Göteborgs Stad

Dokumentnamn: Intraservices rutin för informationsklassning

Beslutad av:	**Gäller för:**	**Diarienummer:**	**Datum för beslutet:**
Intraservices CISO	Samtliga medarbetare	[Nummer]	[Text]
Dokumentsort:	**Giltighetstid:**	**Senast reviderad:**	**Dokumentansvarig:**
Rutin	Tillsvidare	[Datum]	Intraservices CISO

Intraservices rutin för informationsklassning

2024-06-27

IIFS 2-1

Innehåll

Vad är informationsklassning?

Informationsklassning innebär att man värderar organisationens informationstillgångar utifrån interna och externa krav på konfidentialitet, riktighet och tillgänglighet.

Syftet är att sätta rätt nivå av säkerhetsåtgärder beroende på informationens värde. Informationsklassningen är tillsammans med riskanalyser de viktigaste underlagen för att fatta beslut om tillräckliga säkerhetsåtgärder för att skydda informationen.

Ordlista

Ordlistan är en förklaring av vanligt förekommande begrepp. Se Nämnden för Intraservices anvisning för informationsklassning för definitioner av begreppen i ordlistan.

Begrepp	Förklaring
Information	Fakta, idéer eller liknande i en form lämpad för överföring, tolkning eller bearbetning av människor eller av automatiska hjälpmedel.
Informationsmängd	En gruppering av information som kan överföras med hjälp av eller lagras på en eller flera informationsbärare.
Informationsbärare	Den hård- eller mjukvara som används när en informationsmängd överförs, behandlas eller lagras. En informationsmängd kan exempelvis inkomma via ett telefonsamtal, då är telefonisystemet informationsbärare. Informationsmängden kan sedan antecknas i ett verksamhetssystem, då är verksamhetssystemet informationsbärare. Informationsbärarna används för att förmedla, bevara och förädla informationsmängden.
Informationstillgång	Information och informationsbärare som är av värde för en organisation. En informationstillgång är summan av informationen och informationsbäraren.
Informationsägare	Den som ansvarar för den information som skapas och hanteras. Ansvaret för informationen och dess säkerhet följer med ansvaret för verksamheten. Informationssägaren klassificerar och beslutar om informationshantering inom ramen för befintlig lagstiftning och verksamhetskrav.
Systemägare	Den som har ett överordnat ansvar för administration, drift och säkerhet för ett system. Ett system kan innehålla information som tillhör en eller flera informationsägare. Systemägaren ansvarar för att system uppfyller lagkrav och verksamhetskrav som fastställts av informationsägare.
Tillgång	Allt som är av värde för en organisation, exempelvis byggnader, personal, kunskap, applikationer, servrar eller finansiella tillgångar.

Intraservice som myndighet och leverantör

Intraservices modell för informationsklassning tar hänsyn till nämndens organisatoriska uppdelning av förvaltningen som *tjänsteleverantör* å ena sidan och som *förvaltningsmyndighet* å andra sidan.

Som förvaltningsmyndighet upprättar Intraservice information som ska informationsklassas. Det är informationsägaren som har ansvaret för att informationsklassning genomförs. På Intraservice är verksamhetschefer informationsägare.

Som tjänsteleverantör tillhandahåller Intraservice tjänster till staden, och även till Intraservice som förvaltningsmyndighet. Säkerheten i Intraservices tjänster behöver motsvara de krav som uppstår när Intraservice som förvaltningsmyndighet, övriga nämnder, förvaltningar och bolag informationsklassar sin information.

Vem informationsklassar vad

Förvaltningar och bolag som nyttjar Intraservices tjänster ansvarar för att informationsklassa det som kallas *innehållsinformation*.

Exempel: innehållsinformation

Innehållsinformation är den information som uppstår när användare nyttjar tjänsten. Det kan handla om dokument, meddelanden, bilder etc. som skapas i samband med att staden genomför sitt dagliga arbete.

Intraservice som tjänsteleverantör ska endast informationsklassa den information som andra nämnder, förvaltningar eller bolag inte tar ansvar för. Det innebär i praktiken information som upprättas i tjänsterna och används gemensamt av staden, den informationen kallas *gemensam innehållsinformation*.

Exempel: gemensam innehållsinformation

Gemensam innehållsinformation är information som tillhandahålls av tjänsten och nyttjas av flera användare eller tjänster men som inte skapats av användarna. Informationen är så att säga en del av tjänsten.

Det kan handla om användardatabaser, metadatastrukturer, sammanställningar av stora mängder information som presenteras i olika vyer etc.

Utöver den gemensamma innehållsinformationen ska även information som skapas i samband med drift av tjänsten informationsklassas, den informationen kallas *funktions- och säkerhetsinformation*.

Exempel: funktions- och säkerhetsinformation

Funktions- och säkerhetsinformation är den information som tekniskt eller praktiskt upprättas i samband med tjänsteleveransen. Det kan handa om loggar, certifikat, kryptonycklar, listor över komponenter eller applikationer etc.

Beslut om informationsklassning görs av *informationsägaren.* På Intraservice innebär detta att varje processägare är ansvarig för informationsklassning av de processer denna ansvarar för. Processägaren är alltid en verksamhetschef. För processer som fastställts av annan part, exempelvis av kommunstyrelsen eller kommunfullmäktige, ansvarar den verksamhetschef på Intraservice som tilldelats ansvar för verkställande av processen.

För tjänster är det *systemägare,* som på uppdrag av tjänstens informationsägare, ansvarar för att informationsklassning av tjänstens gemensamma innehållsinformation och funktions- och säkerhetsinformation genomförs.

Före workshop

Besluta om informationsklassning

Beslut om att inleda informationsklassning kan föranledas av fyra kategorier händelser:

- Förändrad användning av informationen i en process eller förändringar i en verksamhetsprocess. Även förändringar i lagar, styrande dokument eller avtal som har påverkan på informationen i processen motiverar förnyad informationsklassning.
- Nyinförskaffning av informationsbärare i form av exempelvis nya applikationer i de fall den tekniska lösningen förändrar användningen av informationen, exempelvis om lösningen skapar nya informationsmängder eller förändrar arbetssättet väsentligt.
- Utveckling av nya tjänster eller andra IT-lösningar som påverkar eller skapar nya informationsmängder i processen.
- Periodicitet. Om informationsklassning inte har genomförts av någon annan anledning inom en period av fyra år ska en förnyad informationsklassning genomföras.

Beslut om att informationsklassning ska genomföras görs av *informationsägare*. På Intraservice innebär detta att varje processägare är ansvarig för informationsklassning av de processer denna ansvarar för. Processägaren är alltid en verksamhetschef. För processer som fastställts av annan part, exempelvis av kommunstyrelsen eller kommunfullmäktige, ansvarar den verksamhetschef på Intraservice som tilldelats ansvar för verkställande av processen.

För tjänster är det *systemägare* som på uppdrag av tjänstens informationsägare ansvarar för att informationsklassning av tjänstens gemensamma innehållsinformation och funktions- och säkerhetsinformation informationsklassas.

Beslut om att informationsklassning ska genomföras behöver inte dokumenteras. Om informationsägaren däremot beslutar att informationsklassning inte ska genomföras ska beslut dokumenteras i diariet.

Om informationsklassning ska genomföras bör tidigare informationsklassningar av aktuell process ligga som grund för informationsklassningsarbetet. Man genomför då en så kallad aktualisering. Deltagarna går då igenom tidigare klassning och identifierar eventuella förändringar.

Utse informationsklassningsansvarig

Informationsägaren (eller systemägare som på uppdrag av informationsägare ansvarar för informationsklassning) kan utse en informationsklassningsansvarig som håller i det praktiska arbetet med genomförande av workshop, dokumentation etc. Ansvar och fastställande kan däremot inte överlåtas på informationsklassnings-ansvarig.

Den person som utses bör ha god kännedom om processen som ska informationsklassas samt om de roller som verkar inom processen.

Enheten för informationssäkerhet kan kontaktas som stöd i informationsklassningsarbetet. Detta kan vara hjälpsamt vid informationsklassning av särskilt komplexa eller verksamhetskritiska processer.

Begär ärende

Informationsklassning ska dokumenteras i Intraservices diarie. Begär ärende *”Informationsklassning av [process/tjänst]”*. Ärendet avslutas när informationsklassningen är fastställd. En informationsklassning omfattas sällan av sekretess.

Undersök om det finns någon etablerad verksamhetsprocess

Om det finns en etablerad verksamhetsprocess enligt *Intraservices anvisning för processkarta och processarkitektur* ska den ligga till grund för informationsklassningsarbetet. Om etablerad process saknas behöver processen visualiseras innan eller i samband med workshop. Till er hjälp med att skapa process kan lämpligt verktyg användas, exempelvis Visio, post-it-lappar, 2c8, Powerpoint etc. Stöd finns att tillgå från Kvalitets- och utvecklingsenheten.

Processgrupper ska inte informationsklassas. Se *Intraservices anvisning för processkarta och processarkitektur* för vidare vägledning gällande processer.

Identifiera deltagare

Det är viktigt att belysa informationssäkerheten ur så många aspekter som möjligt vid en informationsklassning. Därför är urvalet av deltagare en central aspekt vid genomförandet. För att säkerställa en kvalitativ informationsklassning ska en väl avvägd grupp deltagare kallas, exempelvis:

- Någon som har aktuell erfarenhet av att arbeta i processen eller delar av processen i praktiken, exempelvis handläggare, administratörer.
- Någon som har erfarenhet av att arbeta med systemstöd i processen, exempelvis systemförvaltare, systemadministratör, tekniker eller IT-arkitekter.
- Någon som har kunskap om eller erfarenhet av processens regleringar, exempelvis jurist, handläggare med lång erfarenhet eller dataskyddskontakter.

Inför informationsklassning ska dataskyddsombudet tillfrågas om denne behöver vara närvarande vid workshoppen. Kontakt sker via funktionsbrevlåda dso@intraservice.goteborg.se.

Se till att grupperingen inte blir för stor men att den ändå täcker ovanstående områden, 5–7 personer brukar vara lämpligt. Vissa komplexa processer spänner över enhets- och verksamhetsgränser och det är viktigt att engagera personer från samtliga berörda verksamheter.

Samla in underlag

Inför informationsklassningsworkshoppen är det lämpligt att samla in relevanta underlag.

- Processkarta och processbeskrivning.
- Lagar eller styrdokument som gäller för processen och som har påverkan på informationshanteringen, exempelvis patientdatalagen, lagen om geografisk miljöinformation etc.

- Avtal eller överenskommelser som reglerar informationshanteringen, exempelvis sekretessavtal eller personuppgiftsbiträdesavtal.
- Eventuella tidigare informationsklassningar, andra förvaltningar eller kommuners klassningar alternativt informationsklassningar av liknande art.

Det underlättar om den som är informationsklassningsansvarig sätter sig in i materialet i förväg. Denne kan då välja bort den information som inte är relevant för just den här informationsklassningen.

Planera en workshop för att informationsklassa

Informationsklassningsansvarig kallar till möte.

Tänk på att informationsklassning kan vara tidskrävande, räkna med minst två sittningar på cirka 2–3 timmar vardera. Det är lättare att genomföra en informationsklassningsworkshop på plats än på distans.

Innan ni börjar:

- Ladda ner en kopia av informationsklassningsmallen. Se bilaga 6 i denna rutin.
- Förbered en digital eller fysisk kopia av processen ni ska informationsklassa. Om det inte finns någon etablerad process ska ni ta fram den process ni ska informationsklassa i verktyget Visio, 2c8 eller liknande. Detta kan göras innan eller i samband med workshoppen. Guide för processmodellering finns att tillgå på sharepointytan för Intraservices processer.
- Den informationsklassningsansvarige sätter sig in i klassningsprocessen.
- Fyll i mallens förstasida innan workshoppen

Klassningsobjekt			Incidentprocessen
Ansvarig:	Silja Löving		Diarienummer: 0243/24
Klassningsdokumentation			
Klassning genomförd:	2024-03-12		
Klassning genomförd av:	Torkel Yrstad - Intraservice		
	Nadja Fors - Intraservice		
	Ahmed Mysk - Intraservice		
	Höjje Blom - ÄVO		
	[Deltagare 5]		
	[Deltagare 6]		
	[Deltagare 7]		
	[Deltagare 8]		
	[Deltagare 9]		
	[Deltagare 10]		

Genomförande av workshop

Vid workshoppen genomförs själva informationsklassningsarbetet.

Utbilda deltagarna

Starta med en kortare utbildning av deltagarna med hjälp av presentation, se bilaga 5.

Undersök om processen omfattas av säkerhetsskydd

Säkerhetsskydd innebär att skydda den information och de verksamheter som är av betydelse för *Sveriges säkerhet* mot spionerі, sabotage, terroristbrott och vissa andra hot. Säkerhetsskydd regleras i säkerhetsskyddslagen, se bilaga 2.

Uttrycket ”Sveriges säkerhet” innefattar sådant som är av grundläggande betydelse för Sverige ur ett nationellt perspektiv, som försvaret, det demokratiska statsskicket, rättsväsendet och samhällsviktig verksamhet.

I sällsynta fall är det möjligt att processen som ska analyseras helt eller delvis är en del av verksamhet som omfattas av säkerhetsskyddslagen och att

detta inte har identifierats i Intraservice säkerhetsskyddsanalys. Om tveksamhet råder ska Intraservice säkerhetsskyddsansvarig alltid kontaktas för konsultation.

Omfattas den aktuella processen av säkerhetsskydd, avbryts informationsklassningen och processen ska i stället hanteras i säkerhetsskyddprocessen.

Exempel: Undersöka om processen omfattas av säkerhetsskydd

En av deltagarna identifierar att processen för Change management kan ha påverkan på ett för *Sveriges säkerhet* viktigt SCADA-system (system för övervakning och styrning av fysiska processer) som omhändertas av ett kommunalt bolag.

Konsekvenserna för *Sveriges säkerhet* är oklara och informationsklassningsansvarig avslutar därför workshoppen och kontaktar säkerhetsskyddsansvarig.

Identifiera informationsmängder

Identifiera de informationsmängder som tillhör varje enskild processaktivitet. I vissa fall hanteras ingen information i processaktiviteten. Gå då vidare till nästa processaktivitet. I andra fall hanteras flera olika informationsmängder i samma processaktivitet. Tänk på att även information i muntlig form och på papper kan behöva klassas.

Informationen ska delas upp i informationsmängder, som består av en väl avgränsad mängd information med ett specifikt syfte i processen. Det kan exempelvis vara faktura, konton, beslut, tjänsteutlåtande, rapport etc.

Ibland kan det vara till hjälp att tänka i termer av ingående - behandling - utgående information:

- Vilken information kommer in i aktiviteten?
- Vilken information uppstår eller behandlas i aktiviteten?
- Vilken information går ut ur aktiviteten?

