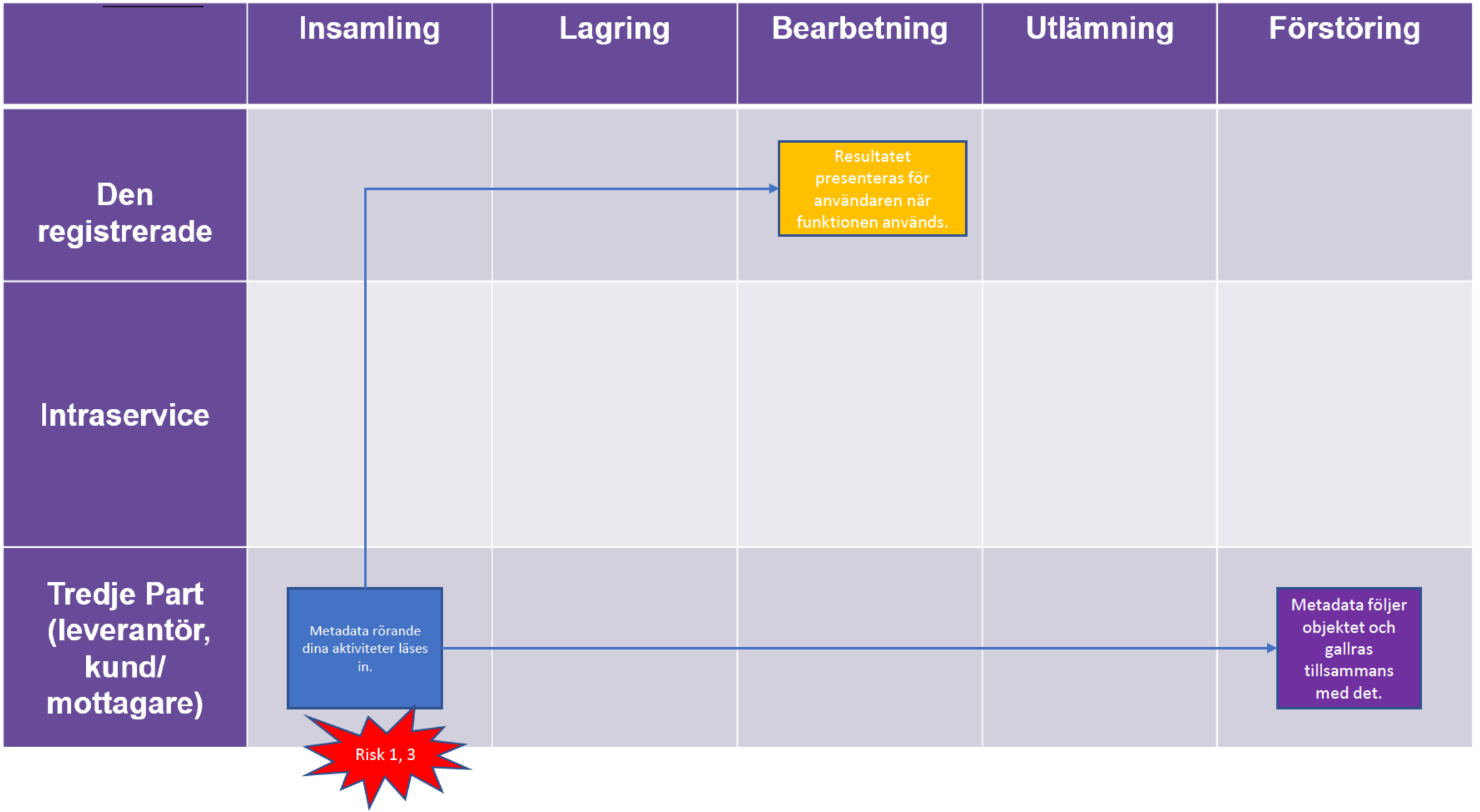
27 - Vem har gjort vad (metadata)



