Sammanfattning av informationsklassning och riskanalys av öppen leverantörsreskontra

Bakgrund

Publicering av öppen leverantörsreskontra innebär att en kommun, region eller statlig myndighet löpande tillgängliggör grundläggande information om inköpta produkter och tjänster. Syftet med att publicera denna data är bland annat att öka transparensen och insynen i den offentliga sektorn, samt att bidra till olika former av samhällsnytta. Genom att tillgängliggöra och dela offentliga data som öppna data skapas nya möjligheter för forskning, granskande journalistik och utveckling av nya tjänster och lösningar som bidrar till ökad effektivitet och kvalitet i den offentliga sektorn, samtidigt som det stärker förtroendet för offentliga institutioner och förbättrar effektiviteten i förvaltningen.

Myndigheten för digital förvaltning, Digg har med anledning av arbetet med inköpsdata i regeringsuppdraget Open data charter[1] bjudit in till en workshopsserie för att genomföra en informationsklassning och riskbedömning av att publicera öppen leverantörsreskontra med syftet att underlätta för offentliga organisationer att dela denna data öppet för vem som helst att använda. Diggs regeringsuppdrag innefattar att främja arbetet med tillgängliggörandet av data som kan bidra till transparens och insyn i den offentliga förvaltningen, särskilt inköpsdata. Uppdraget kopplar nära an till regeringens arbete med att vidareutveckla arbetet med öppna data och antikorruption[2].

Specifikation för öppen leverantörsreskontra

Den datamodell och specifikation som legat till grund för arbetet finns publicerad på Sveriges dataportal, www.dataportal.se. I specifikationen framgår vilka attribut (läs data) som omfattas samt vad de avser. Specifikationen går även att ladda ner via följande länk; https://lankadedata.se/spec/leverantorsreskontra/1.2.

Informationsklassning och riskanalys

Informationsklassningen syftar till att identifiera och bedöma skyddsvärdet för den information som hanteras vid publicering av leverantörsreskontra som öppna data[3]. Riskanalysen fokuserar på att identifiera potentiella risker relaterade till hanteringen av denna information. Resultaten från dessa analyser används som grund till rekommendationer för hur informationen ska hanteras. En säker hantering av

---

[1] Uppdrag att ansvara för genomförandet av Open Data Charters stadga | Digg

[2] Sveriges handlingsplan för Open Government Partnership 2023–2025 - Regeringen.se

[3] Vägledning för att tillgängliggöra information | Digg

informationen är avgörande för att säkerställa tillgången till denna information och för att säkerställa att hanteringen överensstämmer med gällande lagar och regler.

Målet är att alla delar av uppdraget ska omfattas av ett systematiskt och riskbaserat informationssäkerhetsarbete enligt ISO 27000-serien, gällande lagar och regler, samt respektive organisations interna styrning av informationssäkerhetsarbetet. Detta inkluderar att säkerställa och dokumentera säkerhetskritiska administrativa och tekniska processer samt att ha en formell grund där roller, ansvar och befogenheter är tydligt definierade.

Metod

Informationsklassning och riskanalys har genomförts i workshopformat med deltagare från Södertälje kommun, Västra Götalandsregionen (VGR), Myndigheten för digital förvaltning (DIGG), Sveriges Kommuner och Regioner (SKR) samt den Nationella dataverkstaden för regional och kommunal datadelning.

Bedömningar av konsekvenser vid bristande informationssäkerhet bygger på KLASSA-modellen med fem skadenivåer och de tre säkerhetsaspekterna; konfidentialitet, riktighet och tillgänglighet.