Här kan det vara bra att ta en processaktivitet i taget och låta gruppmedlemmarna skriva ner vilka informationsmängder dom uppfattar ingår i processaktiviteten på post-it lappar.

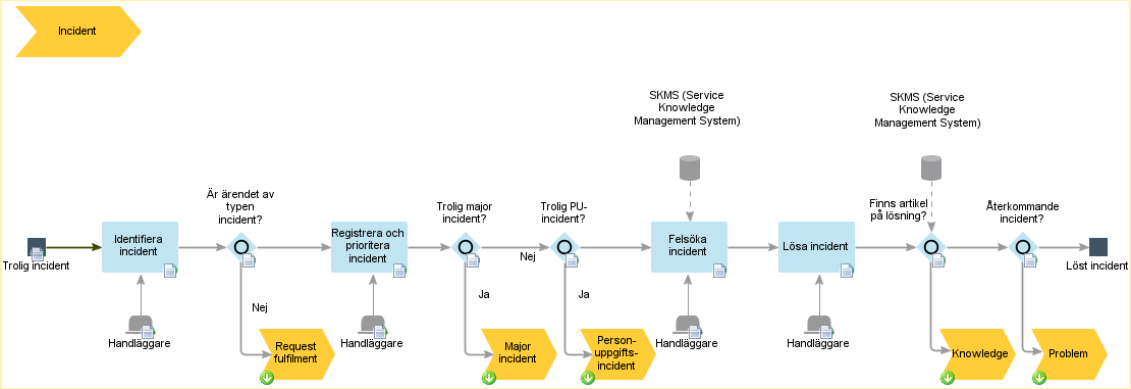
Informationsmängderna ska inte delas upp i mindre beståndsdelar än sin databärare eller handling. Ett papper, en word- eller pdf-fil eller ärendekort ska inte delas upp i mindre beståndsdelar.

Notera att det är informationsmängder som ska identifieras, inte eventuella informationsbärare. En informationsmängd kan behandlas av en eller flera informationsbärare men i denna del av informationsklassningsprocessen är det endast informationsmängderna som är av intresse.

Fyll i de identifierade informationsmängderna i mallen under rubriken "informationsmängder", fyll i vilken processaktivitet informationsmängden är förknippad med och skriv en kort beskrivning av informationsmängden. Fyll i varje identifierad informationsmängd på en ny rad.

#ID	Aktivitet	Informationsmängd	Beskrivning
Instruktion	*Aktivitet i processkartan*	*T.ex. faktura, beslut, logg*	*T.ex. namn, adress, artikel-ID, belopp*
#0001	Identifiera incident	Incidentanmälan	Inkommande rapportering om misstänkt pågående incident
#0002	Registrera och prioritera incident	Incidentärende	Metadata om pågående incident, löpnummer, namn på anmälare mm
#0003	Registrera och prioritera incident	Rapport	Symptom och påverkan av incidenten
#0004	Trolig major incident?	Beslut	Beslut om incidenten är en Major incident
#0005	Trolig PU-incident	Beslut	Beslut om incidenten är en Personuppgiftsincident
#0006	Felsöka incident	Felsökningsprotokoll	Utredning av orsak
#0007	Lösa incident	Kunskapsartiklar	Kunskapsartiklar om hur incidenten kan lösas
#0008	Löst incident	Meddelande	Meddelande till anmälare om att incidenten är löst

Exempel: Identifiera informationsmängder i incidentprocessen



Deltagarna identifierar följande informationsmängder i processen:

- incidentanmälan
- incidentärende
- rapport
- beslut
- felsökningsprotokoll
- kunskapsartiklar
- meddelande

Identifiera reglering

Efter att informationsmängderna har identifierats ska varje informationsmängd eller processen som helhet analyseras i syfte att identifiera om informationen omfattas av någon reglering.

Regleringar kan bestå av lagar, förordningar eller föreskrifter men också stadens eller förvaltningens styrdokument. Ibland är det endast enskilda informationsmängder som omfattas av viss reglering och i andra fall kan det vara samtliga informationsmängder i processen.

Vissa typer av regleringar omfattar nästan alla informationsmängder. Till dessa hör:

- Göteborgs stads riktlinjer för informationssäkerhet (RIS)
- Tryckfrihetsförordningen (TF)
- Offentlighets- och sekretesslagen (OSL)
- Arkivlagen (ArkivL)
- GDPR

Denna klassningsmodell utgår från att samtliga informationsmängder omfattas av någon av ovanstående fem regleringar. I de sällsynta fall en informationsmängd inte är en handling i TF:s bemärkelse eller en informationsmängd inte innehåller några personuppgifter ska detta uppges. Skriv då “ej TF” eller “ej GDPR” i spalten reglering.

I andra fall är det speciallagstiftning eller styrdokument som gäller för enskilda processer eller verksamheter som behöver identifieras. Det är därför viktigt att någon av deltagarna i workshoppen har god kunskap om reglering som gäller för klassningsobjektet.

Exempel: Identifiera reglering

Fram till och med bedömning om Major incident omfattas aktiviteterna även av *NIS-direktivet* eftersom Intraservice är leverantör av digital infrastruktur till Kretslopp och vatten samt Äldrevård- och omsorgsförvaltningen.

#ID	Aktivitet	Informationsmängd	Reglering
Instruktion	Aktivitet i processkartan	T.ex. faktura, beslut, logg	T.ex. lagkrav, styrdokument, sekretessreglering
#0001	Identifiera incident	Incidentanmälan	NIS
#0002	Registrera och prioritera incident	Incidentärende	NIS
#0003	Registrera och prioritera incident	Rapport	NIS
#0004	Trolig major incident?	Beslut	NIS
#0005	Trolig PU-incident	Beslut	
#0006	Felsöka incident	Felsökningsprotokoll	
#0007	Lösa incident	Kunskapsartiklar	
#0008	Löst incident	Meddelande	

Identifiera sekretessreglerade uppgifter

För varje informationsmängd som kan förväntas innehålla sekretessreglerade uppgifter ska aktuell paragraf i offentlighets- och sekretesslagen anges. Se bilaga 1 för vanligt förekommande sekretessreglering på Intraservice. Notera att kunders informationsmängder med stor sannolikhet har andra uppsättningar sekretessregler att förhålla sig till.

Observera att en sekretessreglerad uppgift inte alltid behöver omfattas av sekretess, i stället ska en bedömning göras om uppgifter i

informationsmängden återkommande kan bedömas omfattas av sekretess enligt den givna paragrafen i offentlighets- och sekretesslagen.

Tillämpliga sekretessregleringar ska fyllas i med formaten ”[kapitel]:[paragraf]”, exempel: 18:8.

Exempel: Identifiera sekretessreglerade uppgifter

Deltagarna bedömer att pågående incidentärenden i många fall kan komma att omfattas av sekretess enligt:

- OSL 18 kap. 3 §, uppgifter i en incidentrapport kan komma att ligga till grund för en anmälan till polisen om dataintrång.
- OSL 18 kap. 8 §, detaljuppgifter om IT-miljöns uppsättning och specifika sårbarheter skulle kunna nyttjas av en antagonist om uppgifterna sprids.

#ID	Aktivitet	Informationsmängd	Sekretess
Instruktion	Aktivitet i processkartan	T.ex. faktura, beslut, logg	
#0001	Identifiera incident	Incidentanmälan	18:8
#0002	Registrera och prioritera incident	Incidentärende	18:8
#0003	Registrera och prioritera incident	Rapport	18:8, 18:3
#0004	Trolig major incident?	Beslut	
#0005	Trolig PU-incident	Beslut	
#0006	Felsöka incident	Felsökningsprotokoll	18:8, 18:3
#0007	Lösa incident	Kunskapsartiklar	
#0008	Löst incident	Meddelande	

Identifiera personuppgifter

Kontroller om respektive informationsmängd innehåller personuppgifter. En personuppgift är varje form av upplysning som direkt eller indirekt kan kopplas till en fysisk levande person. Detta innebär att en personuppgifter

inte bara är något som kan härledas direkt, som ett namn eller personnummer. De omfattar även indirekta personuppgifter som IP-nummer, hälsoinformation eller en unik identifierare i en applikation.

Personuppgifter ska delas upp i:

- Personuppgifter
- Extra skyddsvärda personuppgifter
- Känsliga personuppgifter

Extra skyddsvärda personuppgifter är:

Oftast kontextbaserade, det kan exempelvis framgå i lagstiftning eller liknande.

Exempel:

- personnummer
- löneuppgifter
- uppgifter om lagöverträdelser
- barns personuppgifter
- uppgifter om sociala förhållanden

Känsliga personuppgifter är:

- etniskt ursprung
- politiska åsikter
- religiös eller filosofisk övertygelse
- medlemskap i en fackförening
- hälsa
- sexualliv eller sexuell läggning
- genetiska uppgifter
- biometriska uppgifter som används för att entydigt identifiera en person

Exempel: Identifiera personuppgifter

Deltagarna identifierar att personuppgifterna

- namn,
- titel,
- telefonnummer,
- e-post och
- organisatorisk tillhörighet

förekommer i incidentanmälningsformuläret. Inga extra skyddsvärda eller känsliga personuppgifter identifieras.

#ID	Aktivitet	Informationsmängd	Personuppgifter
Instruktion	*Aktivitet i processkartan*	*T.ex. faktura, beslut, logg*	*T.ex. namn, IP-nummer, geografisk lokation*
#0001	Identifiera incident	Incidentanmälan	Namn, e-postadress, telefonnummer, organisatorisk tillhörighet
#0002	Registrera och prioritera incident	Incidentärende	Namn, e-postadress, telefonnummer, organisatorisk tillhörighet
#0003	Registrera och prioritera incident	Rapport	
#0004	Trolig major incident?	Beslut	
#0005	Trolig PU-incident	Beslut	
#0006	Felsöka incident	Felsökningsprotokoll	
#0007	Lösa incident	Kunskapsartiklar	
#0008	Löst incident	Meddelande	Namn, e-postadress, telefonnummer, organisatorisk tillhörighet

Informationsklassa informationsmängderna

Varje informationsmängd i processen ska informationsklassas i enlighet med stadens modell för informationsklassning, se bilaga 4.

Informationsklassningens syfte är att identifiera hur allvarliga konsekvenser som uppstår om informationssäkerheten brister i aspekterna konfidentialitet, riktighet och tillgänglighet. Informationsklassningen är tillsammans med riskanalyser de viktigaste underlagen för att i ett senare skede fatta beslut om tillräckliga säkerhetsåtgärder för att skydda informationen.

För vissa informationsmängder är värdet på informationen som hanteras förutsägbart, för andra informationsmängder kan informationens värde variera kraftigt. Detta gäller framför allt information som inkommer från allmänheten eller i processer med brett informationsinsamlade, exempelvis förvaltningens funktionsbrevlåda eller incidenthantering. Försök i dessa fall ringa in den mest verksamhetskritiska informationen och värdera denna.

Bortse från sådan information som felaktigt hanteras i processen. Om sådan information hanteras sker återkommande bör detta tas med i kommande riskanalys.

Alla Informationsmängder ska klassas på en skala mellan 0-4 för konfidentialitet, riktighet och spårbarhet. I praktiken är det sällsynt att en

informationsmängd klassas på den högsta eller lägsta nivån. Nivå 0 innebär att inget skydd behövs för den givna informationsmängden, detta kan vara aktuellt för konfidentialitet om informationen ska publiceras öppet på exempelvis en webbplats. Nivå 4 innebär information som är av vikt för *Sveriges säkerhet* och ska därför hanteras i enlighet med säkerhetsskyddslagen.

Stadens definition av begreppen konfidentialitet, riktighet och spårbarhet är:

Begrepp	Förklaring
Konfidentialitet	Att information inte tillgängliggörs eller avslöjas för obehöriga.
Riktighet	Att informationen skyddas mot oönskad förändring, att information är korrekt och inte manipulerad eller förstörd.
Tillgänglighet	Att information är tillgänglig och användbar när den behövs.

När ni klassar informationsmängder får de en viss klassningsprofil. För en viss informationsmängd kan det till exempel innebära allvarliga konsekvenser om den avslöjas för obehöriga (konfidentialitet) eller inte går att få fram när den behövs (tillgänglighet), men mindre konsekvenser om den inte är helt korrekt (riktighet). En sådan informationsmängd kan då få klassningsprofilen Konfidentialitet 3, Riktighet 1 och Tillgänglighet 3 (K3R1T3).

En informationsmängd ska informationsklassas utifrån det värde informationen har för verksamheten. Det innebär att eventuella säkerhetsåtgärder som har vidtagits för att skydda informationen inte ska påverka informationsklassningen.

Om det är svårt att fastställa informationsklassningsnivå eller om det råder oenighet i gruppen kan det vara hjälpsamt att genomföra en förenklad riskanalys för den enskilda informationsmängden. Se Intreservices rutin för riskbaserat informationssäkerhetsarbete för vägledning.

Hur ska vi tänka - Konfidentialitet?

Samma informationsmängd kan ha olika värde och därmed klassning i olika sammanhang. En faktura, kan t ex, ha olika klassningar beroende på vad det står på den, var den kommer ifrån och vem den skickas till:

Exempel konfidentialitet - fakturor

1. En faktura som skickas till en förvaltning för tillhandahållande av en tjänst innehåller i normalfallet inte några känsliga uppgifter och bör därför kunna klassas som Konfidentialitet 1.

2. En specificerad faktura från en leverantör där det framgår exakta styckepriser eller namn på konsulter kan omfattas av sekretess till förmån för leverantörens affärsverksamhet och kan sannolikt klassas som Konfidentialitet 2. Detta är under förutsättningen att uppgifterna skadar leverantörens affärsverksamhet. Om leverantören agerar inom en marknad med mycket små prisvariationer eller där tillgången på arbetskraft är stor kan samma uppgifter i stället klassas som Konfidentialitet 1.

3. Faktura som skickas till enskild inom ramen för hälso- och sjukvårdsverksamhet eller företagshälsovård omfattas av sekretess och innehåller uppgifter som definieras som känsliga personuppgifter enligt GDPR. Informationen bör sannolikt klassas som Konfidentialitet 3.

4. En faktura från leverantör som specificerar en uppsättning produkter i kritisk IT-infrastruktur innebär en risk för att en antagonist kan genomföra kartläggning av svaga punkter inför planerade intrångsförsök. Informationen bör sannolikt klassas som Konfidentialitet 3.

Hur ska vi tänka - Riktighet?

Samma informationsmängd kan ha olika värde och därmed klassning i olika sammanhang. En logg, t ex, kan ha olika klassningar ur riktighets-aspekten beroende på vilken verksamhetsinformation systemstödet innehåller, vilken effekt eventuella felaktigheter i loggning får eller eventuella lagkrav verksamheten lyder under gällande uppföljning och loggning.