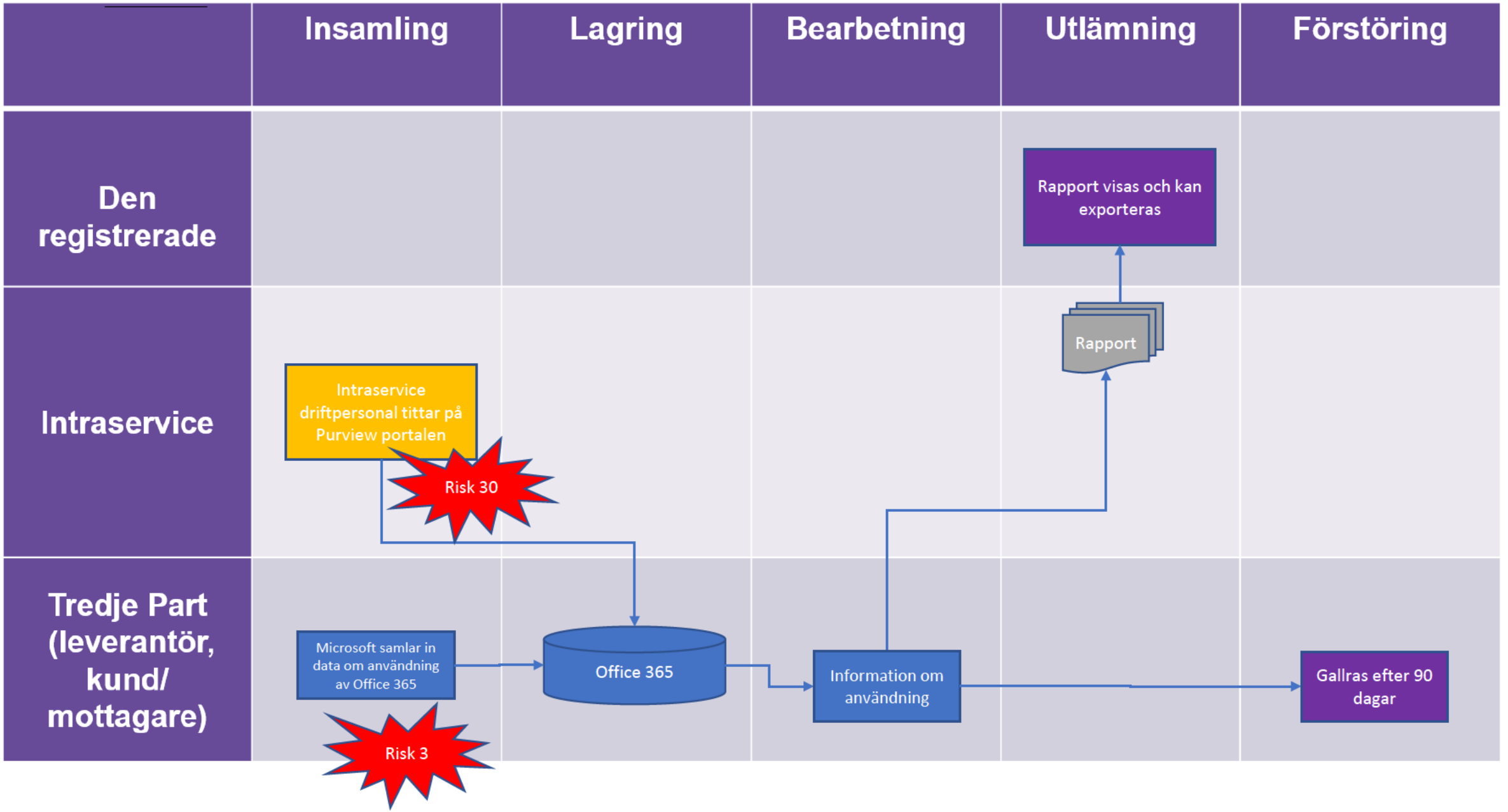
28 - Viva Insights



29 - Delve och liknande SharePoint funktioner



30 - Granskningsloggar



M365/Navet

31- Kontroll av behörighet

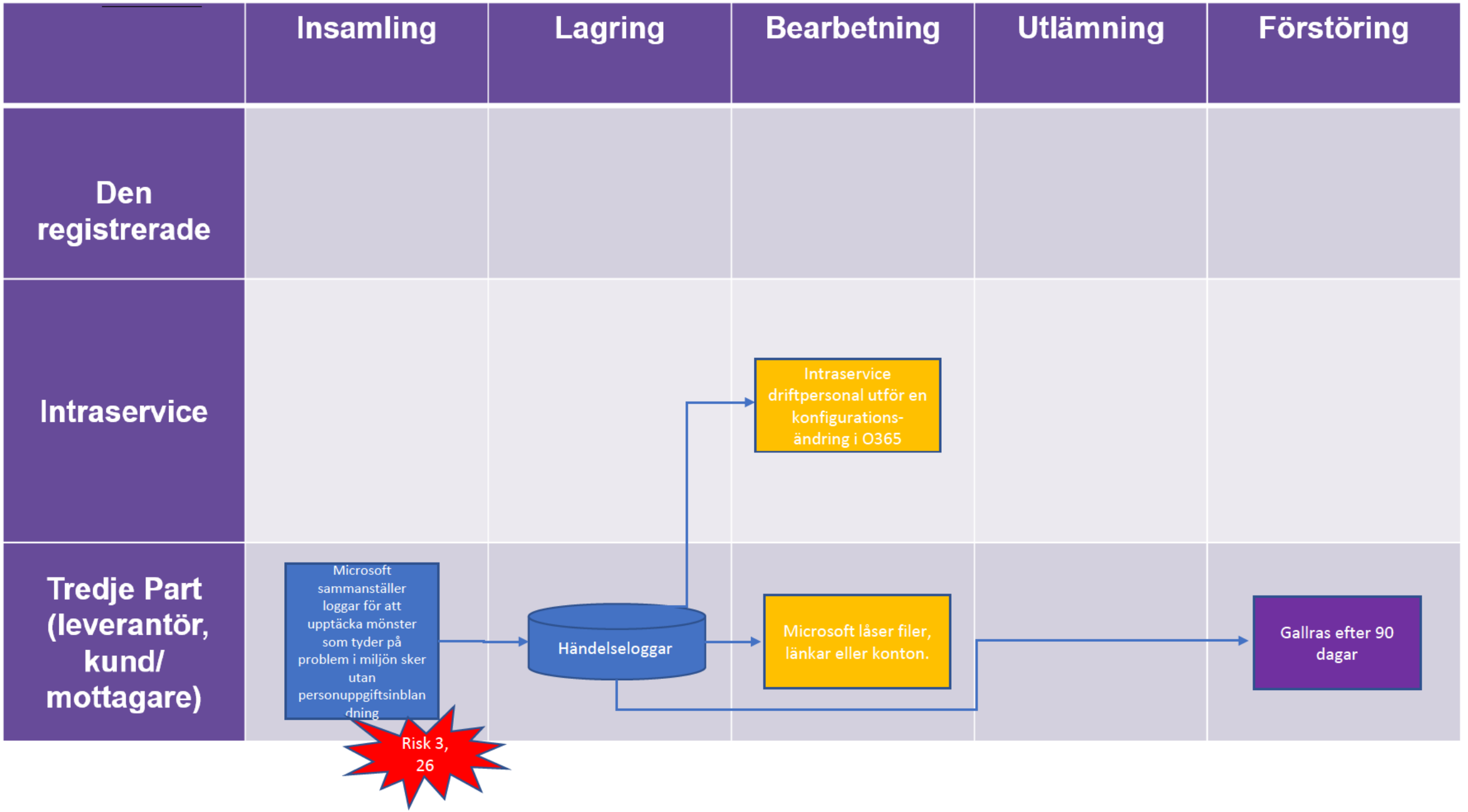
	Insamling	Lagring	Bearbetning	Utlämning	Förstöring
Den registrerade					
Intraservice				Loggar används endast i felsökningssyfte	
Tredje Part (leverantör, kund/ mottagare)	Azure AD håller koll på vad alla konton har rättigheter till. En ny rättighet registreras	Azure AD	Alla förfrågningar om access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

M365/Navet

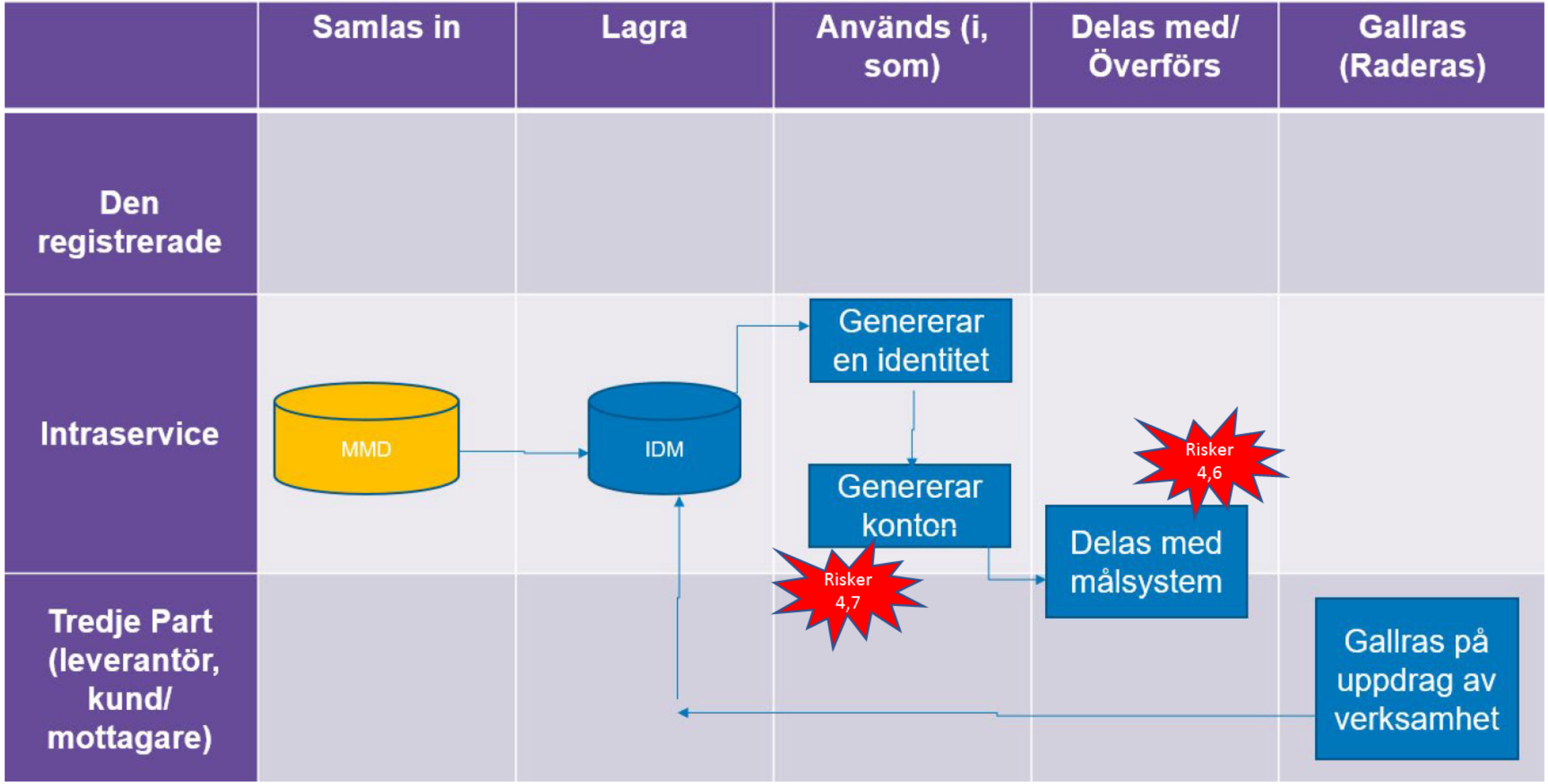
32- Administrativa portaler

	Insamling	Lagring	Bearbetning	Utlämning	Förstöring
Den registrerade					
Intraservice	Intraservice driftpersonal utför en konfigurations-ändring i O365				
Tredje Part (leverantör, kund/ mottagare)	Microsoft tillhandahåller konfiguration av O365 genom administrativa portaler. Info om användare finns i AAD.	Office 365 & Azure AD			Gallras inte eftersom det är en del av O365 tjänsten