Värde	Konfidentialitet	Riktighet	Tillgänglighet
Nivå 4	Röjande av informationen medför **skada för Sveriges säkerhet som inte endast är ringa**.	Uppgifter som obehörigen, av misstag eller på grund av en funktionsstörning ändrats medför **skada för Sveriges säkerhet som inte endast är ringa**.	Ett avbrott som medför **skada för Sveriges säkerhet som inte endast är ringa**.
Nivå 3	Röjande av information medför **allvarlig skada.**	Information som obehörigen, av misstag eller på grund av en funktionsstörning ändrats medför **allvarlig skada.**	Ett avbrott medför **allvarlig skada.**
Nivå 2	Röjande av informationen medför **betydande skada.**	Information som obehörigen, av misstag eller på grund av en funktionsstörning ändrats medför **betydande skada.**	Ett avbrott medför **betydande skada.**
Nivå 1	Röjande av informationen medför **måttlig skada.**	Information som obehörigen, av misstag eller på grund av en funktionsstörning ändrats medför **måttlig skada.**	Ett avbrott medför **måttlig skada.**
Nivå 0	Röjande av informationen medför ingen eller **försumbar skada.**	Information som obehörigen, av misstag eller på grund av en funktionsstörning ändrats medför **ingen eller försumbar skada.**	Ett avbrott medför ingen eller **försumbar skada.**

Fig 1. Matris över skadenivåer och säkerhetsaspekter enligt KLASSA-modellen

Riskanalysen använder sig av samma skadenivåer och en skala för sannolikhet med fyra steg.

Värde	Sannolikhet	Definition	Beskrivning
4	Ofta/Mycket hög/mycket sannolik	Händelsen kommer nästan helt säkert att inträffa	• Händelsen kommer med största sannolikhet att inträffa • Händelsen kan inträffa när som helst under året
3	Regelbundet/Hög/Sannolik	Händelsen kommer sannolikt att inträffa under de flesta förhållanden	• Typen av händelser är allmänt kända för att kunna inträffa • Kan förväntas inträffa under de kommande 1–2 åren
2	Sällan/Medelhög/möjlig	Händelsen kan möjligen inträffa vid enstaka tillfällen	• Det har inträffat i den egna eller i närliggande verksamheter • Kan inträffa under kommande 5 åren
1	Mycket sällan/låg/osannolik	Händelsen är osannolik, men skulle kunna inträffa under exceptionella förhållanden	• Händelsen har aldrig inträffat förr och det finns endast enstaka kända fall av händelsen • Bedöms inte inträffa under de närmaste 5 åren

Fig 2. Matris över nivåer för sannolikhet

Genomförande

Publicering av leverantörsreskontra som öppna data sker vanligtvis i tre steg för att säkerställa att denna data tillgängliggörs och publiceras på ett säkert och ändamålsenligt sätt. Publicering sker vanligtvis en gång per månad i samband med att månadsbokslutet är slutfört, runt den 15:e dagen varje månad.

I det första momentet sker **utläsning** av den information som ska publiceras som öppna data. Grundläggande information om anskaffade produkter och tjänster exporteras från ekonomisystemet till en fil i csv-format. Det sker genom en manuell eller automatiserad rapport och exportfunktion i ekonomisystemet.

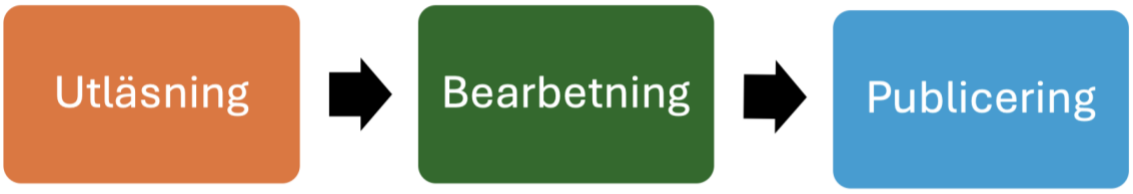

Fig 2. Illustration av ett ungefärligt genomförande av publicering av leverantörsreskontra

I nästa moment sker **bearbetning** av den data som exporterats. Bearbetningen syftar till att anpassa exporterade data så att information som inte ska publiceras modifieras och/eller filtreras bort. Detta sker genom att exempelvis ersätta uppgifter som utgör personuppgifter med andra standardvärden; personnummer ersätts vanligtvis med en nolla (0) och leverantörsnamn ersätts med en standardtext som talar om att leverantörsnamnet kan innehålla personuppgifter. På motsvarande sätt filtreras sekretessbelagda köp av produkter och tjänster bort. Modifieringen sker vanligtvis med hjälp av en integrationsplattform enligt ett förutbestämt regelverk. Detta steg är avgörande för att säkerställa att den data som publiceras öppet har den kvalitet och regelefterlevnad som kan förväntas.

