Lämplighetsbedömning avseende Sekretessbrytande regel i OSL vid teknisk bearbetning och lagring

Migrering Testladdning utökning Kroniska Diagnoser

SDV Programmet

Innehållsförteckning

1 Övergripande information

2 Säkerhetsskyddsanalys enligt Säkerhetsskyddslagen (2018:585)

3 Systematisk beskrivning av utkontrakteringen, tekniska bearbetningen och lagringen

4 Lämplighetsbedömning Säkerhet

5 SAMMANSATT BEDÖMNING

Region Skåne tillgodoser sitt behov av säker och effektiv it-drift genom att utkontraktera delar av it-driften till privata tjänsteleverantörer. I samband med en utkontraktering tillgängliggörs i regel en omfattande mängd uppgifter för tjänsteleverantören. En uppgift som omfattas av sekretess och som görs tillgänglig för en tjänsteleverantör betraktas som utlämnad eller röjd i offentlighets- och sekretesslagens mening. Ett sådant röjande är bara tillåtet om sekretess inte hindrar att uppgiften lämnas ut.

Den myndighet som i samband med en utkontraktering gör uppgifter tillgängliga för en tjänsteleverantör måste utöver sekretesslagstiftningen även beakta dataskyddslagstiftningen och se till att åtgärden är förenlig med båda dessa regelverk – regelverken är inte likstämmiga eller utbytbara. Myndigheten måste också överväga vilka konsekvenser åtgärden får för handlingarnas status etc. enligt tryckfrihetsförordningen.

Enligt den sekretessbrytande bestämmelsen i 10 kap. 2 a § OSL hindrar sekretess inte att en uppgift lämnas till en tjänsteleverantör som för den utlämnande myndighetens räkning har i uppdrag att endast tekniskt bearbeta eller tekniskt lagra uppgiften, om det med hänsyn till omständigheterna inte är olämpligt att uppgiften lämnas ut. Region Skåne behöver inför ett utlämnande göra en lämplighetsbedömning för att avgöra om uppgifterna kan tillgängliggöras för en tjänsteleverantör på ett rättsenligt, säkert och lämpligt sätt, och att Region Skåne därmed får lämna ut sekretessbelagda uppgifter med stöd av den sekretessbrytande bestämmelsen.

Avgörande vikt vid lämplighetsbedömningen är att beakta hur de intressen som sekretessen avser att skydda tillgodoses av mottagaren. Region Skåne är ytterst ansvarig för att den information som hanteras av myndigheten själv *eller av någon annan* får ett ändamålsenligt skydd och i övrigt hanteras i enlighet med gällande rätt. Därav måste Region Skåne lämplighetsbedöma tjänsteleverantören förmåga att skydda uppgifterna, det vill säga säkerställa att tjänsteleverantören är lämplig för detta ändamål.
Generell vägledning för lämplighetsbedömningen är att göra ett ställningstagande efter genomgång av avsnitt 2 på vilka delar av lämplighetsbedömningen som är tillämpliga. Avsnitt som ej är tillämpliga kan utlämnas med en motivering i delbedömningens summering.
Använd i så stor utsträckning som möjligt bilagor eller referenser till befintlig dokumentation istället för att kopiera informationen och dubbeldokumentera.

1 Övergripande information

1.1 Informationsägare för uppgifterna som ska lämnas ut

Personuppgift om patient – HSS Direktör Pia Lundbom

1.2 Kontaktpersoner för lämplighetsbedömningen

1.2.1 GENOMFÖRANDE

Namn och e-post till den/de som medverkat vid lämplighetsbedömningens genomförande och kan fungera som kontaktpersoner i ärendet om någon del behöver förtydligas eller följas upp.

Niklas Strid – Projektledare Regelefterlevnad SDV

1.2.2 FÖRVALTNING

Namn och e-post till den/de som ansvarar för att förvalta lämplighetsbedömningen, vilket innebär att se till att den är aktuell och att åtgärderna är fortsatt effektiva om behandlingen, omständigheter eller risker ändras.

Marie Louise Arendt, MarieLouise.Arendt@skane.se

1.3 Projektinformation

Om utkontraktering planeras inom ramen för ett projekt, ange projektnamn och eventuellt projekt-ID.

SDV Programmet – Millennium Migrering

1.4 Systeminformation

Om utkontrakteringen sker eller kommer att ske inom ett it-system, ange systemnamn/en och system-ID/n.

SDV System id 00889

1.5 Kortfattad beskrivning av utkontrakteringen och/eller tjänsteleverantören

Beskriv kortfattat utlämnandet, tjänsteleverantören, it-systemet, den nya funktionen i it-systemet etc. som utkontrakteringen avser. Denna information kan exempelvis finnas i en projektplan. Beskriv även avgränsningen för denna lämplighetsbedömning. Förändring av tjänsteleveransen som medför att lämplighetsbedömningen behöver uppdateras beskrivs här.