Tänk på att riktighet ur ett informationssäkerhetsperspektiv inte ska jämställas med datakvalitet. Förlust av riktighet har att göra med informationen obehörigt, av misstag eller på grund av funktionsstörning har förändrats. Datakvalitet kan variera på grund av brister i riktighet, men även på grund av medvetna val från förvaltningen gällande uppställda krav på hur exakt informationen ska motsvara verkliga förhållanden.

Basnivå (riktighet 1) ska inte jämställas med att riktigheten i informationen är oviktig eller att det inte spelar någon roll om informationen är felaktig. Grundnivå av riktighet speglar ett helt normalt krav på riktighet och inte godtycklighet eller att det inte spelar någon roll om informationen är felaktig.

Exempel riktighet - loggar

1. Loggar som visar på systemhälsa i ett icke-kritiskt system kan tänkas ha krav på Riktighet 1.

2. Loggar som dokumenterar säkerhetshändelser i ett icke-kritiskt system eller applikation kan tänkas ha krav på Riktighet 2. En högre riktighetsaspekt är viktig för säkerhetshändelser. Det beror bland annat på att en utredning vid intrång eller missbruk försvåras om riktigheten i loggarna kan ifrågasättas.

3. Loggar som skapas för cyberfysiskt system eller IoT och som fyller en viktig funktion för att tillse att produkten beter sig som förväntat. Loggar för uppföljning av dricksvattenkvalitet eller mängden kemikalier i dricksvatten har höga krav på riktighet och kan troligtvis sättas som Riktighet 3.

4. Loggar där det finns höga krav på att kunna identifiera en fysisk person, exempelvis vid digitala underskrifter. Även i de fall det förekommer lagkrav på hög nivå av tillförlitlighet, exempelvis i hälso- och sjukvårdstillämpningar av system bör Riktighet 3 sättas.

Hur ska vi tänka - Tillgänglighet?

Krav på tillgänglighet av information varierar beroende på hur tidskritisk informationen är i förhållande till processen. I en livsuppehållande process som inte går att genomföra utan tillgång till information bör rimligtvis tillgänglighetsvärdet på informationen bestämmas högt.

Kravet på tillgänglighet kan ibland variera beroende på tidpunkt på året, månaden eller dagen. Tillgängligheten på ett lönesystem är rimligtvis mycket högre i slutet av månaden än i början av månaden.

Observera att tillgänglighetskravet för information i offentlig verksamhet i allmänhet är högt på grund av kravställning i Tryckfrihetsförordning gällande begäran av allmänna handlingar.

Exempel tillgänglighet - kontaktlista

1. En kontaktlista med kundrepresentanter i stadens förvaltningar och bolag är viktig för att informera om kommande förändringar eller utbildningar men har ingen avgörande påverkan om den är otillgänglig under en längre period. Kan sannolikt bedömas till Tillgänglighet 1.

2. Kontaktlistan från punkt 1 kan få en viktigare roll i samband med kommunikation av akuta förändringar eller incidenter i ett systemstöd eller tjänst. Verksamheterna kan behöva lägga om sin verksamhet eller senarelägga vissa åtgärder och kan behöva kontaktas skyndsamt. En kontaktlista kan i det här fallet sannolikt bedömas till Tillgänglighet 2.

3. Om kontaktlistan gäller ett samhällskritiskt system eller tjänst, eller en tjänst/system som är en del av en samhällsviktig tjänst: I de fall en tjänst utgör stöd för hälso- och sjukvård, akuta ärenden inom socialtjänsten eller liknande samhällsbärande tjänster som ger stora konsekvenser är det viktigt att inte bara informationen i tjänsten har en hög grad av tillgänglighet utan att relevanta personer kan kontaktas i samband med störning i tjänsten eller systemet. Om kontaktlistan inte finns tillgänglig kan den samhällsviktiga eller samhällskritiska tjänsten inte bli informerad inom rimliga tidsramar för att påbörja sitt kontinuitetsarbete. Kontaktlista för samhällskritiska eller samhällsviktiga tjänster kan sannolikt bedömas till Tillgänglighet 3.

Brist i konfidentialitet, riktighet och tillgänglighet kan också värderas utifrån vilka konsekvenser de får för följande konsekvenskategorier:

- Verksamhet
- Samhälle
- Individ
- Ekonomi
- Varumärke/förtroende

#ID	Aktivitet	Informationsmängd	K	R	T
Instruktion	*Aktivitet i processkartan*	*T.ex. faktura, beslut, logg*			
#0001	Identifiera incident	Incidentanmälan	3	2	3
#0002	Registrera och prioritera incident	Incidentärende	3	2	3
#0003	Registrera och prioritera incident	Rapport	3	2	3
#0004	Trolig major incident?	Beslut	1	2	1
#0005	Trolig PU-incident	Beslut	1	2	1
#0006	Felsöka incident	Felsökningsprotokoll	2	2	1
#0007	Lösa incident	Kunskapsartiklar	1	2	1
#0008	Löst incident	Meddelande	1	1	1

Exempel: Informationsklassa informationsmängderna i incidentprocessen

Gruppen bedömer att incidenter initialt kan vara mycket känsligt både när det gäller konfidentialitet och tillgänglighet innan det avgjorts om incidenten är en major incident och/eller en personuppgiftsincident.

När det gäller tillgänglighet bedöms informationsmängden(?) *inkommande anmälningar* som kritiska eftersom frånvaron av tillgänglighet kan leda till att verksamheten inte får reda på allvarliga incidenter.

När det gäller konfidentialitet bedöms informationsmängden(?) kunskapsartiklar inte som känsliga eftersom det finns en rutin som uppger att känslig information inte ska läggas där. Tillgänglighetsaspekten berörs men gruppen beslutar att kunskapsartiklarna främst är ett hjälpmedel för att lösa incidenter snabbt och att kunskapen finns hos någon i gruppen även vid avsaknad av kunskapsartiklar.

En löst incident är i normalfallet inte längre känslig ur ett konfidentialitets, riktighets eller tillgänglighetsperspektiv.

Identifiera informationsbärare

För varje informationsmängd ska en eller flera informationsbärare identifieras. En informationsbärare är det medium som informationen överförs med eller behandlas och lagras på. Vanligen är detta en applikation eller lagringsyta, men det kan också vara muntligt, via telefon eller på annat sätt. I vissa fall finns det flera informationsbärare för samma informationsmängd, exempelvis kan en anmälan inkomma via brev, e-post, telefonsamtal eller muntligen.

Informationsmängden får genom detta ett antal beroenden till en eller flera informationsbärare. Informationsklassningen av informationsmängderna är genom detta ett sätt att ställa informationssäkerhetskrav på tjänster, applikationer och infrastruktur.

För tekniska informationsbärare behöver beroende inte anges på lägre nivå än applikationsnivå. Det är alltså inte nödvändigt att ange de tekniska komponenter en applikation stödjer sig på så som databaser, nätverkskomponenter, serverhallar etc. I de fall den tekniska informationsbäraren är något annat än applikation ska detta dock anges. Det kan handla om USB-minnen, lagringsytor etc.

Exempel: Identifiera informationsbärare

Deltagarna identifierar att inkommande anmälningar om misstänkt incident har beroenden till informationsbärarna

- mailsystemet,
- telefonin
- muntliga kontakter och
- ServiceNow.

Detta ställer i sin tur krav på tjänsterna Microsoft365, telefonileveransen och på incidentgruppen själva.

#ID	Aktivitet	Informationsmängd	Informationsbärare
Instruktion	Aktivitet i processkartan	T.ex. faktura, beslut, logg	T.ex. Exchange, Treserva, telefonisystem, Sharepoint
#0001	Identifiera incident	Incidentanmälan	Telefonisystem, Outlook, Logpoint, muntlig kontakt
#0002	Registrera och prioritera incident	Incidentärende	ServiceNow, ServiceNow Inc
#0003	Registrera och prioritera incident	Rapport	ServiceNow
#0004	Trolig major incident?	Beslut	ServiceNow
#0005	Trolig PU-incident	Beslut	ServiceNow
#0006	Felsöka incident	Felsökningsprotokoll	ServiceNow, Outlook
#0007	Lösa incident	Kunskapsartiklar	ServiceNow, KB-databasen
#0008	Löst incident	Meddelande	Telefonisystem, Outlook

Identifiera leverantörer

För varje enskild informationsbärare ska en leverantör identifieras. Syfte är att veta vem kraven på säkerhetsåtgärder ska riktas mot. I de flesta fall är leverantören Intraservice eller en privat leverantör av IT-lösningar, men i vissa fall kan leverantören vara en annan nämnd eller en statlig myndighet. Det är alltid närmsta nivå i leverantörsledet som ska anges, i de flesta fall en tjänst på Intraservice. Om oklarhet råder anges endast Intraservice som leverantör.

Tillhandahålls lösningen on-prem (installerat i Intraservices miljö) faller en större del av säkerhetsåtgärderna på Intraservice förvaltning än om lösningen

levereras som en SaaS-lösning (installation driftad och omhändertagen av leverantör).

Exempel: Identifiera leverantörer

Deltagarna identifierar att leverantör av

- *telefonitjänster* är Nämnden för Demokrati och medborgarservice,
- *mail och Microsoft365* är tjänsten Office 365
- *Logpoint* är tjänsten IT-säkerhet
- *ServiceNow* är Intraservices förvaltning

#ID	Aktivitet	Informationsmängd	Leverantör
Instruktion	Aktivitet i processkartan	T.ex. faktura, beslut, logg	
#0001	Identifiera incident	Incidentanmälan	Demokrati och medborgarservice, Office 365, IT-säkerhet, Intraservice
#0002	Registrera och prioritera incident	Incidentärende	Intraservice
#0003	Registrera och prioritera incident	Rapport	Intraservice
#0004	Trolig major incident?	Beslut	Intraservice
#0005	Trolig PU-incident	Beslut	Intraservice
#0006	Felsöka incident	Felsökningsprotokoll	Intraservice, Office 365
#0007	Lösa incident	Kunskapsartiklar	Intraservice
#0008	Löst incident	Meddelande	Demokrati och medborgarservice, Office 365

Fastställ informationsklassning

Informationsägaren ska efter genomförd workshop fastställa informationsklassningen. Fastställande är ett delegationsbeslut, använd mallen i bilaga 6. När informationsklassningen är fastställd betraktas den som klar.

Fastställ tidpunkt för aktualisering

I samband med att informationsägaren fastställer informationsklassningen ska en tidpunkt för aktualisering fastställas. Informationsklassning ska aktualiseras minst vart fjärde år. Detta bör noteras i verksamhetens förvaltningsplan eller liknande. Vid en aktualisering går deltagarna igenom tidigare informationsklassning och identifierar om några förändringar har skett.

Efter workshop

Bevara informationsklassningen

Efter fastställning av informationsklassning ska excelarket med klassningen diarieföras i Intraservices diarie under det diarienummer som upprättades i början av processen. Om ytterligare informationssäkerhetsaktiviteter ska genomföras i närtid kan dessa under samma diarienummer. Det är exempelvis vanligt att man genomför riskanalys, lämplighetsbedömningar eller liknande i samband med informationsklassning.

Följande handlingar ska diarieföras

- Excelfil där ni genomfört informationsklassningen
- En bild över processen som informationsklassats
- Delegationsbeslut i enlighet med mall i bilaga 6

När informationsklassningen och närliggande aktiviteter är genomförda och registrerade i diariet kan ärendet avslutas.

Informera berörda

Den färdigställda informationsklassningen för processen delges de systemansvariga (tex systemägare och systemförvaltare) för de system som processen använder sig av genom att diarienumret översänds via mail.

Syftet med denna rutin

Rutinen ska användas som ett praktiskt hjälpmedel för förvaltningen i arbete med att genomföra informationsklassningar, i enlighet med Nämnden för Intraservices anvisning för informationsklassning. Rutinen används som en ‘steg-för-steg’-guide för informationsägaren och informationsklassningsansvarig i syfte att producera en kvalitativ och standardiserad informationsklassning.

Vem omfattas av rutinen

Denna rutin gäller tills vidare för samtliga medarbetare.

Koppling till andra styrande dokument

Göteborgs stads riktlinjer för informationssäkerhet

Göteborgs Stads riktlinje för styrning, samordning och finansiering av digital utveckling och förvaltning

Nämnden för Intraservices anvisning för informationsklassning.

Nämnden för Intraservices anvisning för roller, ansvar och mandat kopplat till informationssäkerhet

Anvisning för ansvar och roller i informationssäkerhetsarbetet

Stödjande dokument

Bilaga 1 - Lista med vanligt förekommande sekretessregleringar i Intraservices verksamhet

Sekretess regleras i offentlighets- och sekretesslagen (2009:400). Listan är inte uttömmande. Tänk på att kunders verksamheter kan omfattas av andra sekretessregleringar än de som gäller på Intraservice. I vissa fall kan sekretess överföras mellan myndigheter, vilket innebär att även Intraservice kan omfattas av andra myndigheters sekretessbestämmelser när vi t.ex. övertar uppgifter från andra myndigheter, en sådan överförd sekretess framgår också av bestämmelserna i relevant kapitel i offentlighets- och sekretesslagen.

För frågor eller osäkerhet gällande offentlighets- och sekretesslagen, kontakta jurist på Intraservice.

Bilagan är tänkt att vara ett stöd för informationsklassning och ska inte användas i samband med sekretessprövning vid utlämning av uppgifter eller handlingar.

18 kap. 3 § - Myndigheter som biträder åklagarmyndigheter m. fl

Uppgifter som Intraservice bistår Åklagarmyndigheten, Polisen, Säkerhetspolisen etc. kan vara sekretessreglerade om uppgifterna hänför sig till en förundersökning i brottmål. Uppgifter av det här slaget kan exempelvis omfatta loggar, e-post, diagnostik mm som polisen begär ut från Intraservice i samband med en förundersökning.

Sådana uppgifterna kan omfattas av sekretess redan innan någon formell begäran från ovan angivna myndigheter inkommit, om verksamheten har goda skäl att anta att materialet kommer begäras inom kort. Det kan exempelvis vara i en situation när Intraservice har gjort en anmälan om brott och förväntar sig att få begäran om underlag från Polisen.

18 kap. 8 § - Säkerhets- eller bevakningsåtgärd

Uppgifter gällande säkerhets- eller bevakningsåtgärd kan omfattas av sekretess om det kan antas att syftet med åtgärden motverkas vid en utlämning. Sekretessregleringen är uppdelad i sju punkter varav tre av dessa kan vara aktuella för verksamheter inom Intraservice:

- Byggnader eller andra anläggningar, lokaler eller inventarier:
  Ritningar över larmsystem, tjänstgöringslistor för bevakningspersonal, kabeldragningar. Även listor över kritiska tekniska inventarier, brännvidd på övervakningskameror etc.
- Telekommunikation eller system för automatiserad behandling av information:
  Detaljerade säkerhetsåtgärder kopplade till tekniska system, exempelvis loggningsverktyg, portöppningar, radiofrekvenser, säkerhetsloggning, autentisering, behörighetsgrupper, konfiguration av brandvägg etc. Övergripande beskrivningar av program och komponenter bör i normalfallet falla utanför sekretessregleringen med undantag för programvara som har kända sårbarheter.
- Behörighet att få tillgång till upptagning för automatiserad behandling av information:
  Gäller behörighetskoder, lösenord, system för behörighetstilldelning eller certifikat som inte är allmänt tillgängliga.