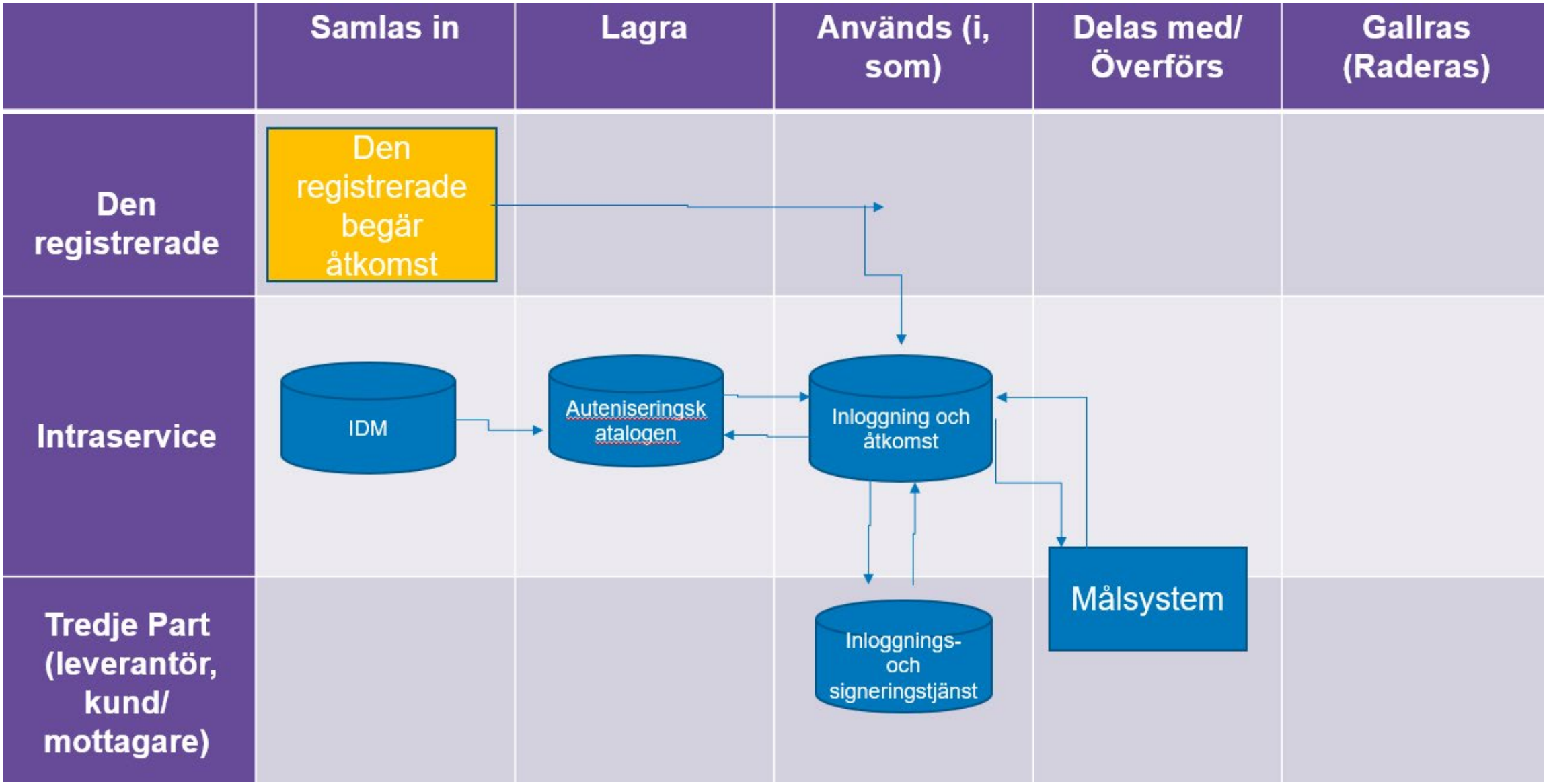
33- Systemkontroller



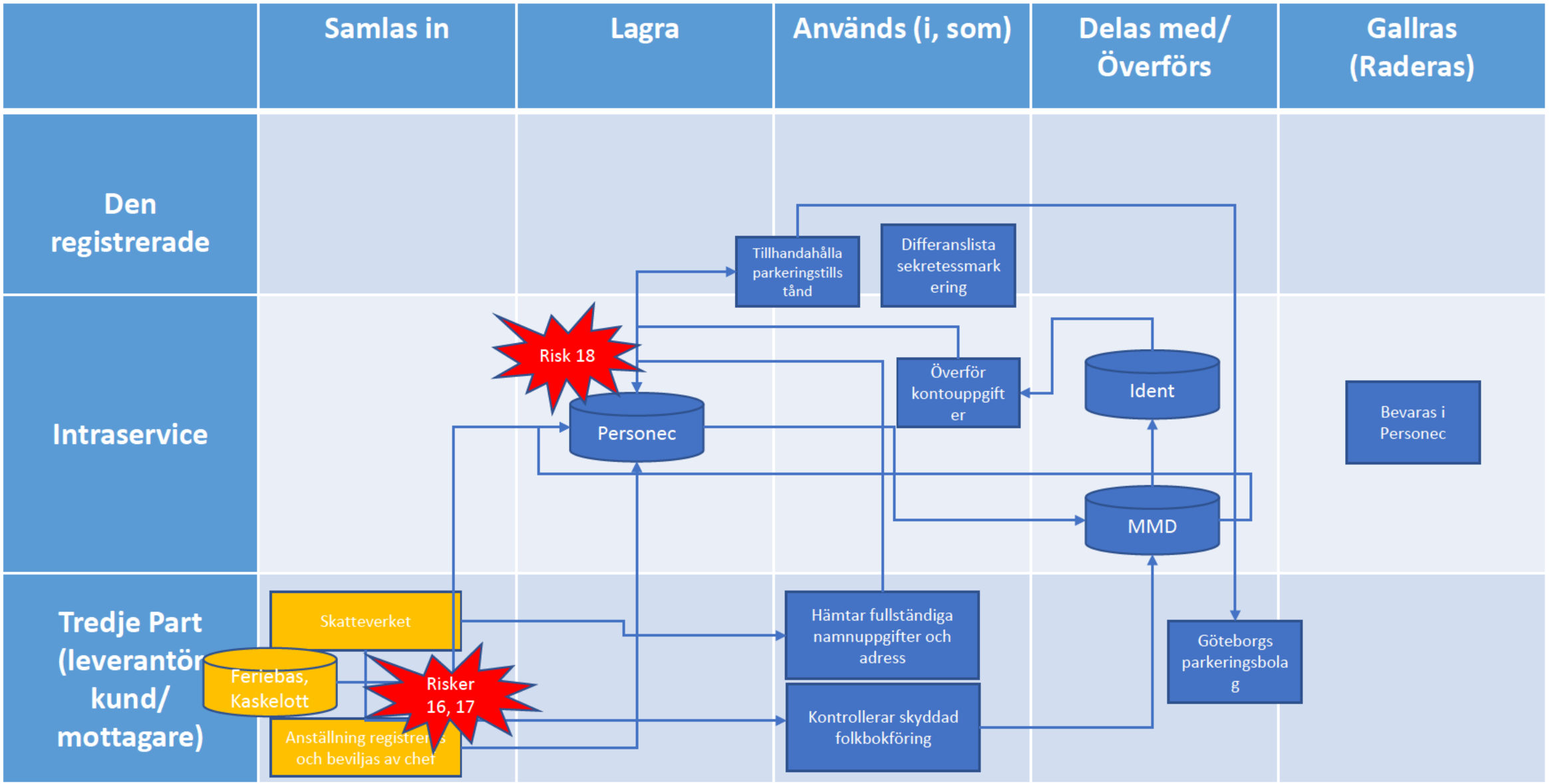
34. Personuppgiftsflöde Identitet



35. Personuppgiftsflöde åtkomst



36. Aktivitet #01 Skapa anställning

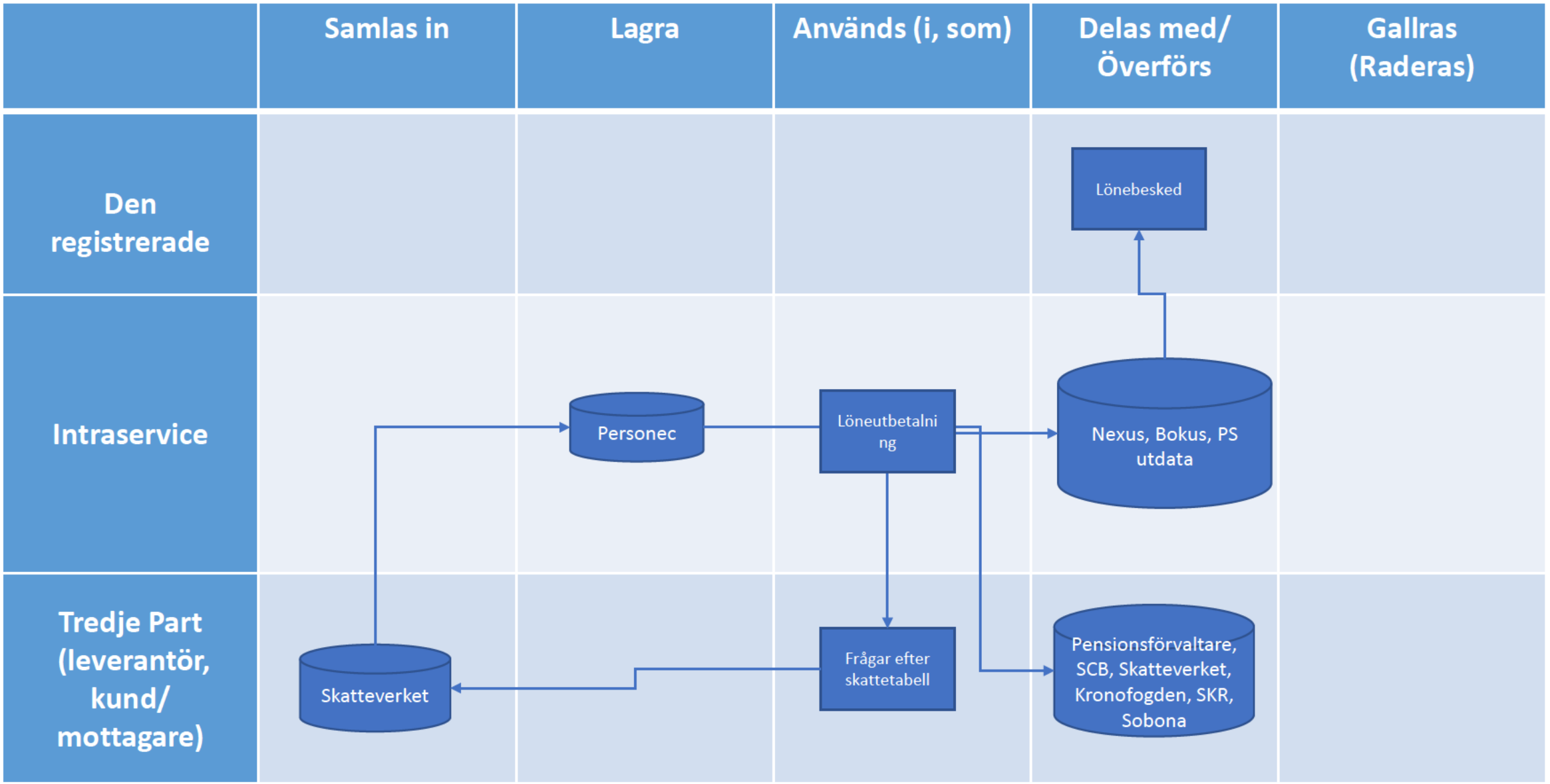


HR & Lön

37. Aktivitet #02 Lönebearbetning

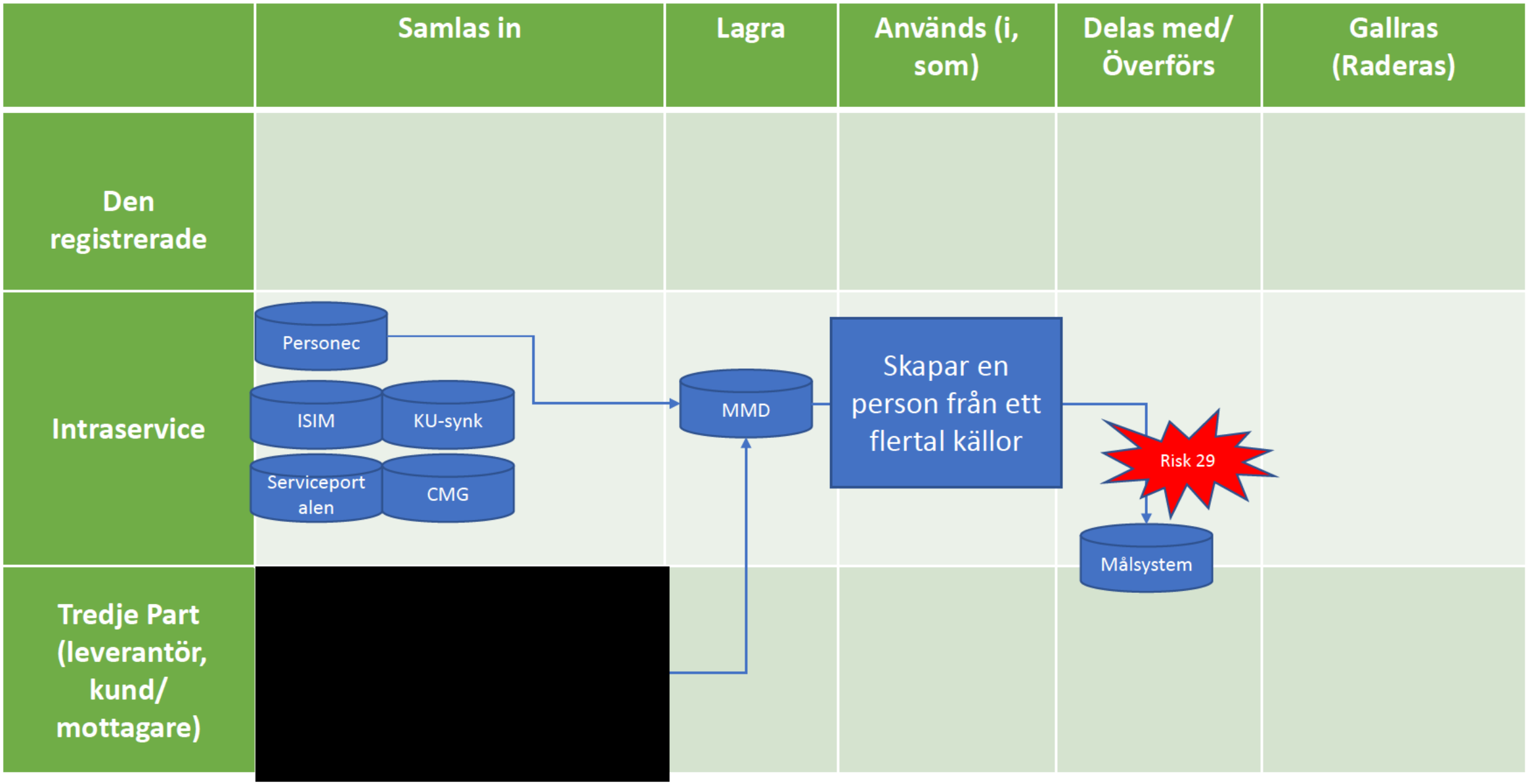
	Samlas in	Lagra	Används (i, som)	Delas med/ Överförs	Gallras (Raderas)
Den registrerade					
Intraservice	Treserva, Timecare	Personec förhandling Personec	Lönebearbetning	Winlas, MMD, Timecare	
Tredje Part (leverantör, kund/ mottagare)	Lex, IFS, Benify, Hastus		Script för kvalitetssäkring	Adato, Försäkringskassan, Benify	

38. Aktivitet #03 Verkställande av lön



Kvalitetssäkrad information

39. Personuppgiftsflöde MMD (Navet)



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

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.