I det avslutande steget sker **publicering** av den öppna leverantörsreskontran. Den färdigbearbetade datan tillgängliggörs och publiceras via organisationens metadatakatalog som öppna data för vidare användning. Vanligtvis publiceras denna data dels i form av en fil som kan laddas ned och dels som ett API som kan anropas av en applikation. I metadatakatalogen publiceras en beskrivning av datamängden och eventuellt API med länk till distributionen.

Resultat från informationsklassning

Informationsklassningsmodellen i SKR:s verktyg KLASSA[4] omfattar skala noll till fyra, ju högre siffra, desto högre konsekvens vid bristande säkerhet.

Vid informationsklassningen fick analysobjektet öppen leverantörsreskontra **skadenivå tre**, **allvarlig skada**, för säkerhetsaspekten **konfidentialitet**. Konsekvenser vid bristande konfidentialitet omfattar:

- Bristande konfidentialitet för den information som hanteras innebär betydande negativa konsekvenser för enskild individ, exempelvis kränkning av individers rätt till privatliv om känsliga personuppgifter sprids.
- Bristande konfidentialitet innebär att lagkrav såsom krav på sekretess och dataskydd inte efterlevs med negativ påverkan på kvalitet i uppdraget att tillgängliggöra öppen leverantörsreskontra.
- Förlust av konfidentialitet kan innebära ekonomiska sanktioner som medför betydande ekonomiska kostnader för ansvarig verksamhet.
- Brister i konfidentialitet kan innebära missnöje och negativ påverkan på förtroendet för samhällets grundläggande principer och verksamhetens förmåga att hantera känslig information parallellt med uppdraget att tillhandahålla öppen leverantörsreskontra.

För säkerhetsaspekten **riktighet** resulterade analysen i **skadenivå tre**, **allvarlig skada**. Konsekvenser vid bristande riktighet omfattar:

- Bristande riktighet innebär att verksamheten har svårt att säkerställa att rätt data publiceras. Det kan innebära allvarlig negativ påverkan på kvalitet och tillförlitlighet för den öppna data som publiceras och möjligheten att vidareutnyttja den för andra ändamål såsom uppföljning eller utveckling av tjänster och produkter.
- Bristande riktighet kan innebära kostnader och merarbete som kräver tillskott eller omfördelning för de aktörer vars verksamhet bygger på den öppna data som publiceras. Bristande riktighet kan också innebära ekonomiska sanktioner som medför betydande ekonomiska kostnader för ansvarig verksamhet.
- Bristande riktighet kan innebära betydande missnöje och försämrat förtroende för aktörens förmåga att tillgängliggöra öppna data.

[4] KLASSA

Utifrån aspekten **tillgänglighet** landade bedömningen på **skadenivå tre**, **allvarlig skada**. Konsekvenser vid bristande tillgänglighet omfattar:

- Bristande tillgänglighet innebär att verksamheten har svårt att säkerställa att rätt data publiceras. Det kan innebära allvarlig negativ påverkan på kvalitet och tillförlitlighet för den öppna data som publiceras och möjligheten att vidareutnyttja den för att andra ändamål såsom uppföljning eller utveckling av tjänster och produkter.
- Bristande tillgänglighet kan innebära kostnader och merarbete som kräver tillskott eller omfördelning för de aktörer vars verksamhet bygger på den öppna data som publiceras.
- Bristande tillgänglighet kan innebära betydande missnöje och försämrat förtroende för aktörens förmåga att tillgängliggöra öppna data.

Resultat från genomförd riskanalys

Under påföljande riskanalys kompletteras de initiala bedömningarna i informationsklassningen med potentiella oönskade scenarion som riskerar att äventyra informationssäkerheten. Resultatet sammanställs i en riskmatris (fig 3) där respektive risk representeras av sitt ID. Höga risker, det vill säga de risker som hamnar på orange och röd del av skalan, ska prioriteras i arbetet med att implementera säkerhetsåtgärder. Riskmatrisen ger en översikt av allvarlighetsgraden i identifierade risker.