18 kap. 9 § - Chiffer, kod, m.m.

Uppgifter om krypteringsnycklar, acesstokens, nyckellängder, certifikat och metoder för att generera krypteringsnycklar m.m. omfattas av sekretess i de fall syftet med åtgärden är att skydda sekretessreglerade uppgifter eller kontrollera om data i allmänhet har förvanskats.

Regleringen skyddar även lösenord, pin-koder m.m.

18 kap. 13 § - Risk- och sårbarhetsanalyser m.m.

Uppgifter i risk- och sårbarhetsanalyser kan hemlighållas om det kan antas att uppgifterna skulle kunna utnyttjas i syfte att förhindra Intraservice eller någon annan offentlig verksamhet att förebygga kriser eller incidenter. Även uppgifter som gäller planering eller förberedelser inför kriser eller incidenter kan hemlighållas, exempelvis uppgifter i kontinuitetshanterings- eller återställningsplaner.

Om uppgifterna hänför sig till planering, risk- och sårbarhetsanalyser eller förberedelser inför höjd beredskap gäller istället 15 kap. 2 § Försvarssekretess.

19 kap. 1 § - Affärs- och driftsförhållanden

Uppgifter gällande affärsmässiga överväganden eller förhållanden där Intraservice agerar på en konkurrensutsatt marknad omfattas av sekretess om uppgifterna kan gynna en konkurrent till Intraservice.

Uppgifter kan omfatta beräkningskalkyler, undersökningar, statistik, prislistor, cv:n osv. Regleringen borde främst gälla för de tjänster som inte är en del av det obligatoriska basutbudet och där förvaltningar och bolag har möjlighet att välja en annan leverantör än Intraservice.

Regleringen ger även stöd för att hemlighålla unik källkod som är framtagen av Intraservice. Syftet med källkoden måste dock vara att tillhandahålla en tjänst för Intraservices kunder.

I 19 kap. 2 § finns motsvarande skydd för uppgifter Intraservice får ta del av för en annan myndighets räkning, så kallad överförd sekretess.

19 kap. 3 § - Upphandling m.m.

Underlag till upphandlingar eller annan typ av förvärvs- eller anförskaffningsverksamhet i form av exempelvis kostnadskalkyler, förutsättningar, kravställningar m.m. omfattas av sekretess i den mån Intraservice eller annan offentlig verksamhet kan lida ekonomisk skada vid ett röjande. Sekretessen gäller oftast inte längre än till dess att tilldelningsbeslut fastställts.

Regleringen omfattar även uppgifter av mer långsiktig karaktär, så som detaljerade upphandlingsbudgetar, detaljerade strategier för inköp om det allmänna skulle kunna lida ekonomisk skada om uppgifterna röjs.

Sekretess gäller också för anbud till dess att tilldelningsbeslut fattats.

21 kap. 1 § - Hälsa och sexualliv

Sekretess gäller för uppgifter om enskilds hälsa eller sexualliv, såsom uppgifter om sjukdomar, missbruk, sexuell läggning, könsbyte, sexualbrott eller liknande. Sekretessen gäller i all offentlig verksamhet och är en säkerhetsventil om övriga preciserade sekretessregleringar av någon anledning inte skulle gälla.

Sekretess enligt 21 kap. 1 § har ett ovanligt skaderekvisit, vilket innebär att den enskilde eller någon närstående till denne måste lida betydande men om uppgiften blir allmän. Det ska med andra ord vara mycket graverande uppgifter om en enskild person för att sekretessregleringen ska kunna användas. Sekretessen gäller inte för uppgift som ingår i ett beslut.

För Intraservices del är regleringen främst aktuell i egenskap av tjänsteleverantör för andra eller för driften av stadengemensamma persondatabaser.

21 kap. 3 § - Adress, telefon, m.m

Uppgifter om enskilds lokalisering kan hemlighållas i fall där det finns särskild anledning att anta att personen eller dennes närstående kommer att

utsättas för våld, hot eller lida allvarligt men om uppgiften kommer ut. Uppgifter som kan hemlighållas är adress, arbetsplats, föreningsmedlemskap eller liknande som möjliggör för annan person att lokalisera den skyddade personen.

Även uppgifter som möjliggör för någon att kontakta den skyddade personen bör hemlighållas, så som IP-adresser, e-post eller telefonnummer.

För Intraservices del är regleringen främst aktuell i egenskap av tjänsteleverantör för andra eller för driften av stadengemensamma persondatabaser.

22 kap 1 § - Folkbokföring och annan liknande registrering av befolkningen m.m.

Sekretess gäller för uppgift om en enskilds personliga förhållanden om det av särskild anledning kan antas att den enskilde eller någon närstående till denne lider men av att uppgiften röjs. Denna reglering är det som hos Skatteverket kallas ”sekretessmarkering”. Det är alltså Skatteverket som tillför en sekretessmarkering på den enskilda personuppgiften i folkbokföringsregistret. Sekretessmarkeringen ärvs sedan av funktioner som hämtar information från exempelvis Navet. För sekretessmarkering gäller att Skatteverket bedömer att det kan finnas särskild anledning att anta att en person eller någon närstående till denne riskerar att lida men om uppgifter om personen lämnas ut.

Att tänka på:

- Det vanligast förekommande uppgifterna som är skyddsvärda gäller vart personen befinner sig fysiskt. Det gäller dels uppgifter från folkbokföringen, dels ytterligare uppgifter som arbetsplats, föreningsengagemang. Även indirekta uppgifter som kan lokaliserade personen är viktiga att tänka på. Subdomänen intraservice.goteborg.se i en e-postadress indikerar exempelvis vart personen befinner sig minst två dagar i veckan.
- Även uppgifter som inte direkt kan koppla personen till en fysisk plats kan vara skyddsvärda, så som telefonnummer, privata e-postadresser eller alias på sociala nätverk. Dessa uppgifter kan användas för att trakassera en skyddsvärd person.

Sekretessen är sannolikt främst aktuellt i Intraservice centrala HR-, identitets- och kommunikationssystem.

22 kap. 2 § - Skyddad folkbokföring och fingerade personuppgifter

En starkare form av skydd än vad 22 kap 1 § medger. Uppgifter om en individs folkbokföringsadress överförs inte från Skatteverket i de fall beslut om skyddad folkbokföring har fattas. Det kan ändå finnas anledning att uppmärksamma sekretessen eftersom Intraservice kan ha fått del av folkbokföringsuppgifter gällande individen på annat sätt, exempelvis via anställning.

Rekommendationerna från 22 kap. 1 § gäller också för 22 kap. 2 §.

24 kap. 8 § - Statistik

Sekretess gäller för uppgifter som avser en enskilds personliga eller ekonomiska förhållanden och som kan hänföras till den enskilde. Sekretessen gäller även uppgiftsinsamling till förmån för annan myndighets statistikproduktion. För Intraservice gäller detta främst uppgifter förvaltningen är skyldiga att lämna till Arbetsmiljöverket och SCB gällande exempelvis arbetsskada eller lön.

31 kap. 16 § - Affärsförbindelse med myndighet

Uppgifter om ett företags affärs- eller driftsförhållanden kan omfattas av sekretess om röjande av uppgift skulle skada företaget ekonomiskt. Förutsättningen för att sekretessbelägga uppgifter om företag är att företaget och Intraservice har ingått någon form av affärsförbindelse, exempelvis genom att företaget har lämnat anbud på ett förfrågningsunderlag.

Vanligtvis ställer upphandlande förvaltning krav på att företaget i sina anbud ska inkomma med redogörelse av vad i deras anbud dom anser vara känsligt. Det är fortfarande Intraservice och inte företaget som gör bedömning om hemlighållande. Uppgifter som i och för sig skulle kunna skada företaget ekonomiskt men som beror på företagets underlåtenhet att följa avtal, exempelvis brister vid revision etc. omfattas vanligtvis inte av regleringen.

Uppgifter i CV:n, detaljerade prislistor, unika affärsmodeller, kundlistor är ofta känsliga och kan hemlighållas med stöd av regleringen.

Avseende villkor i ett avtal är huvudregeln att sekretess enligt denna bestämmelse föreligger längst i två år, avseende kommunal affärsverksamhet kan bestämmelsen som längst tillämpas i fem år från det att avtalet slöts.

39 kap. 1 § - Personalsocial verksamhet

Sekretess gäller för uppgifter om individers personliga förhållanden i personalsocial verksamhet så som psykologisk undersökning, behandlingar,

social rådgivning m.m. Regleringen täcker även en anställds samtal med chef som sker av ovanstående anledning.

Enligt 39 kap. 5 § gäller sekretess enligt 39 kap. 1-4 §§ även hos myndighet som har som uppgift att bedriva personaladministrativ verksamhet för andra myndigheter. Sekretessen gäller således även för det arbete Intraservice utför som tjänst för andra förvaltningar och bolag i staden.

39 kap. 2 § - Personaladministrativ verksamhet i övrigt

Sekretess gäller för uppgift om anställds hälsotillstånd. Främst berör detta HR-processer och handlingar så som personalakter eller handlingar i särskilda systemstöd för hantering av uppgifter om anställda.

Sekretess gäller även för personliga förhållanden i övrigt för uppgifter i ärenden om omplacering eller pensionering av en anställd. Notera att sekretess inte gäller för ärenden om disciplinansvar, exempelvis avsked, utfärdande av varning m.m.

Enligt 39 kap. 5 § gäller sekretess enligt 39 kap. 1-4 §§ även hos myndighet som har som uppgift att bedriva personaladministrativ verksamhet för andra myndigheter. Sekretessen gäller således även för det arbete Intraservice utför som tjänst för andra förvaltningar och bolag i staden.

39 kap. 3 § - Adresser, telefonnummer, m.m.

Sekretess gäller i all personaladministrativ verksamhet för uppgifter om anställds personliga förhållanden om det kan antas att den anställda eller någon närstående till den anställda kan komma att utsättas för hot eller våld om uppgiften röjs.

Sekretessen gäller i övrigt för samtliga privata kontaktuppgifter för alla anställda förvaltningen är i besittning av. Detta inkluderar bostadsadress, privat telefonnummer eller privat e-postadress och andra jämförbara elektroniska kontaktvägar. Även fotografiska bilder föreställande anställda som tagits fram för internt bruk omfattas.

Enligt 39 kap. 5 § gäller sekretess enligt 39 kap. 1-4 §§ även hos myndighet som har som uppgift att bedriva personaladministrativ verksamhet för andra myndigheter. Sekretessen gäller således även för det arbete Intraservice utför som tjänst för andra förvaltningar och bolag i staden.

39 kap. 5 a § - Urvalstester

Sekretess gäller för urvalstester som genomförs som grund för anställning. Regleringen omfattar exempelvis personlighets- och logiktester om det är

möjligt att identifiera personen som genomfört testet. Urvalstester som genomförs på redan anställd personal omfattas inte av regleringen.

40 kap. 5 § - Teknisk bearbetning och lagring

Sekretess gäller för utförare av teknisk bearbetning och lagring som avser uppgifter om enskilds personliga eller ekonomiska förhållanden. Sekretessen är aktuell för Intraservices verksamhet som består i drift av IT-tekniska tjänster så som databasdrift, applikationsdrift, nätverkstjänster m.m. som Intraservice utför åt andra.

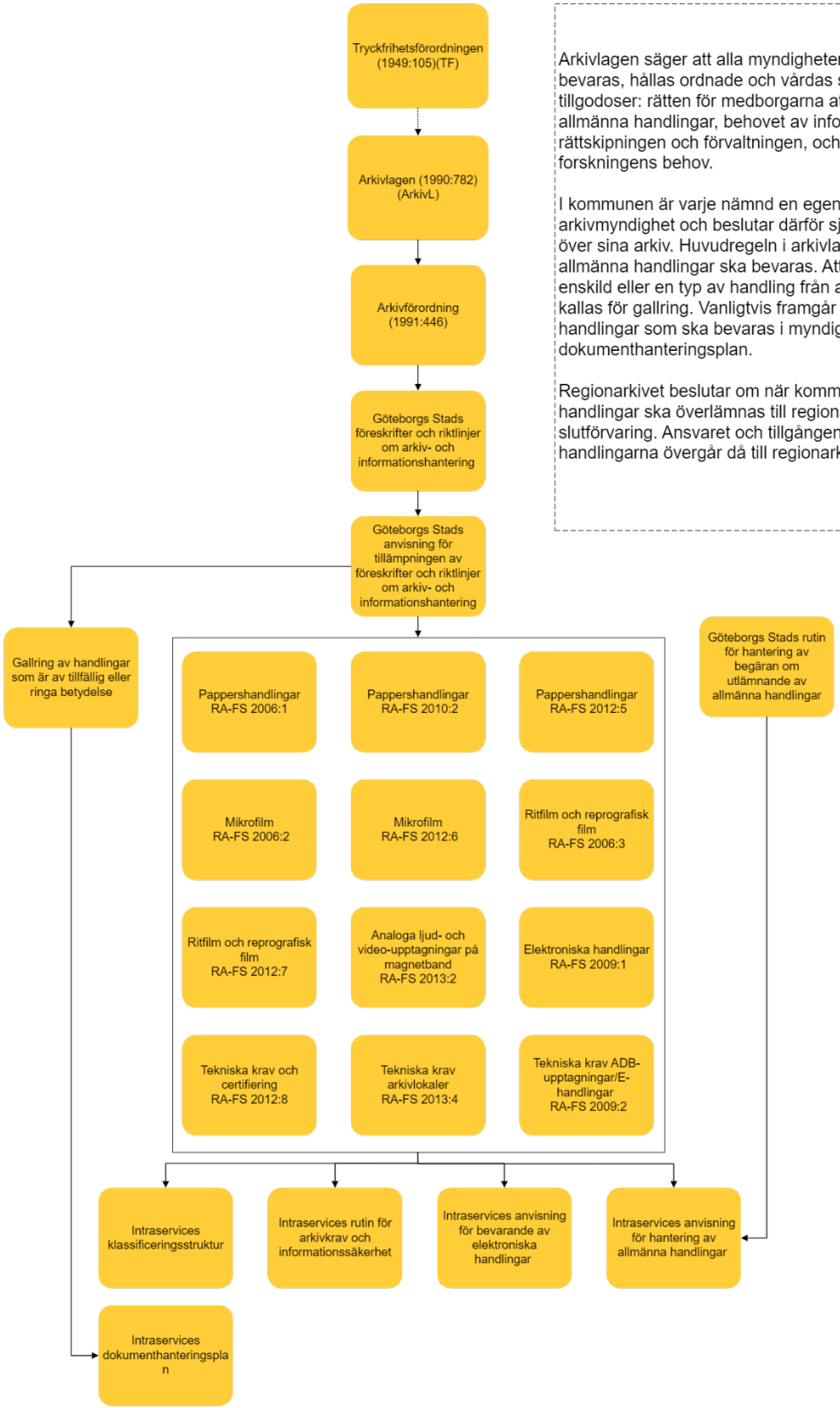
Förutsättningen för att regleringen ska vara aktuell är att Intraservice endast tekniskt bearbetar och/eller lagrar uppgifterna. Definitionen av begreppet teknisk bearbetning och lagring har ansetts sträcka sig till support, utveckling av produkt, IT-säkerhetsrelaterade tjänster etc. Om Intraservice som förvaltning utför någon annan form av bearbetning så som handläggning av ärenden, rådgivning eller dylikt i samband med driften omfattas uppgifterna inte av sekretess enligt regleringen.