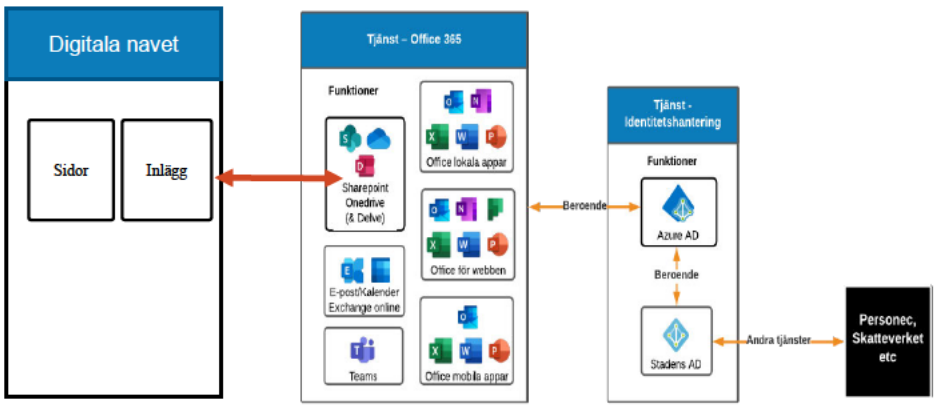
För den som ska fungera som redaktör är det obligatoriskt att gå redaktörsutbildningen och därigenom få access som redaktör.
För att nå Digitala navet om man inte har tillgång till Intraservice gemensamma Microsoft 365-tjänst kan man få så kallad gästkontoaccess. Tjänsten begränsas då till information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

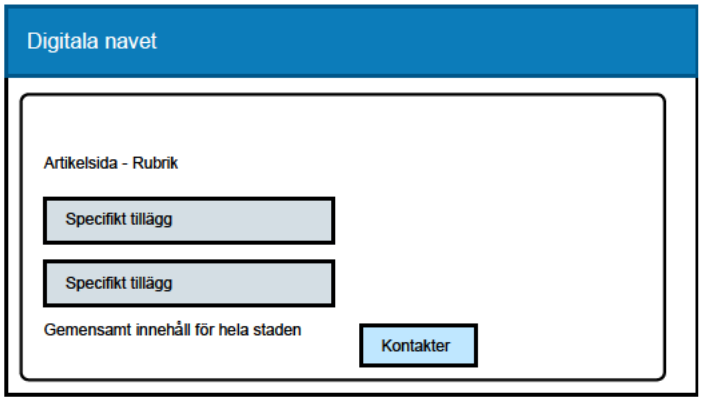
Som redaktör kan man skapa innehåll på sidor i ämnesstrukturen och inlägg i nyhetskanaler som riktar sig till medarbetare inom olika verksamhetsområden och med olika roller. Sharepoint loggar alla sidor/inlägg som skapas och vem som skapat dem. Data baseras på den typen av data som syns i tabellen från 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).

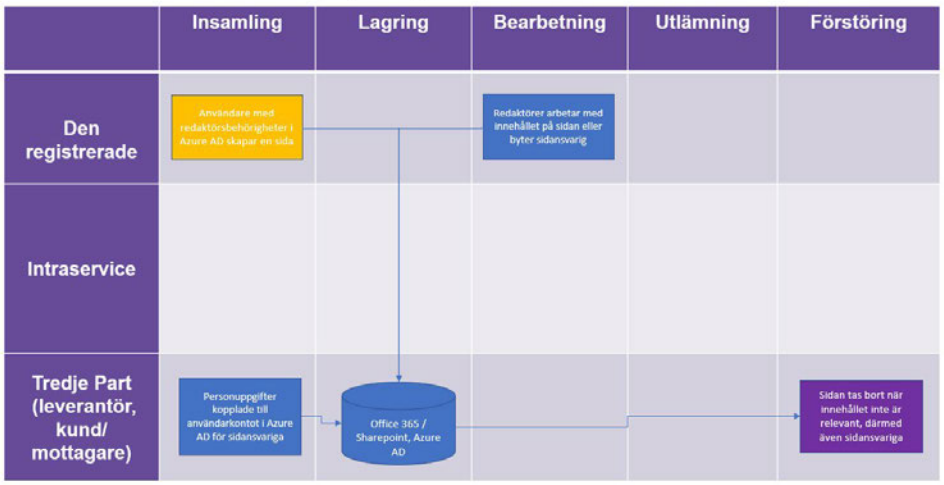
Det finns även möjlighet att inkludera kontakter relaterat till innehållet, både på artikelsidor och specifika tillägg. Kontakter kan exempelvis vara handläggare eller administratörer och behöver inte vara de som ansvarar för sidan. Kontakter kan fyllas i manuellt av redaktören eller via Sharepoints 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

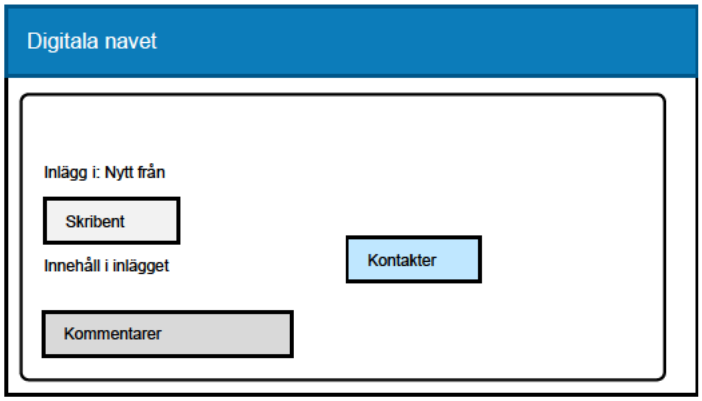
Varje verksamhet som producerar innehåll i artikelsida ansvarar för aktiviteten nedan, vilket är en personuppgiftsbehandling som förvaltning utför med enligt egna mål och medel.

- 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.

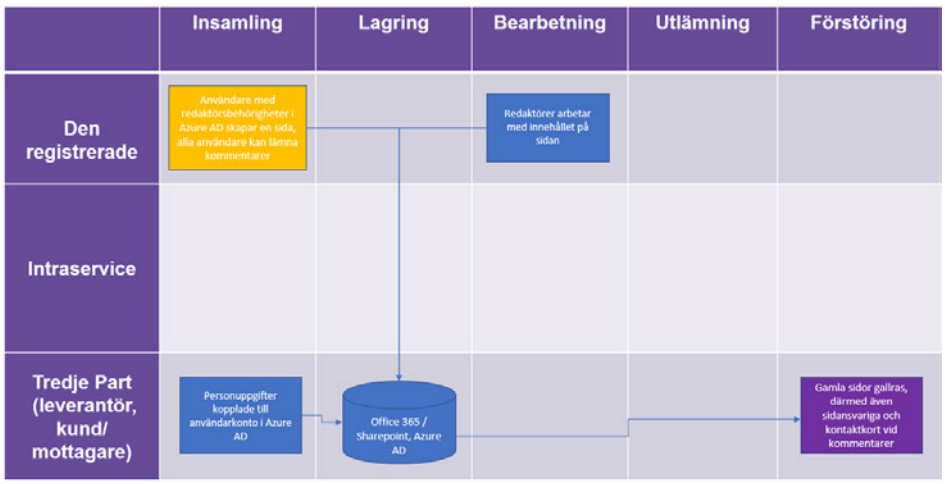
Kommentarsfält kan användas på inlägg i kommunikativa kanaler. I kommentarsfältet kan alla medarbetare lämna kommentarer på inlägget,

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.