Sannolikhet \ Konsekvens	Mycket sällan	Sällan	Regelbundet	Ofta
Försumbar	7,8	5		
Måttlig		6,9		
Betydande	4	3	2	
Allvarlig			1	

Fig 3. Riskmatris över identifierade risker i samband med hantering av leverantörsreskontra

En fullständig redogörelse för samtliga risker som identifierades och bedömdes i riskanalysen finns redovisade i fig 4 nedan.

Konfidentialitet - vad kan inträffa så att görs tillgänglig för obehöriga eller används på ett otillåtet sätt.					
ID	Konsekvens	Sannolikhet	Riskvärde	Händelse och konsekvens	Åtgärd
1	Allvarlig	Hög/sannolik	12	Underlag som avslöjar säkerhetsåtgärder eller förmåga röjs genom publicering på grund av att fakturor inte har sekretessmarkerats (filteringen tar med fakturan). Kan få konsekvenser för sveriges säkerhet på aggregerad nivå för att det avslöjar förmåga att stå emot angrepp.	Hantera fakturor som har betydelse för sveriges säkerhets utanför ekonomisystemet. Se över rutin för manuell sekretessprövning. Filtrering av fakturor bygger på markering i ekonomisystemet.
2	Betydande	Hög/sannolik	9	Fält för fakturanummer används för kommentarer för att det är smidigt och fritextfält möjliggör varierad användning. Konsekvensen blir att information som inte ska delas sprids.	Se över användning av fritextfält, fasta val eller instruktioner för ifyllnad.
3	Betydande	Medelhög/möjlig	6	Uppgifter på företag som tillhandahåller skyddat boende publiceras på grund av handhavandefel (fakturan bokförs fel). Konsekvenserna omfattar att enskildas integritet kränks och att säkerheten i skyddat boende inte kan garanteras.	Säkerställ rutiner och kunskap hos medarbetare som konterar fakturor. Stickprov för att kontrollera att rutinen fungerar.
4	Betydande	Låg/osannolik	3	Exakta beloppet på köpt vård (tex faktura från försäkringskassan eller annan vårdgivare) kan kopplas till en enskild vilket gör att känsliga personuppgifter publiceras utan rättslig grund. Konsekvenserna omfattar att enskildas integritet kränks. Risk för ekonomiska sanktioner och försämrat anseende i publicerande verksamhet.	En patient/en åtgärd på en faktura. En möjlig åtgärd är att undanta fakturan vid kontering. Undersöka möjligheten till kvartalsfakturor så att fler åtgärder och patienter faktureras tillsammans (finns dock nationella beslut på att fakturering ska ske löpande).

	Riktighet - vad kan hända så att informationen är felaktig eller inaktuell?				
	Konsekvens	Sannolikhet	Riskvärde	Händelse och konsekvens	Åtgärd
5	Försumbar	Medelhög/möjlig	2	Dataspecifikation är inte aktuell på grund av bristande förvaltning så att verksamheter som bygger tjänster på öppna data inte kan nyttja den publicerade informationen och interoperabiliteten försämras.	Versionshantering så att data blir jämförbar över tid. Säkerställ förvaltning och livscykelhantering över tid.
6	Måttlig	Medelhög/möjlig	4	Det uppstår interna varianter av dataspecifikation så att publicerad data varierar i innehåll (kan avvika från officiell dataspecifikation) så att verksamheter som bygger tjänster på öppna data inte kan nyttja den publicerade informationen och interoperabiliteten försämras. Kan leda till stopp i tjänsten eller merarbete i verksamheter som nyttjar data.	Bör upptäckas när en tjänst som nyttjar datan sätts upp.
7	Försumbar	Låg/osannolik	1	Metadatan är inaktuell på grund av att det saknas etablerade begrepp (och utrymme för variation) vilket kan leda till att datan inte kan hittas eller förstås.	Landa i klarspråksanpassade begrepp som andra kan förstå

	Tillgänglighet - vad kan inträffa så att information inte finns tillgänglig?				
	Konsekvens	Sannolikhet	Riskvärde	Händelse och konsekvens	Åtgärd
8	Försumbar	Låg/osannolik	1	Data publiceras inte på grund av personalomsättning som påverkar manuella rutiner för publicering. Konsekvenser blir att aktuell data inte är tillgänglig. Det kan påverka förtroendet negativt för offentlig sektors förmåga.	En månad ger inga större konsekveser. Säkerställ att det finns rutiner och redundans i bemanning av uppgiften att publicera.
9	Måttlig	Medelhög/möjlig	4	Publicering genomförs inte som planerat på grund av tekniskt fel i något moment av genomförandet. Konsekvener blir att aktuell data inte är tillgänglig. Det kan påverka förtroendet negativt.	Säkerställa SLA (kravställning på tillgänglighet) på den part som tillhandahåller drift - motsvara tillgänglighetskraven.