Bilaga 2 – Vanligt förekommande lagstiftning

Nedan listas vanligt förekommande lagstiftning och styrdokument som kan ha påverkan på hur information får hanteras. Lagstiftning som påverkar en verksamhet eller tillvägagångssätt men inte ställer krav på hur information eller informationsbärare får hanteras är inte av intresse för en informationsklassning och listas därför inte. Listan är inte uttömmande.

I många fall finns det underliggande förordningar och riktlinjer kopplade till lagstiftning. Förordningar och riktlinjer specificerar hur en viss lagstiftning ska verkställas och ligger ofta på en högre detaljrikedom än lagstiftningen i sig.

Arkivlagen



Arkivlagen säger att alla myndigheters arkiv skall bevaras, hållas ordnade och vårdas så att de tillgodoser: rätten för medborgarna att ta del av allmänna handlingar, behovet av information för rättskipningen och förvaltningen, och forskningens behov.

I kommunen är varje nämnd en egen arkivmyndighet och beslutar därför självständigt över sina arkiv. Huvudregeln i arkivlagen är att allmänna handlingar ska bevaras. Att undanta en enskild eller en typ av handling från att bevaras kallas för gallring. Vanligtvis framgår vilka handlingar som ska bevaras i myndighetens dokumenthanteringsplan.

Regionarkivet beslutar om när kommunens handlingar ska överlämnas till regionarkivet för slutförvaring. Ansvaret och tillgången till handlingarna övergår då till regionarkivet.

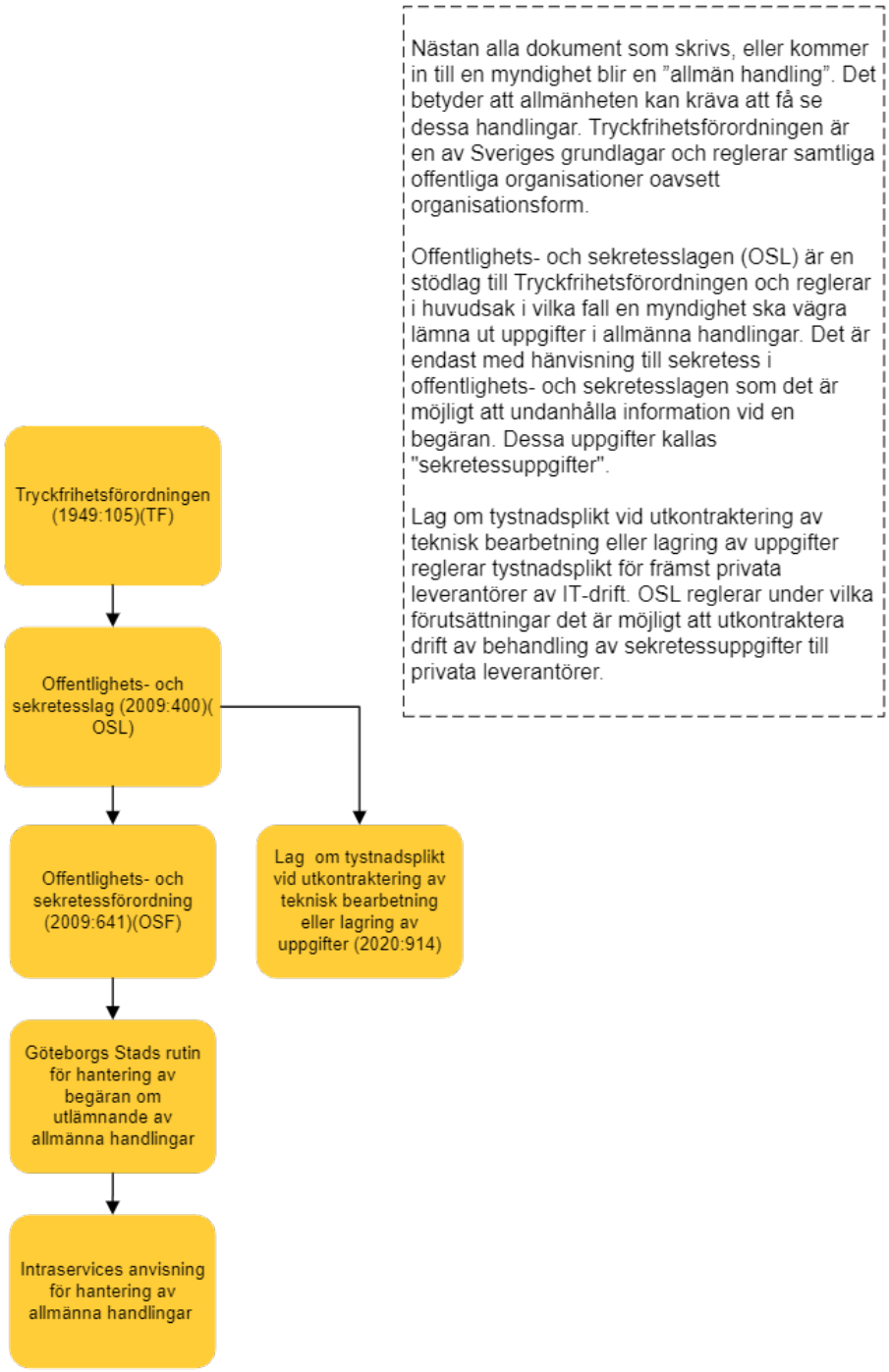
Lag om skydd för geografisk information

Enligt lagen om skydd för geografisk information krävs tillstånd för spridning av landgeografisk information som inhämtats från luftfartyg. Med detta menas flygbilder och liknande registreringar som film, laserskannade data, värmekameradata, radardata etc. Syftet med tillståndskravet är att i möjligaste mån undvika skada för totalförsvaret.

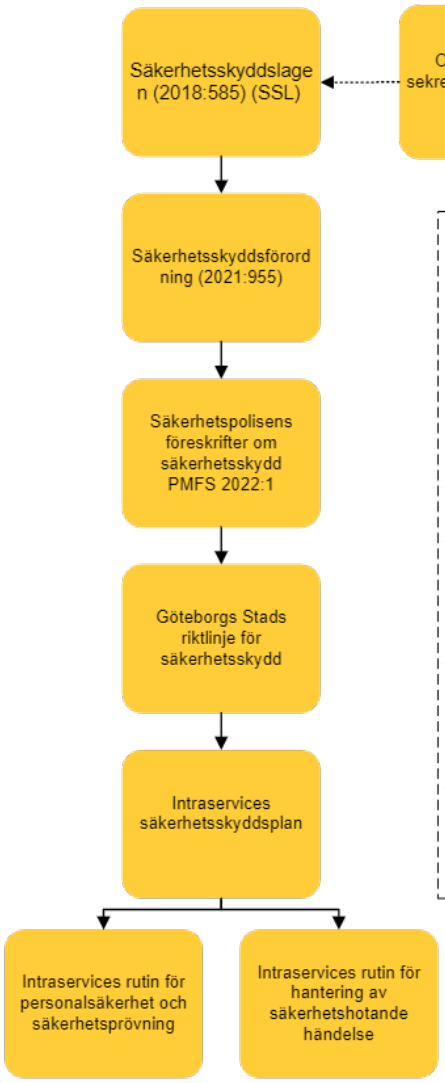
Det är också förbjudet att sprida en sammanställning av geografisk information om förhållanden i ett visst vattenområde eller en viss sträcka av ett vattenområde som avser Sveriges sjöterritorium, med undantag av insjöar, vattendrag och kanaler, eller över andra delar av svenskt territorium, om informationen har inhämtats från luftfartyg genom fotografering eller liknande registrering.

Tillstånd för spridning av uppgifter utfärdas av Lantmäteriet respektive Sjöfartsverket. Lagen ger undantag för information inhämtad med hjälp av satellit.

Tryckfrihetsförordningen och offentlighets- och sekretesslagen



Säkerhetsskyddslagen



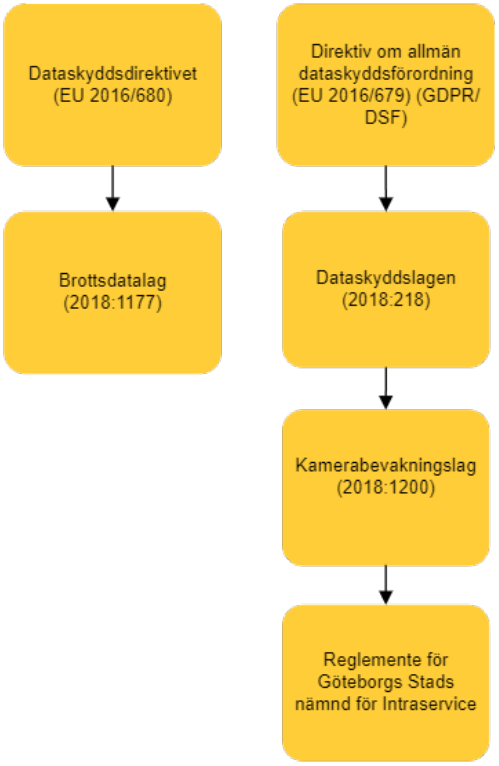
Säkerhetsskydd handlar om att skydda den information och de verksamheter som är av betydelse för Sveriges säkerhet mot spionerі, sabotage, terroristbrott och vissa andra hot.

Om vissa myndigheter och företag i Sverige utsätts för antagonistiska handlingar kan det orsaka allvarliga konsekvenser för Sveriges säkerhet. Det kan till exempel handla om verksamheter inom rättsväsendet, energi- eller vattenförsörjningen, telekommunikationer eller transportsektorn.

Dessa verksamheter kan i sitt uppdrag behöva hantera uppgifter som är av betydelse för Sveriges säkerhet. Om dessa uppgifter röjs, förstörs eller ändras kan det inverka på Sveriges säkerhet. Det är därför verksamheter som behöver ett särskilt skydd, säkerhetsskydd.

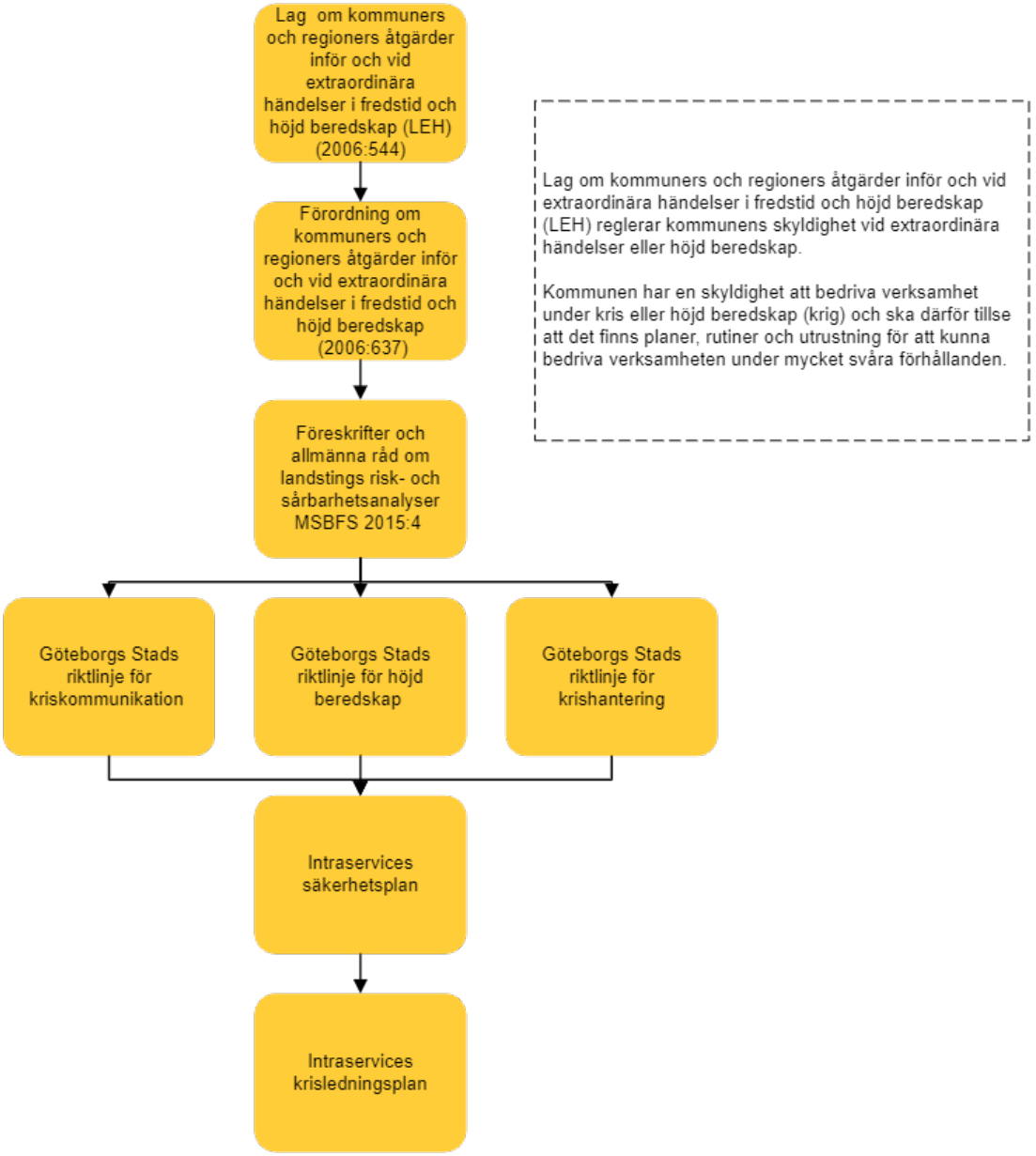
Offentlighets- och sekretesslagen reglerar förutsättningarna för vilka uppgifter som kan komma att omfattas av säkerhetsskyddslagstiftningen.