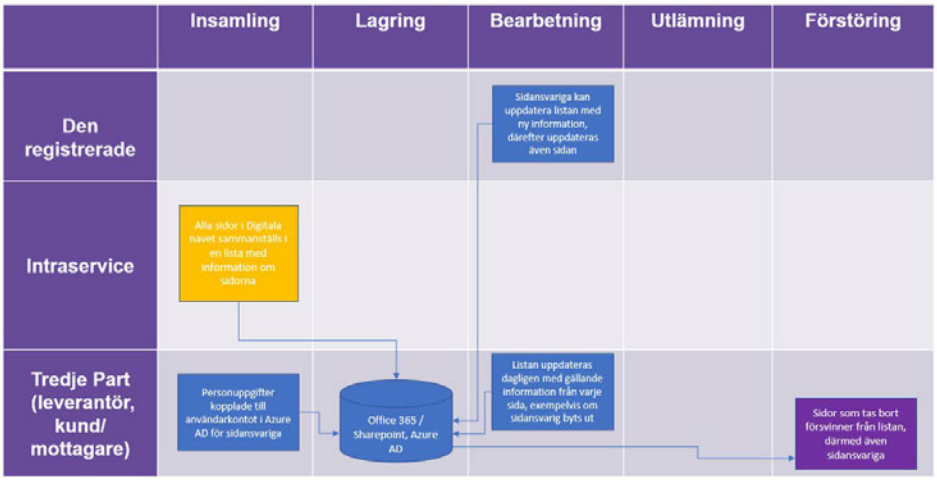
Dessa listor är till för att ge redaktörer en god möjlighet att kunna organisera sitt arbete och en tydlig överblick över varje redaktörs ansvarsområde. Det ska även gå att sortera fram innehåll baserat på vilken förvaltning som ansvarar för innehållet och vara enkelt att ta reda på vem man ska kontakta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

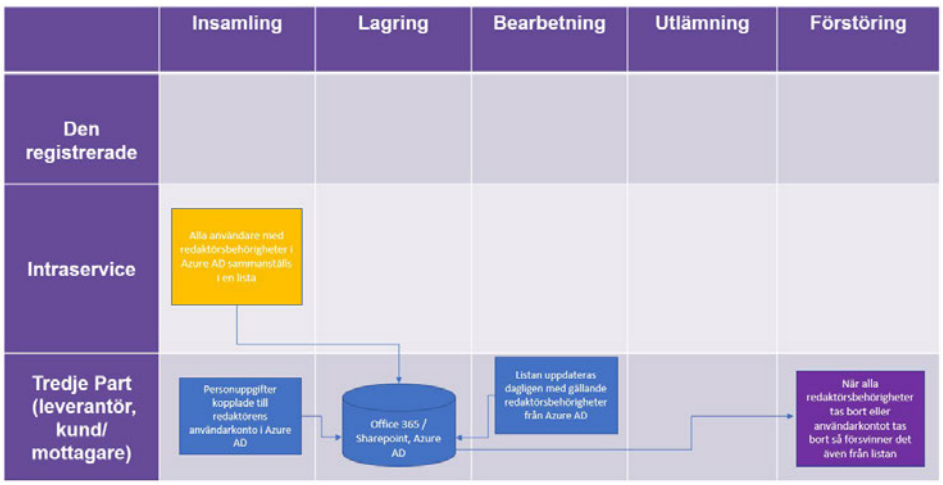


2.2.3.2 Lista över redaktörsbehörigheter

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

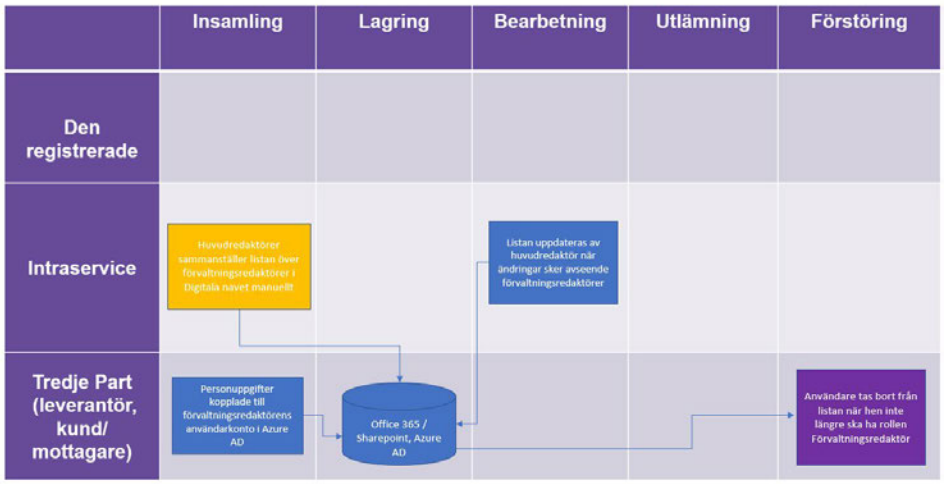


2.2.3.3 Lista över förvaltningsredaktörer

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

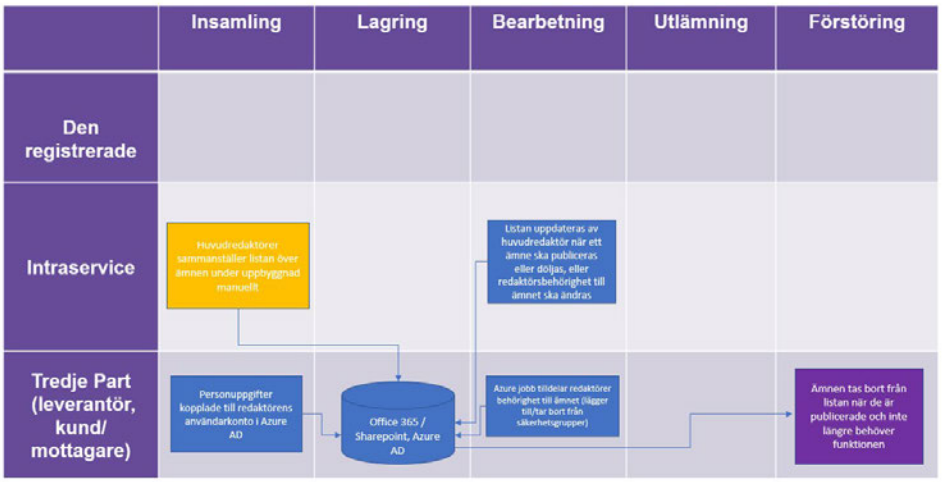


2.2.3.4 Lista för ämnen under uppbyggnad

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

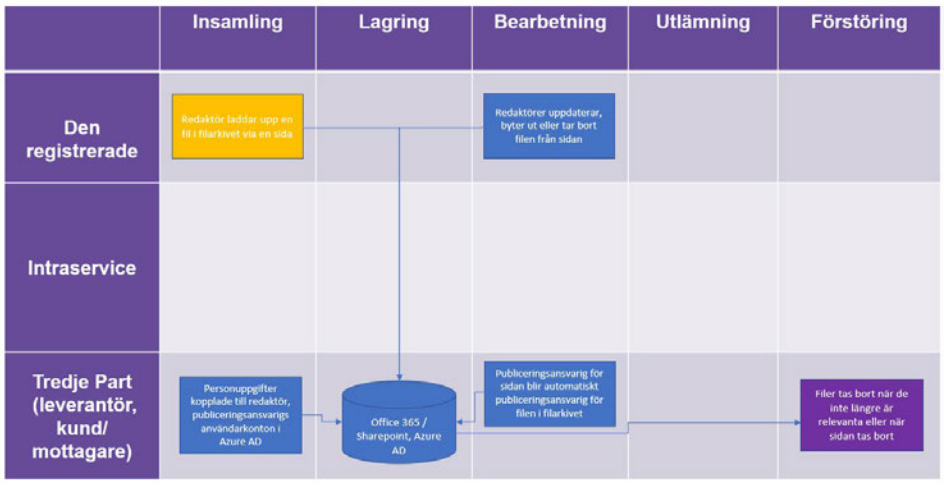


2.2.3.5 Filarkivet i Digitala navet

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.