Fig 4. Identifierade risker

Rekommenderade säkerhetsåtgärder

Föreslagna säkerhetsåtgärder syftar till att säkerställa att grundläggande informationssäkerhetskrav uppfylls enligt ISO 27000 samt att säkerställa att identifierade risker vid tillgängliggörande och publicering av öppen leverantörsreskontra hanteras på ett informationssäkert och ändamålsenligt sätt. Säkerhetsåtgärderna omfattar organisatoriska och tekniska säkerhetsåtgärder. Säkerhetsåtgärderna ska ses som förslag på viktiga aspekter att fånga i genomförandet, de behöver analyseras utifrån respektive verksamhets klassning av informationen med tillhörande identifierade risker i det aktuella sammanhanget, så att säkerhetsåtgärderna implementeras genom ett medvetet val på ett sätt som ger avsedd effekt. Förslaget är därmed inte komplett utan för att uppnå adekvat säkerhetsnivå behöver samtliga krav i ISO 27000 beaktas för att säkerställa en förmåga att upprätthålla skydd över hela livscykeln.

Beroende på respektive verksamhets förutsättningar behöver säkerhetsåtgärderna omsättas till handling som en del av verksamhetens ordinarie planering och genomförande. Om exempelvis drift, förvaltning och utveckling av it-komponenter är utkontrakterade till en extern part behöver säkerhetskraven hanteras inom ramen för samma överenskommelse, för att inte introducera ytterligare risker vid tillgängliggörande och publicering av öppen leverantörsreskontra.

Tekniska säkerhetsåtgärder:

- **Kryptering**: Kryptera information med högt skyddsvärde både i vila (data som lagras på servrar eller databaser) och under överföring (när data sänds mellan system eller till externa användare). Använd starka krypteringsprotokoll för att säkerställa att data inte kan avlyssnas eller manipulera under överföring.
- **Åtkomsthantering**: Implementera rollbaserad åtkomstkontroll för att säkerställa att endast behöriga användare har tillgång till känslig data. Använd principen om minst möjliga behörighet för att begränsa åtkomst till information baserat på användarnas behov.
- **Autentisering:** Använd multifaktorautentisering (MFA) för att förbättra säkerheten vid åtkomst till system och databaser som innehåller öppna data. Detta säkerställer att endast auktoriserade användare kan få tillgång till dessa data.
- **Pseudonymisering**: Analysera hur pseudonymisering kan tillämpas för att dölja känslig information när den inte behöver exponeras i klartext.
- **Sårbarhetshantering**: Säkerställ att alla system som används för att lagra och publicera öppna data hålls uppdaterade med de senaste säkerhetsuppdateringarna. Det minskar risken för att utnyttja kända sårbarheter i mjukvaran. Använd sårbarhetsskanning och penetrationstester för att identifiera säkerhetshål i de system som hanterar öppna data. Vidta åtgärder så att dessa system är skyddade mot externa attacker och obehörig åtkomst.
- **Loggning och övervakning**: Implementera loggning och övervakning av åtgärder som rör öppna data, särskilt för användarinteraktioner och systemändringar. Det

gör det möjligt att upptäcka misstänkta aktiviteter och spåra incidenter i efterhand.
- **Regelbunden säkerhetskopiering**: Säkerställ att öppna data och relaterade system säkerhetskopieras regelbundet för att skydda mot dataförlust. Säkerhetskopior bör också krypteras för att skydda data om någon obehörig får åtkomst till dem.
- **Återställningsplaner**: Utveckla och testa återställningsplaner för att kunna återställa data snabbt efter en incident, som exempelvis dataintrång eller systemfel. Detta minskar driftstopp och säkerställer tillgängligheten för öppna data.