Dataskyddsförordningen/GDPR

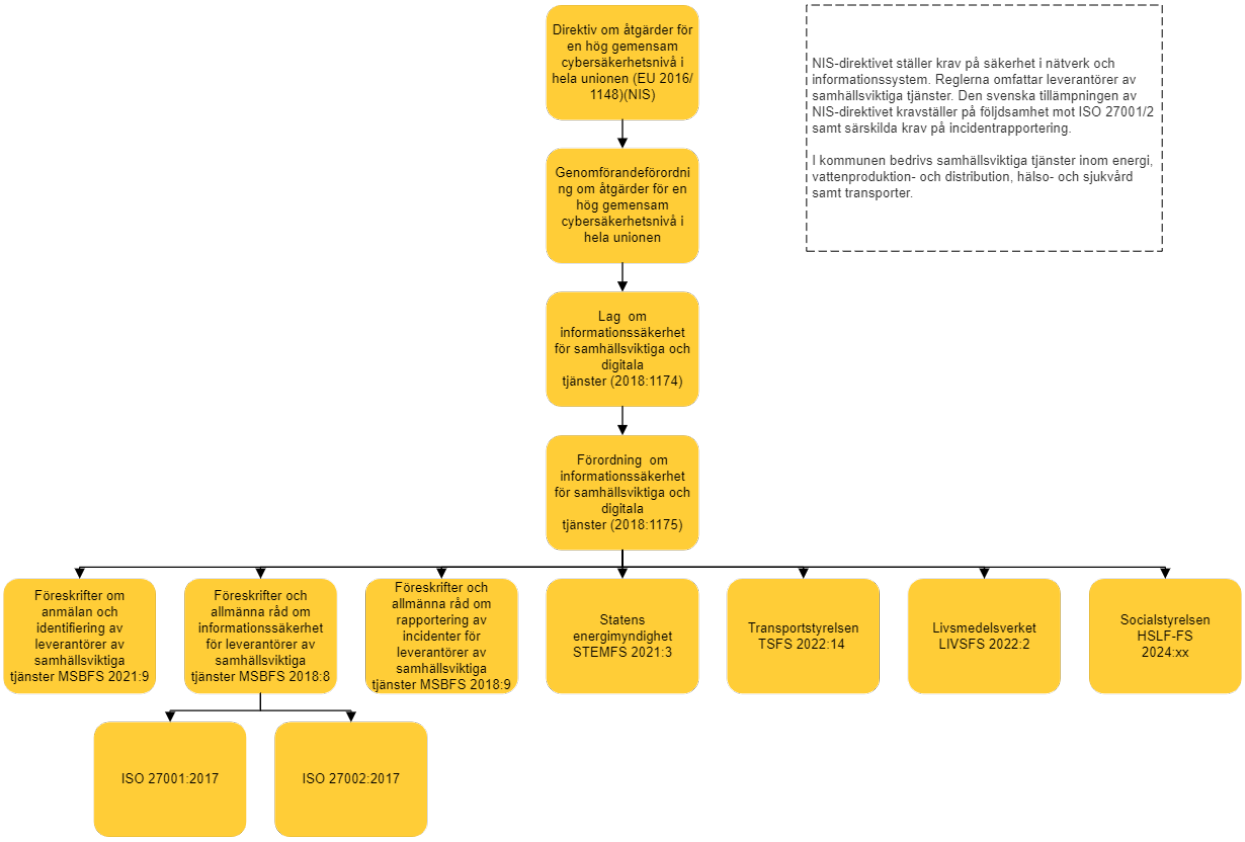


Dataskyddsförordningen reglerar hur personuppgifter får behandlas. Det finns olika saker att ta hänsyn till beroende på om personuppgifterna klassas som känsliga eller inte. Dataskyddsförordningens bestämmelser gäller oavsett i vilken form personuppgifter hanteras. Personuppgifter kan även vara indirekta, det vill säga uppgifter som kan identifiera en fysisk person i ett andra led.

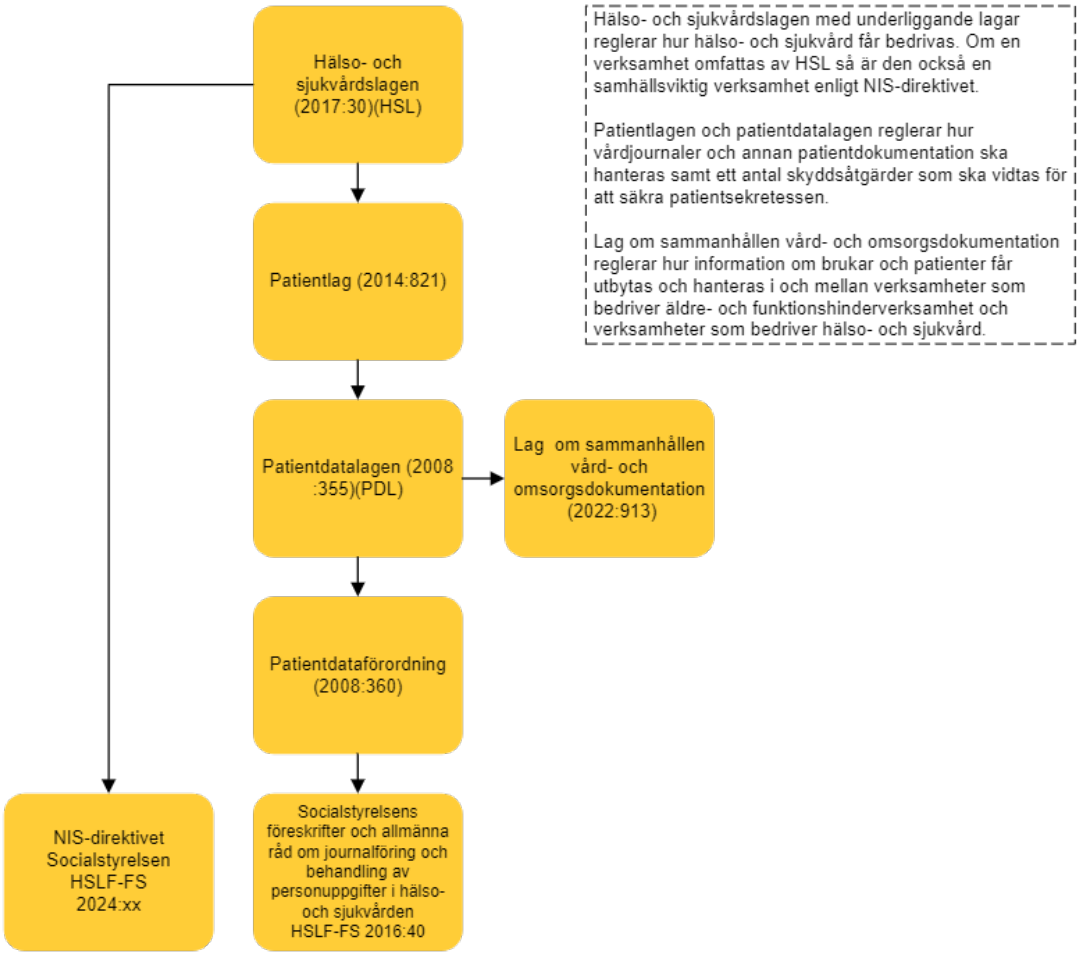
Lag om kommuners och regioners åtgärder inför och vid extraordinära händelser i fredstid och höjd beredskap



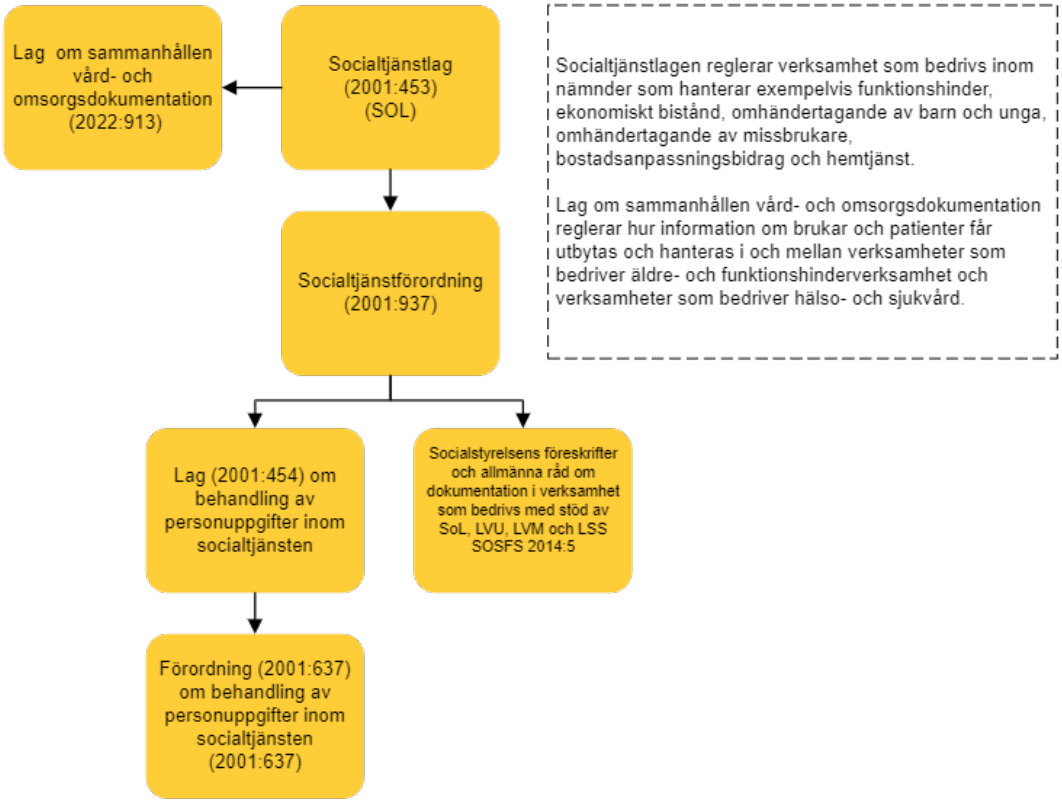
NIS-direktivet



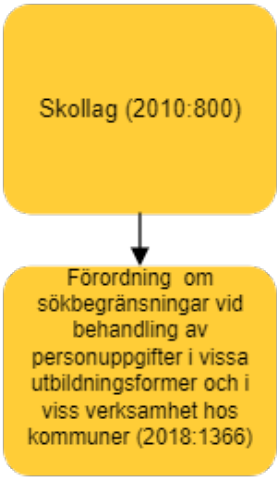
Hälso- och sjukvårdslagen



Socialtjänstlagen



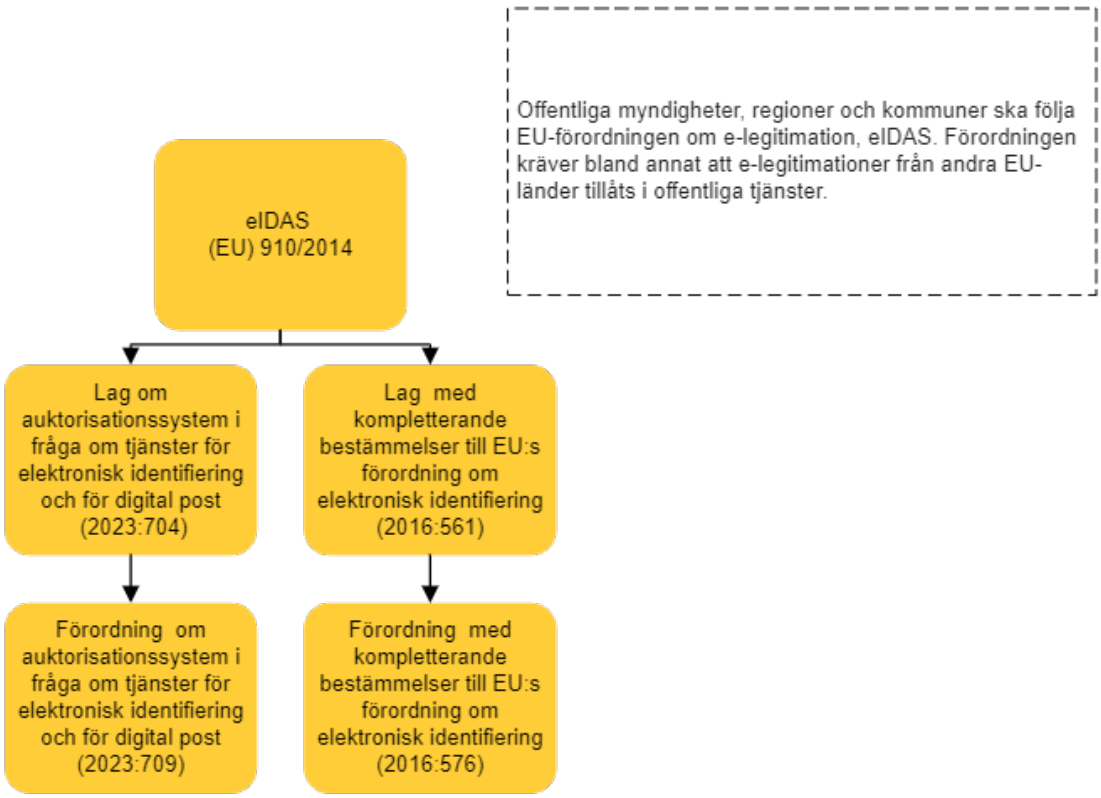
Skollagen



Skollagen reglerar vilka rättigheter och skyldigheter barn, elever och vårdnadshavare har. I lagen står också vilka krav som ställs på huvudmannen för verksamheten.