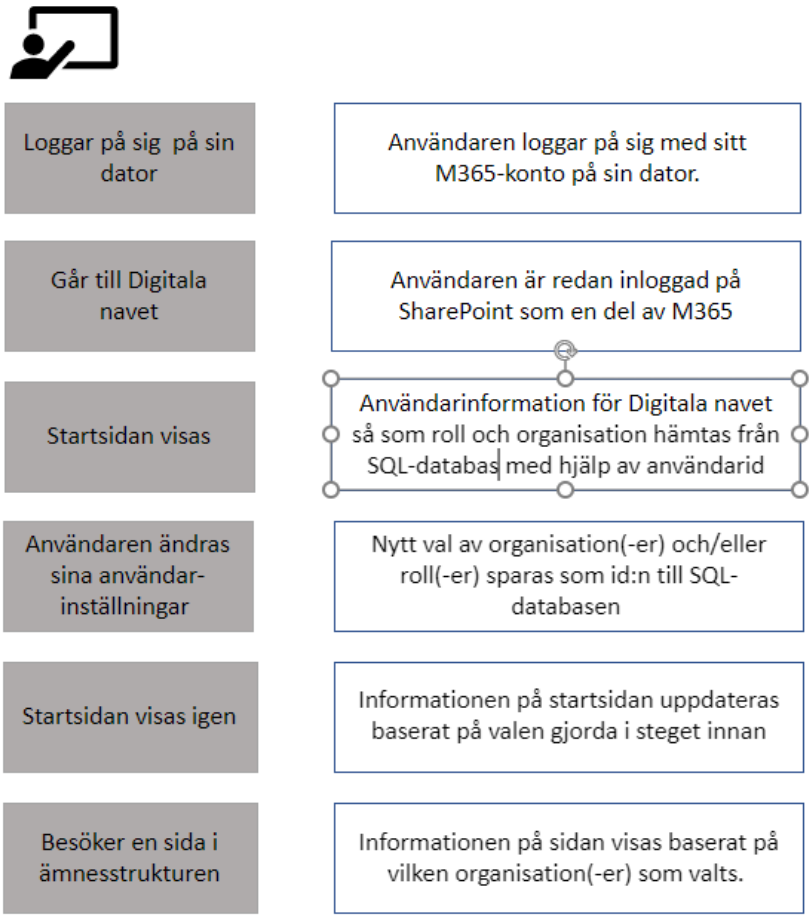
Kommentarer: en sektion i botten på inlägg i kommunikativa kanaler, där vanliga användare kan kommentera inlägget och även tagga andra användare.

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

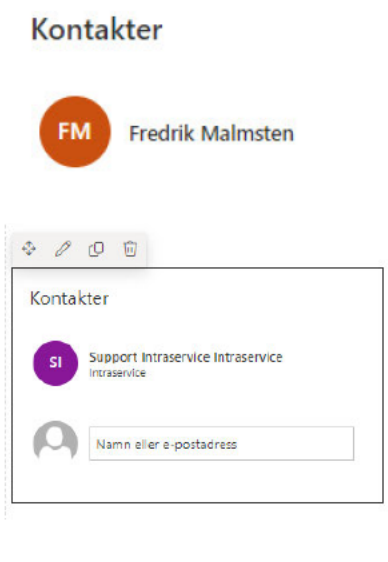
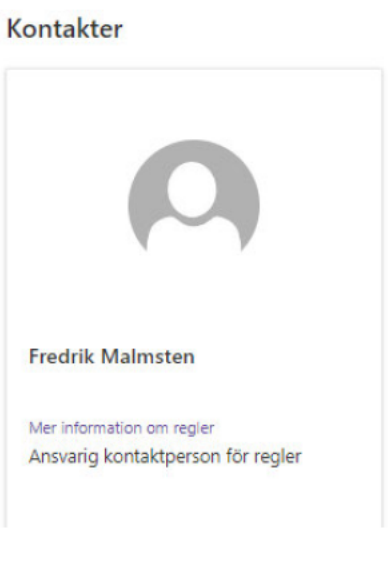
2.3.1 Intraservice användning av personuppgifter

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

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.

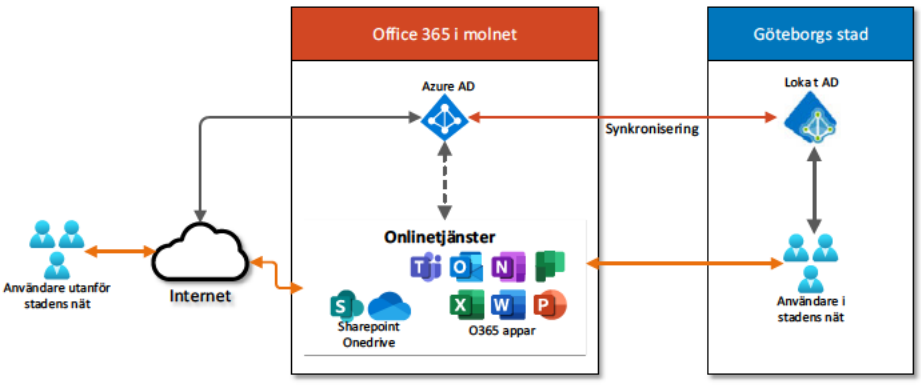
Genom tjänsten kan stadens medarbetare kommunicera, samarbeta och på ett effektivt och säkert sätt få saker gjorda oavsett var man är.

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.

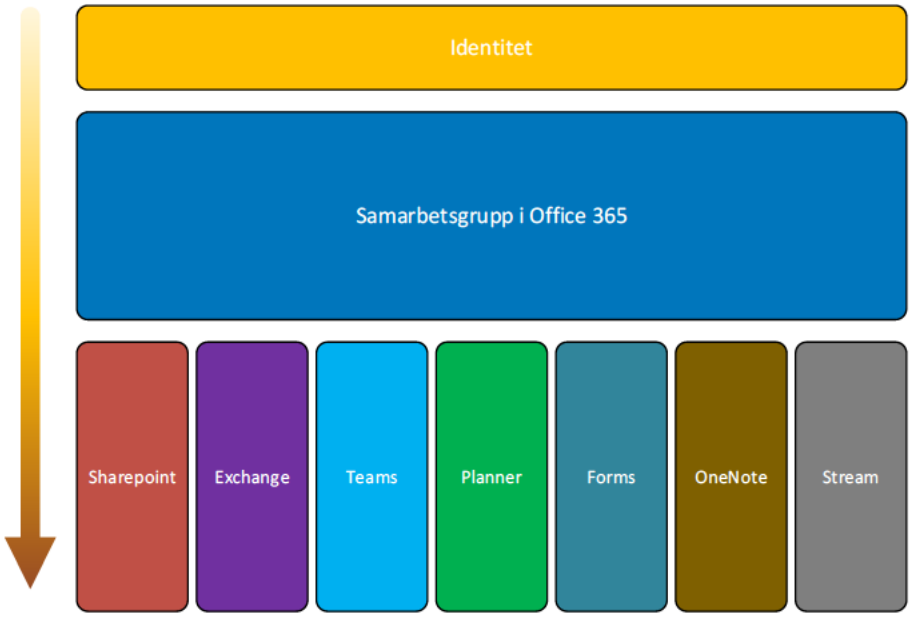
Tjänsten utvecklas utifrån stadens samlade behov. Arbetet med att utveckla tjänsten sker i en utvecklingsorganisation där kundrepresentanter deltar för att fånga in behov kopplade till tjänsten, analysera och prioritera behoven, lansera nya lösningar och förändra arbetssätt.



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.