Organisatoriska säkerhetsåtgärder

- **Datahantering**: Skapa en strategi för datahantering, där det definieras vem som ansvarar för vilken data och hur känslig information ska hanteras. Inkludera alla relevanta intressenter, från sakkunniga till dataskyddsansvariga och tekniska team.
- **Hantering av tillgångar**: Tillämpa en modell och arbetssätt för informationsklassning, exempelvis Klassa. Ta fram hanteringsregler för att säkerställa att information hanteras enligt dess skyddsvärde genom alla moment som påverkar leveransen av öppna data.
- **Riskhantering**: Genomför regelbundna riskbedömningar för att identifiera potentiella hot och sårbarheter som kan påverka publicerade öppna data, särskilt när det gäller oavsiktlig exponering av känslig information. Använd en systematisk metod, för att prioritera och hantera dessa risker.
- **Utbildning:** Ge regelbundna utbildningar till de anställda om säkerhetspolicyer, datahantering och risker. Säkerställ att alla som hanterar data som utgör öppna data är medvetna om riskerna med att inkludera känslig information och förstår sin roll i hanteringen.
- **Riktlinjer för datasekretess**: Ta fram och implementera riktlinjer för att identifiera och skydda känslig information innan den publiceras. Vid publicering av data ska det finnas en tydlig process med etablerade roller och ansvarsförhållanden för att säkerställa att endast avsedd information görs tillgänglig för allmänheten. Säkerställ efterlevnad och relevans genom stickprov för att avgöra data innehåller personuppgifter eller information om säkerhetsåtgärder och andra känsliga detaljer.
- **Incidenthantering**: Ta fram och testa en plan för att hantera säkerhetsincidenter, såsom felaktig offentliggörande av känslig information, för att snabbt kunna åtgärda problem och minska skador om det inträffar. Planen bör inkludera åtgärder för att upptäcka, rapportera, och hantera säkerhetshändelser relaterade till öppna data.
- **Säkerhet i leverantörsrelationer**: Utför säkerhetsbedömningar av alla leverantörer som hanterar komponenter som ingår i publicering av öppna data. Säkerställ att dessa leverantörer följer lämpliga säkerhetsstandarder och att de är medvetna om sina säkerhetsåtaganden genom kontrakt och avtal.
- **Risker i leverantörsrelationer**: Bedöm potentiella risker i leverantörsrelationerna, såsom om leverantören har tillgång till känslig data eller om deras tjänster är kritiska för driften av öppna data.

- **Säkerhetskrav i avtal**: Inkludera säkerhetskrav och sekretessavtal i kontrakt med leverantörer för att säkerställa att de upprätthåller lämpliga säkerhetsåtgärder och skyddar integriteten och konfidentialiteten hos data. Ange tydliga ansvarsfördelningar och rapporteringskrav i händelse av säkerhetsincidenter som kan påverka dataskydd eller tillgång till öppna data.

Efterlevnad

- **Dataskydd**: Säkerställ att all hantering av personuppgifter följer principerna i dataskyddsförordningen. Detta inkluderar bland annat bedömning av rättslig grund, att säkerställa öppenhet gentemot registrerade samt att upprätthålla rätt att få tillgång till, rätta eller ta bort personuppgifter när det är nödvändigt samt rapportering av incidenter.
- **NIS-direktivet**: Säkerställ att verksamheten som publicerar öppna data följer de krav som ställs av NIS-direktivet vilket inkluderar ett systematiskt och riskbaserat säkerhetsarbete i hela organisationen, engagerad ledning, hantering av leverantörskedjor, förmåga till kontinuitet och rapportering av incidenter.

Kontinuitetshantering

- **Kontinuitetsplan**: Skapa och underhåll en robust verksamhetskontinuitetsplan som inkluderar åtgärder för att hantera avbrott eller problem. Detta kan innebära redundanta lösningar eller att ha alternativa leverantörer tillgängliga för att säkerställa att tillgången till öppna data inte äventyras.
- **Återställningsplan:** Utveckla och testa återhämtningsplaner för att återställa öppna data om en tjänst eller en teknisk lösning går ner. Testa dessa planer regelbundet för att säkerställa att de ger avsedd effekt.