Skollagen reglerar utöver grundskola och gymnasieskola utbildningsverksamhet i förskola och vuxenutbildning.

eIDAS


Offentliga myndigheter, regioner och kommuner ska följa EU-förordningen om e-legitimation, eIDAS. Förordningen kräver bland annat att e-legitimationer från andra EU-länder tillåts i offentliga tjänster.
eIDAS
(EU) 910/2014
Lag om auktorisationssystem i fråga om tjänster för elektronisk identifiering och för digital post (2023:704)
Lag med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering (2016:561)
Förordning om auktorisationssystem i fråga om tjänster för elektronisk identifiering och för digital post (2023:709)
Förordning med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering (2016:576)

Bilaga 3 – Göteborgs stads klassificeringsmodell

	Konsekvensnivå	Konfidentialitet	Riktighet	Tillgänglighet
4	Sveriges Säkerhet Säkerhetsskydd	**K4** Information som omfattas av Säkerhetsskyddslagstiftningen *Särskild hantering - Riktlinje för säkerhetsskydd.*		
3	Allvarlig skada (hög skyddsnivå)	**K3** Viktig information som, om den tillgängliggörs, röjs eller sprids till obehöriga, kan medföra allvarliga konsekvenser för Göteborgs Stads verksamhet, tillgångar, annan organisation eller individer.	**R3** Viktig information som, om den ej är riktig och fullständig, kan medföra allvarliga konsekvenser för Göteborgs Stads verksamhet, tillgångar, annan organisation eller individer.	**T3** Viktig information som, om den ej är tillgänglig, kan medföra allvarliga konsekvenser för Göteborgs Stads verksamhet, tillgångar, annan organisation eller individer.
2	Betydande (utökad skyddsnivå)	**K2** Information som, om den tillgängliggörs, röjs eller sprids till obehöriga, kan medföra betydande negativ påverkan på Göteborgs Stads verksamhet, tillgångar, annan organisation eller individer	**R2** Information som, om den ej är riktig och fullständig, kan medföra betydande negativ påverkan på Göteborgs Stads verksamhet, tillgångar, annan organisation eller individer	**T2** Information som, om den ej är tillgänglig, kan medföra betydande negativ påverkan på Göteborgs Stads verksamhet, tillgångar, annan organisation eller individer.
1	Måttlig (grundläggande nivå)	**K1** "Intern" information som om den tillgängliggörs, röjs eller sprids till obehöriga kan medföra måttlig negativ påverkan på Göteborgs Stads verksamhet, tillgångar, annan organisation eller individer	**R1** Information som, om den ej är riktig och fullständig, kan medföra måttlig negativ påverkan på Göteborgs Stads verksamhet, tillgångar, annan organisation eller på individer	**T1** Information som, om den ej är tillgänglig, kan medföra måttlig negativ påverkan på Göteborgs Stads verksamhet, tillgångar, annan organisation eller individer
0	Försumbar skada (ingen skyddsnivå)	**K0** Information som, om den tillgängliggörs, röjs eller sprids till obehöriga, inte medför någon negativ skada för Göteborgs Stads verksamhet, tillgångar, annan organisation eller individer	**R0** Information där förlust av riktighet inte medför någon negativ skada för Göteborgs Stads verksamhet, tillgångar, annan organisation eller individer	**T0** Information där förlust av tillgänglighet inte medför någon negativ skada för Göteborgs Stads verksamhet, tillgångar, annan organisation eller individer

Bilaga 4 – Checklista

Informationsägare – innan workshop

- ☐ Besluta om genomförande av informationsklassning
- ☐ Utse informationsklassningsansvarig

Informationsklassningsansvarig – innan workshop

- ☐ Begär ärende
- ☐ Inhämta process
  - ☐ Inhämta etablerad verksamhetsprocess
  - ☐ Alternativt visualisera process
- ☐ Identifiera deltagare
  - ☐ Personer med erfarenhet av arbete i processen
  - ☐ Personer med erfarenhet av arbete med systemstöd i processen
  - ☐ Personer med kunskap om regleringar i processen
  - ☐ Kontakta dataskyddsombud
- ☐ Samla in underlag
  - ☐ Processkarta eller beskrivning
  - ☐ Lagar och styrdokument
  - ☐ Avtal
  - ☐ Tidigare genomförda informationsklassningar
- ☐ Ladda ner kopia av informationsklassningsmallen
  - ☐ Fyll i mallens förstasida
- ☐ Kalla till workshop

Informationsklassningsansvarig – genomförande av workshop

- ☐ Utbilda deltagare med hjälp av presentation (bilaga 5)
- ☐ Utred om processen omfattas av säkerhetsskydd
- ☐ Identifiera informationsmängder
- ☐ Identifiera reglering för informationsmängderna
- ☐ Identifiera sekretessreglerade uppgifter
- ☐ Identifiera personuppgifter
- ☐ Informationsklassa informationsmängderna
- ☐ Identifiera informationsbärare
- ☐ Identifiera leverantörer

Informationsägare – efter workshop

- ☐ Fastställ informationsklassning
- ☐ Fastställ tidpunkt för aktualisering av informationsklassning

Informationsklassningsansvarig – efter workshop

- ☐ Diarieför informationsklassning
  - ☐ Diarieför ifylld klassningsmall
  - ☐ Diarieför bild över den informationsklassade processen

- ☐ Diarieför delegationsbeslut om fastställd informationsklassning
- ☐ Kontakta registrator för anmälan till nämnd av delegationsbeslut

☐ Begär avslut av ärende

☐ Informera berörda om att informationsklassning är genomförd

Göteborgs Stad

Informationsklassning

Vad ska skyddas?

Göteborgs Stad

Information

Så att informationens behov av skydd för

- Konfidentialitet,
- Riktighet och
- Tillgänglighet

kan upprätthållas.

Vad är konfidentialitet, riktighet och tillgänglighet?

Konfidentialitet	att information inte tillgängliggörs eller avslöjas för obehöriga.
Riktighet	att informationen skyddas mot oönskad förändring, att information är korrekt och inte manipulerad eller förstörd.
Tillgänglighet	att information är tillgänglig och användbar när den behövs.

Hur skyddar vi informationen?

Göteborgs Stad

Med säkerhetsåtgärder

- Vi arbetar med informationssäkerhet på ett systematiskt och riskbaserat sätt, och
- Inför olika säkerhetsåtgärder som skyddar informationen utifrån dess värde.

Klassa information

Värdera information utifrån kommunens klassningsmodell för att

- Förstå informationens värde för kommunen,
- Hitta kritisk och känslig information och
- Få ett underlag inför att välja säkerhetsåtgärder.

Klassa information

Värderingen sker utifrån klassningsmodellens kriterier för:

Göteborgs stads klassningsmodell

Riktlinjer för informationssäkerhet

- Klassificeringsmodell med fem nivåer.
- Säkerhetsskydd är en egen nivå.
- Konsekvensnivåer utifrån fem konsekvenskategorier:
  - Verksamhet,
  - Samhälle,
  - Individ,
  - Ekonomi,
  - Varumärke.

	Konsekvensnivå	Konfidentialitet	Riktighet	Tillgänglighet
4	Sveriges Säkerhet Säkerhetsskydd	**K4** Information som omfattas av Säkerhetsskyddslagstiftningen *Särskild hantering - Riktlinje för säkerhetsskydd.*		
3	Allvarlig skada (hög skyddsnivå)	**K3** Viktig information som, om den tillgängliggörs, röjs eller sprids till obehöriga, kan medföra allvarliga konsekvenser för Göteborgs Stads verksamhet, tillgångar, annan organisation eller individer.	**R3** Viktig information som, om den ej är riktig och fullständig, kan medföra allvarliga konsekvenser för Göteborgs Stads verksamhet, tillgångar, annan organisation eller individer.	**T3** Viktig information som, om den ej är tillgänglig, kan medföra allvarliga konsekvenser för Göteborgs Stads verksamhet, tillgångar, annan organisation eller individer.
2	Betydande (utökad skyddsnivå)	**K2** Information som, om den tillgängliggörs, röjs eller sprids till obehöriga, kan medföra betydande negativ påverkan på Göteborgs Stads verksamhet, tillgångar, annan organisation eller individer	**R2** Information som, om den ej är riktig och fullständig, kan medföra betydande negativ påverkan på Göteborgs Stads verksamhet, tillgångar, annan organisation eller individer	**T2** Information som, om den ej är tillgänglig, kan medföra betydande negativ påverkan på Göteborgs Stads verksamhet, tillgångar, annan organisation eller individer.
1	Måttlig (grundläggande nivå)	**K1** "Intern" information som om den tillgängliggörs, röjs eller sprids till obehöriga kan medföra måttlig negativ påverkan på Göteborgs Stads verksamhet, tillgångar, annan organisation eller individer	**R1** Information som, om den ej är riktig och fullständig, kan medföra måttlig negativ påverkan på Göteborgs Stads verksamhet, tillgångar, annan organisation eller på individer	**T1** Information som, om den ej är tillgänglig, kan medföra måttlig negativ påverkan på Göteborgs Stads verksamhet, tillgångar, annan organisation eller individer
0	Försumbar skada (ingen skyddsnivå)	**K0** Information som, om den tillgängliggörs, röjs eller sprids till obehöriga, inte medför någon negativ skada för Göteborgs Stads verksamhet, tillgångar, annan organisation eller individer	**R0** Information där förlust av riktighet inte medför någon negativ skada för Göteborgs Stads verksamhet, tillgångar, annan organisation eller individer	**T0** Information där förlust av tillgänglighet inte medför någon negativ skada för Göteborgs Stads verksamhet, tillgångar, annan organisation eller individer

Genomförande

Klassningsprocessen

Det finns ett flertal metoder för att genomföra informationsklassning.

Intraservice har valt att basera klassningen på våra processer.

Följande steg behöver genomföras:

- Identifiera informationsmängder
- Identifiera regleringar
- Identifiera sekretessbelagda uppgifter
- Identifiera personuppgifter
- Klassa informationsmängderna
- Identifiera informationsbärare
- Identifiera leverantörer

Utvärdera om er process omfattas av säkerhetsskydd

- Säkerhetsskydd innebär att skydda den information och de verksamheter som är av betydelse för Sveriges säkerhet mot spionering, sabotage, terroristbrott och vissa andra hot.
- Om ni misstänker att processen omfattas av säkerhetsskydd ska klassningen avslutas och säkerhetsskyddsansvarig kontaktas.
- Det är mycket ovanligt att en process omfattas av säkerhetsskydd.

Vad är en informationsmängd?

En informationsmängd är en gruppering av information, vilken informationsbärare den behandlas med eller lagras på spelar ingen roll.

En informationsmängd kan överföras med hjälp av eller lagras på en informationsbärare.

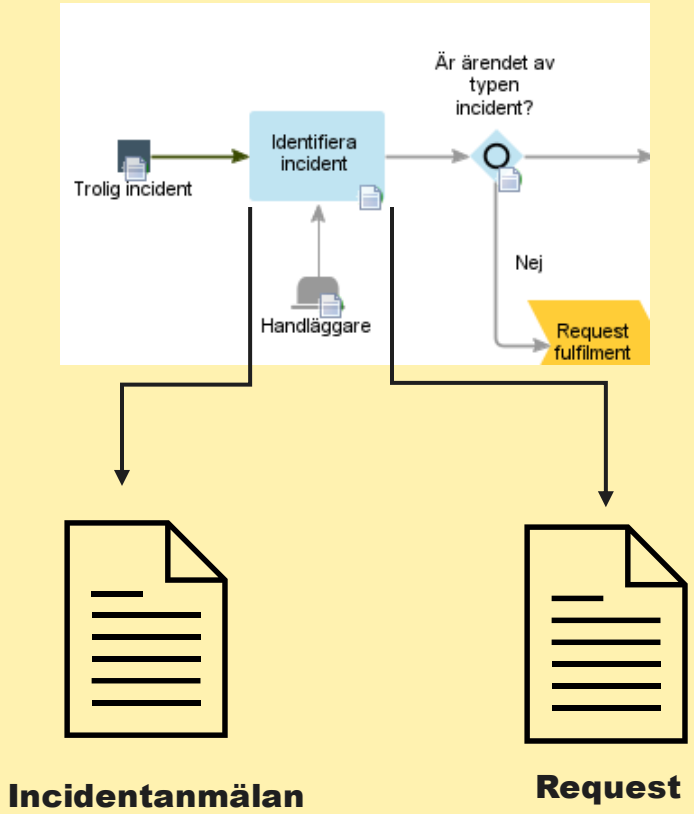
Exempel på informationsmängder

- *faktura,*
- *användare,*
- *temperatur,*
- *beslut om utlämning av handling,*
- *protokoll,*
- *anmälan,*
- *incidentanmälan,*
- *ärendekort.*

Identifiera informationsmängder

- Identifiera informationsmängder kopplade till processaktiviteterna.
- Det kan finnas flera informationsmängder kopplade till en processaktivitet. Det finns även processaktiviteter som inte har någon informationsmängd kopplad till sig.

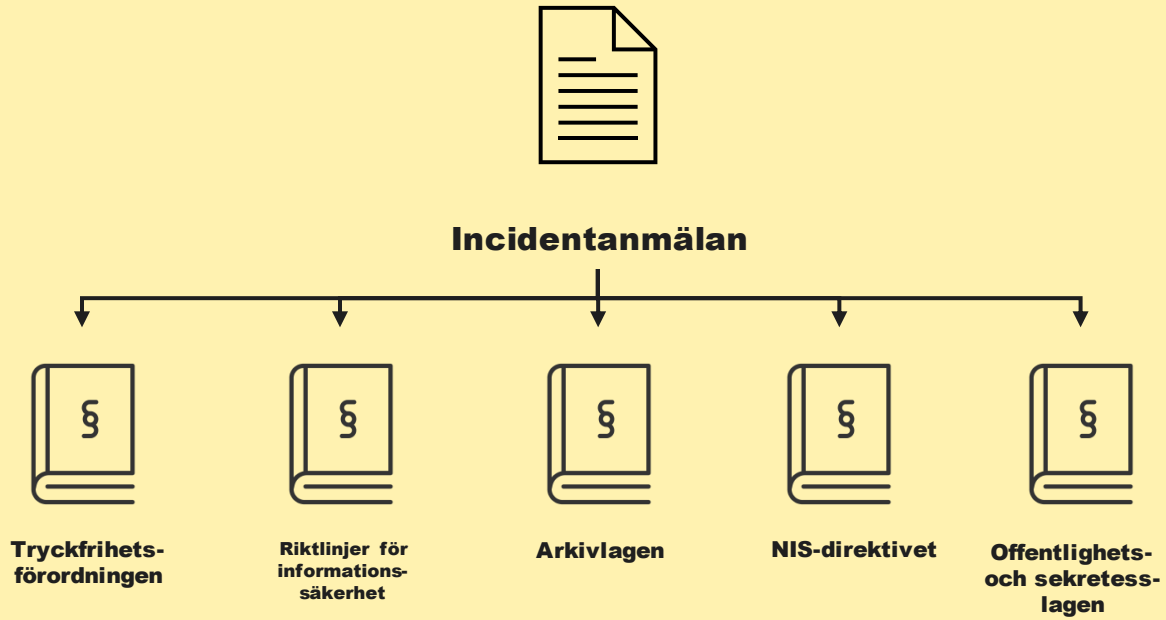
Exempel:



Identifiera reglering

- Koppla styrdokument och lagar som är relevanta för informationshanteringen till de enskilda informationsmängderna.
- Se bilaga 2 för vanligt förekommande lagstiftning inom informationssäkerhetsarbetet.