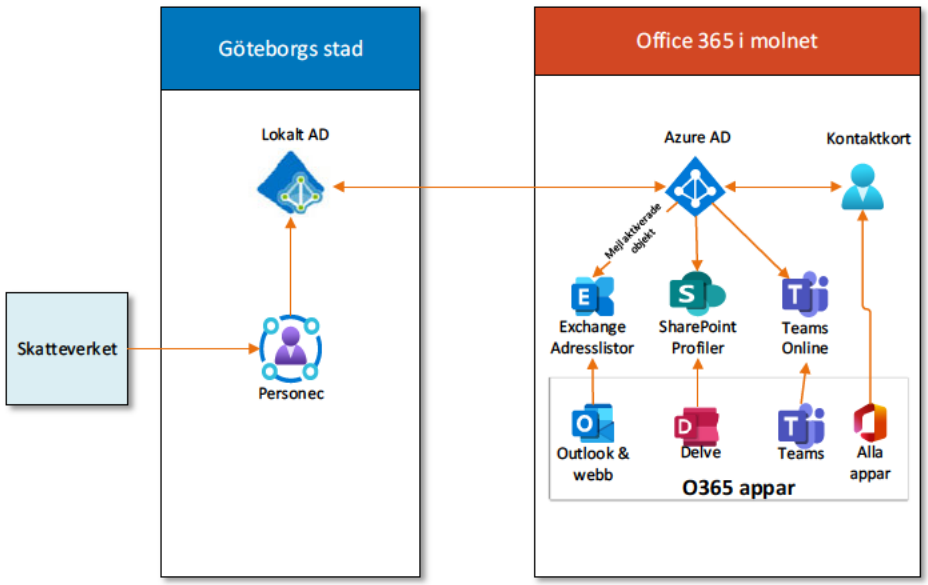


Illustration av personuppgift flödet i Office 365 och den centrala delen kontaktkortet.

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.

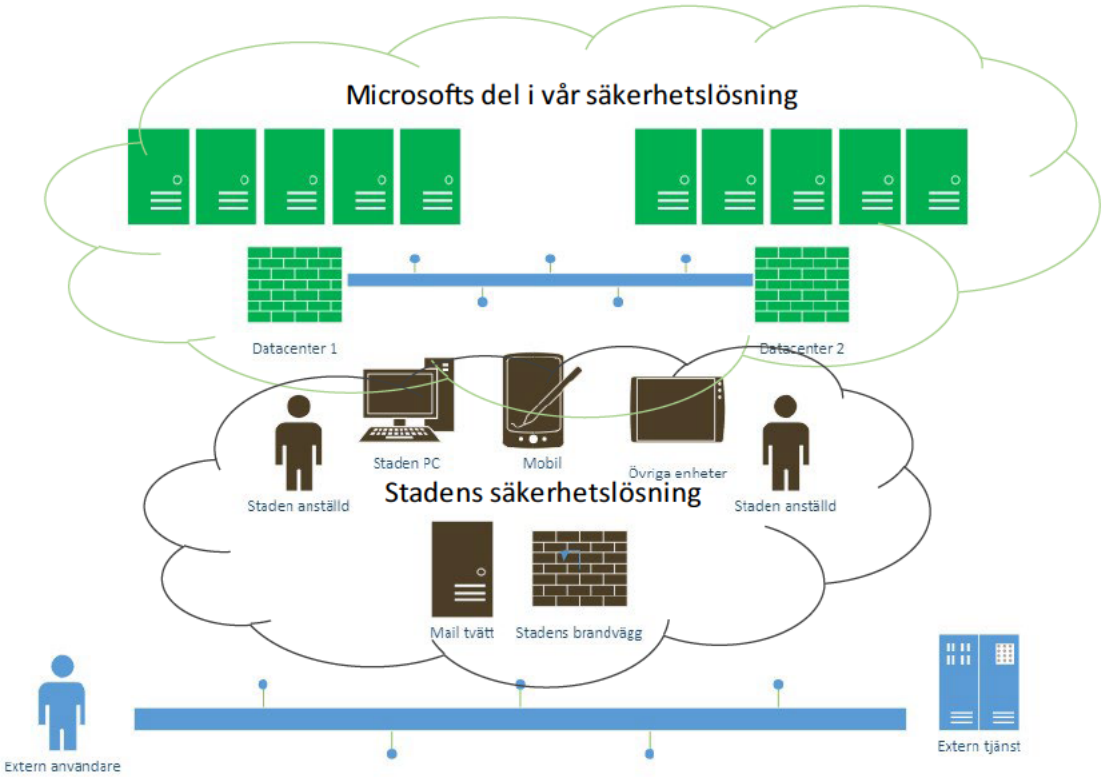


Illustration av tekniska säkerhetslösningen för O365.

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

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

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

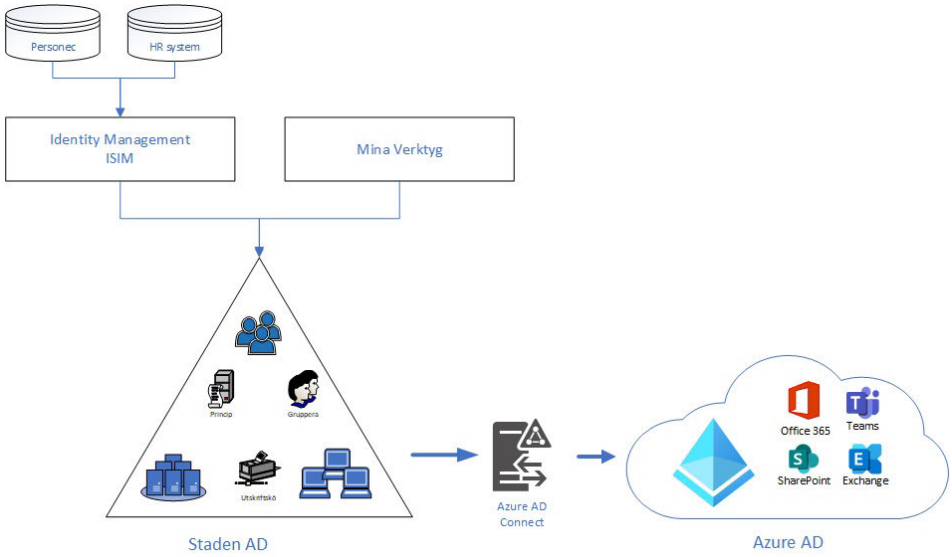
Dessa data omfattar inte användarens namn eller e-postadress eller innehållet i användarens filer.

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.

<table>
<tr><th>Funktion</th><th>Beroende</th><th>Peronsuppgifter</th><th>Syfte</th></tr>
<tr><td>Azure AD</td><td>Stadens AD</td><td>
<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>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</td></tr>
</table>

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

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

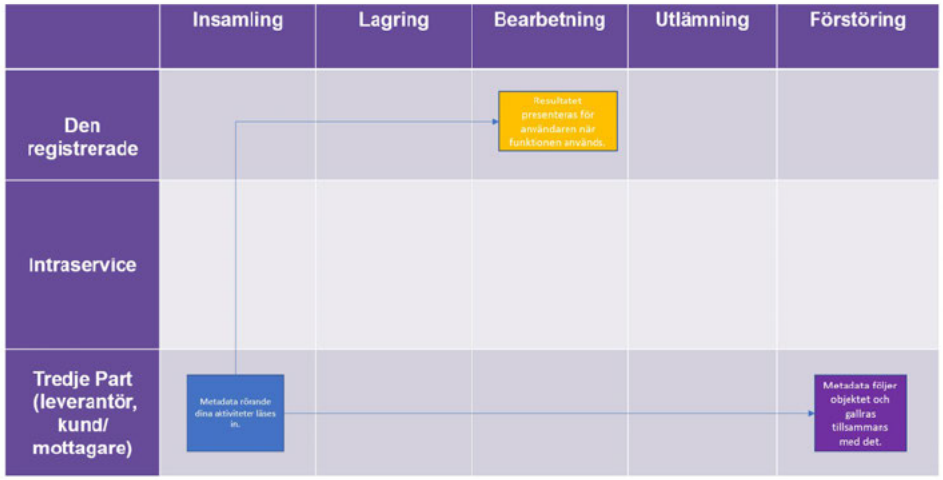
2.2.1 Personuppgiftsflöde

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