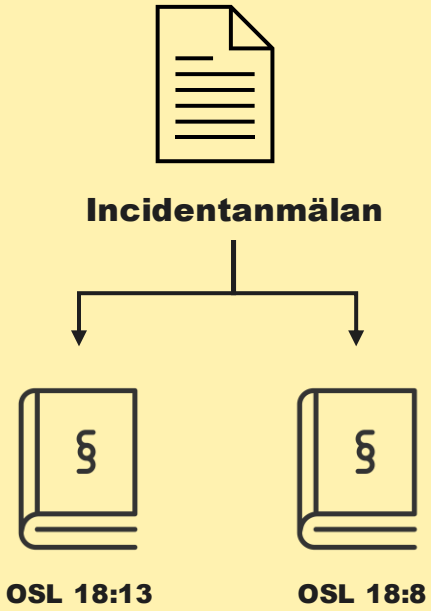
Exempel:



Identifiera sekretessreglerade uppgifter

- Sekretess regleras i offentlighets- och sekretesslagen (OSL).
- Identifiera om och i så fall vilka sekretessregleringar som kan vara aktuella för varje informationsmängd.
- Att en informationsmängd kan omfattas av sekretess är ett viktigt underlag för att bedöma informationsmängdens konfidentialitet.
- Se bilaga 1 för vanligt förekommande sekretess

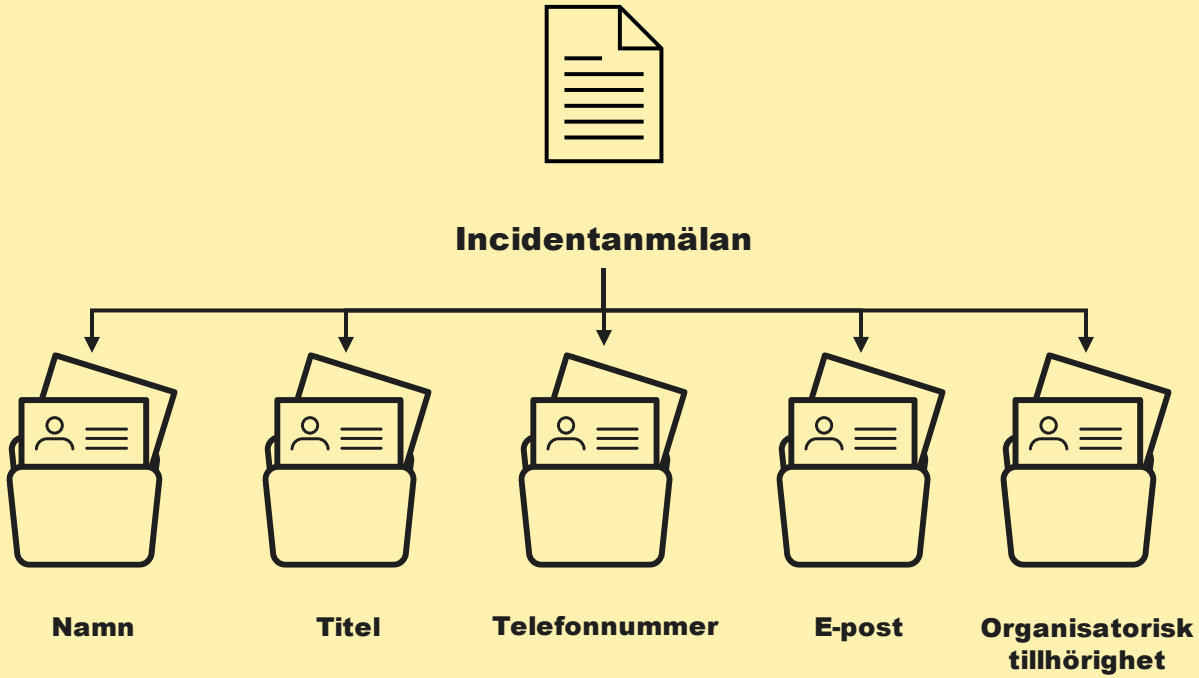
Exempel:



Identifiera personuppgifter

- Om en informationsmängd innehåller personuppgifter ska dessa identifieras.
- Personuppgifter kan vara ”direkta”, ex. namn, personnummer, e-post, bilder m.m.
- Personuppgifter kan också vara indirekta, ex IP-nummer, vissa typer av cookies, anställningsnummer m.m.
- Personuppgifter ska delas in i ”vanliga”, extra skyddsvärda och känsliga personuppgifter.

Exempel:



Klassa informationsmängderna

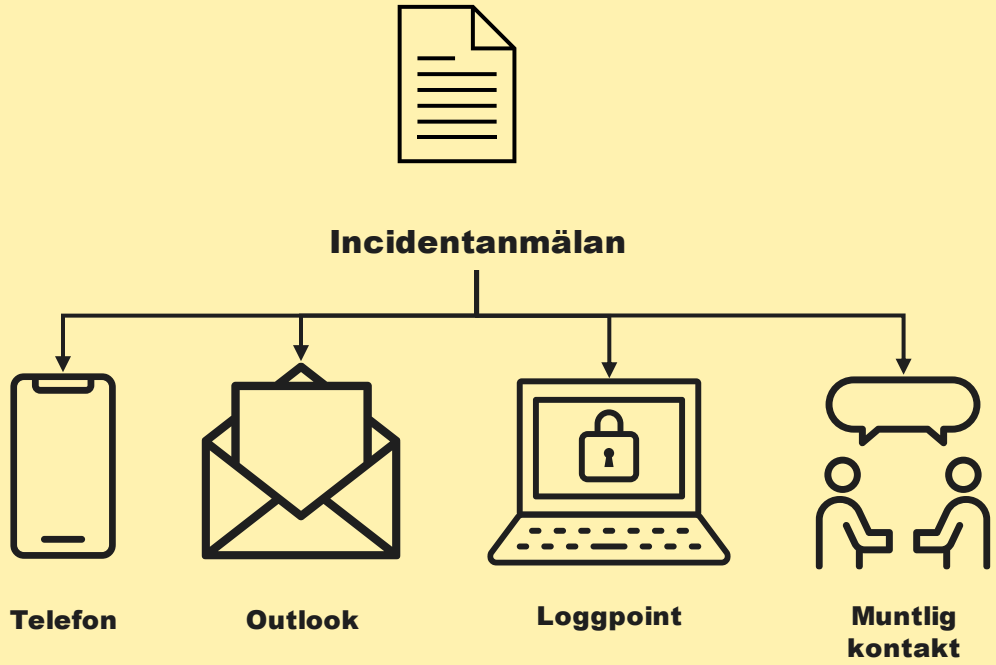
- Klassa varje enskild informationsmängd utifrån Stadens klassningsmodell.
- Klassningen ska göras utifrån konfidentialitets-, riktighets- och tillgänglighetsperspektiv.
- Den identifiering av sekretess och personuppgifter som genomförts tidigare ger en fingervisning om informationsmängdens känslighet.

Exempel:

Identifiera informations-bärare

- Varje informationsmängd hanteras av en eller flera informationsbärare.
- Identifieringen syftar till att krav ska kunna ställas på tjänster, system eller organisationer baserat på de lagar, personuppgifter och klassningen ni genomfört tidigare.

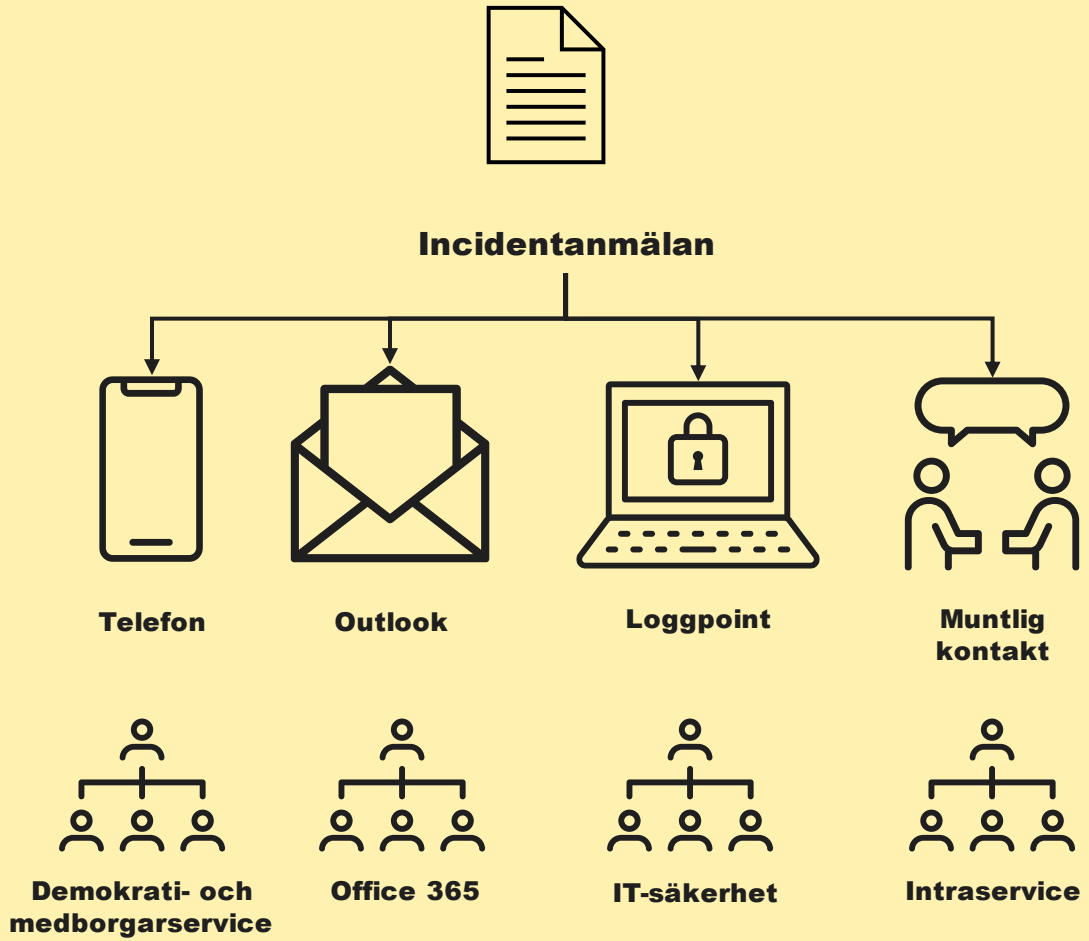
Exempel:



Identifiera leverantör

- För varje informationsbärare ska en leverantör identifieras
- Identifieringen syftar till att krav ska kunna ställas en viss organisation eller på leverantör av tjänst eller system.

Exempel:



Klassningen genomförd!

Bra jobbat!

Göteborgs Stad

Kontakt

Enheten för styrning och uppföljning av informationssäkerhet
ciso@intraservice.goteborg.se

Delegationsbeslut

Diarienummer	Kapitel i delegations-ordningen	Handläggare	Verksamhet/enhet
[XXXX/XX]	Kapitel 2.27	[Namn Namnsson]	[Verksamhet/enhet]

Datum för beslutet	Beslutsfattare	Anmäls	Delges
[20XX-XX-XX]	[Namn Namnsson]	*Anmäls till nämnden*	Klicka eller tryck här för att ange text. *Ange person/roll som berörs av beslutet.*

Beslut	*Fastställande av informationsklassning av [process]*
Beskrivning	*I enlighet med Göteborg Stads riktlinje för informationssäkerhet ska nämndens information informationsklassas. Nämnden för Intraservices anvisning för informationsklassning anger att informationsklassningen ska fastställas.*

Denna beslutsmall är ett stödjande dokument till *Intraservices anvisning för delegerade beslut*. Anvisningen hittas på intranätet under Styrande dokument i avsnittet *Styrning och uppföljning*.

Denna mall används för samtliga beslut som fattas enligt Intraservices delegationsordning. För att möta kraven på spårbarhet och transparens måste alla uppgifter i mallen fyllas i. Ifylld beslutsmall ska diarieföras (se Anvisning för delegerade beslut).

Kontakta Intraservices kansli vid frågor.

_____

[namnförtydligande, verksamhetschef]

Informationsklassning

#ID	Aktivitet	Informationsmåned	Beskrivning	Reglerine	Sekretess	Personuppgifter	Övriga krav	K	R	T	Informationsbärare	Leverantör	Kommentar
Instruktion	*Aktivitet i processkartan*	*T.ex. faktura, beslut, logg*	*T.ex. namn, adress, artikel-ID, belopp*	*T.ex. lagkrav, styrdokument, sekretessreglering*	*T.ex. 18:8, 26:1*	*T.ex. namn, IP-nummer, geografisk lokation*	*T.ex. Avtal*				*T.ex. Exchange, Treserva, telefonisystem, Sharepoint*	*T.ex. Intraservice, Microsoft, DIGG*	*Andra förhållanden, motiv m.m.*
#0001								Välj	Välj	Välj			
#0002								Välj	Välj	Välj			
#0003								Välj	Välj	Välj			
#0004								Välj	Välj	Välj			
#0005								Välj	Välj	Välj			
#0006								Välj	Välj	Välj			
#0007								Välj	Välj	Välj			
#0008								Välj	Välj	Välj			
#0009								Välj	Välj	Välj			
#0010								Välj	Välj	Välj			
#0011								Välj	Välj	Välj			
#0012								Välj	Välj	Välj			
#0013								Välj	Välj	Välj			
#0014								Välj	Välj	Välj			
#0015								Välj	Välj	Välj			
#0016								Välj	Välj	Välj			
#0017								Välj	Välj	Välj			
#0018								Välj	Välj	Välj			
#0019								Välj	Välj	Välj			
#0020								Välj	Välj	Välj			
#0021								Välj	Välj	Välj			
#0022								Välj	Välj	Välj			
#0023								Välj	Välj	Välj			
#0024								Välj	Välj	Välj			
#0025								Välj	Välj	Välj			
#0026								Välj	Välj	Välj			
#0027								Välj	Välj	Välj			
#0028								Välj	Välj	Välj			
#0029								Välj	Välj	Välj			
#0030								Välj	Välj	Välj			
#0031								Välj	Välj	Välj			
#0032								Välj	Välj	Välj			
#0033								Välj	Välj	Välj			
#0034								Välj	Välj	Välj			
#0035								Välj	Välj	Välj			
#0036								Välj	Välj	Välj			
#0037								Välj	Välj	Välj			
#0038								Välj	Välj	Välj			
#0039								Välj	Välj	Välj			
#0040								Välj	Välj	Välj			
#0041								Välj	Välj	Välj			
#0042								Välj	Välj	Välj			
#0043								Välj	Välj	Välj			
#0044								Välj	Välj	Välj			
#0045								Välj	Välj	Välj			
#0046								Välj	Välj	Välj			
#0047								Välj	Välj	Välj			
#0048								Välj	Välj	Välj			
#0049								Välj	Välj	Välj			

Klassningsobjekt [process/etc]

Ansvarig: [informationsägare]
Klassnings faställd av: [namn och befattning]

Diarienummer:
Datum för aktualisering: [datum]

Klassningsdokumentation

Klassning genomförd:	[Datum]

Klassning genomförd av:	[Deltagare 1] - Organisation
	[Deltagare 2]
	[Deltagare 3]
	[Deltagare 4]
	[Deltagare 5]
	[Deltagare 6]
	[Deltagare 7]
	[Deltagare 8]
	[Deltagare 9]
	[Deltagare 10]