Region Skåne har beslutat att använda Cerner Sverige ABs leverans Millennium för att hantera journalföring. Som en del av detta beslut kommer det att vara nödvändigt att dela information om både patienter och anställda i enlighet med tillämpliga dataskyddslagar, inklusive Offentlighets- och sekretesslagen (OSL). I detta tillägg kommer Kroniska diagnoser samt de tillhörande ICD10 koder att delas med Cerner Sverige AB för teknisk bearbetning och lagring.

1.6 Lämplighetsbedömningens effektmål

i *Dessa frågor besvarar vad Region Skåne vill uppnå med tekniska bearbetningen och lagringen och vilka positiva effekter det kommer att få med systemet eller utkontrakteringen*

Beskriv vilka förväntade effekter utkontrakteringen kommer att få för Region Skåne.

Genom utkontraktering till Cerner Sverige AB och inköp av programsviten Millennium för journalföring vill vi säkerställa att information om både patienter och anställda delas i enlighet med Offentlighets- och sekretesslagen (OSL). Främsta fokus är patientsäkerhet. Genom effektivare informationsflöde och möjlighet att erbjuda sammanhållen journalföring, kommer vi att minska risken för felaktiga beslut och lösa en tydlig brist inom hälso- och sjukvården i Skåne idag.

Vi strävar efter att upprätthålla överensstämmelse med dataskyddslagar för att skydda patienternas integritet och sekretess. Därigenom stärker vi förtroendet för våra vårdtjänster. Målet är att öka patientsäkerheten, minimera risker för felaktig medicinsk behandling och garantera att patientdata är korrekt och säkert hanterad. Detta kommer att gynna patienterna och främja en hög standard av vårdkvalitet inom Region Skåne

Tillägg av Kroniska diagnoser och dess tillhörande ICD10 koder kommer att möjliggöra ytterligare tester av systemet för att försäkra sig om att såväl funktionella som icke funktionella krav kan verifieras innan systemet driftsättes

1.7 För ny funktion i it-system, utökning av utkontraktering eller för befintlig tjänsteleverantör

i *Dessa frågor besvarar vad Region Skåne tidigare har bedömt i befintliga system/utlämnade/leverantörer relaterat till det nya utlämnandet eller tjänsteleverantören. Vägledning till kommande avsnitt*

Beskriv eventuell relation till befintligt system, utkontraktering eller tjänsteleverantör.

Beskriv vilka förändrade förutsättningar utkontrakteringen kommer att få för Region Skåne.

Denna partner har inte tidigare genomgått Lämplighetsbedömning. Dock så har menprövning gjorts för tidigare utlämning till Cerner Sverige AB med ett positivt resultat

Länk till tidigare beslut: https://www.skane.se/namndshandlingar/8170301/

2 Säkerhetsskyddsanalys enligt Säkerhetsskyddslagen (2018:585)

Steg 1 är att genomföra en säkerhetsskyddsanalys. Efter det görs en säkerhetsskydds–bedömning och en lämplighetsprövning. Syftet med lämplighetsprövningen är att klarlägga om en utkontraktering kan leda till skadekonsekvenser på nationell nivå. Underlaget används sen till att bedöma om utkontrakteringen är lämpligt ur ett säkerhetsskyddsperspektiv.

2.1 Har Särskild säkerhetsskyddsbedömning genomförts enligt Region Skånes process?

i

Inledningsvis måste en säkerhetsskyddsanalys följt av en särskild säkerhetsskyddsbedömning enligt Säkerhetsskyddslagen (2018:585) genomföras för utlämningen och det tilltänkta systemet enligt Region Skånes riktlinjer. Frågorna i detta avsnitt måste besvaras med ”ja”, annars är utlämningen olämplig och lämplighetsbedömningen avslutas.

Kriterium	Ja	Nej
Är säkerhetsskyddsbedömningen genomförd i samråd med enhetens säkerhetsskyddsamordnare?	Ja	
Hanterar IT-systemets samtliga uppgifter klassificerade på nivå ” Ej Säkerhetsskyddsklass”?	Ja	
Är konsekvenserna för hantering av informationen på Konsekvensnivå 1?	Ja	

2.2 Summerad bedömning inom Säkerhetsskyddsperspektiv

Gör en summerade bedömningen om det är olämpligt/inte olämpligt att genomföra den föreslagna utlämningen för tekniska bearbetning och lagring hos tjänsteleverantören utifrån säkerhetsskyddsperspektiv.

Utifrån ett Säkerhetsskyddsperspektiv är utlämnandet inte olämpligt

3 Systematisk beskrivning av utkontrakteringen, tekniska bearbetningen och lagringen

Detta avsnitt ska ge en tydlig överblick över den aktuella utkontrakteringen, tekniska bearbetningen och lagringen

3.1 Informationssäkerhetsklassificering

Informationssäkerhetsklassificering är av yttersta vikt för att skydda och hantera konfidentiell information inom Region Skåne och skall genomföras enligt processen som beskrivs på intranätet En korrekt genomförd informationssäkerhetsklassificering underlättar inte bara vid bedömningen av hur känslig information ska skyddas utan är även ett stöd för att bestämma vilka åtgärder som bör vidtas för att säkerställa adekvat hantering. Detta ligger som grund för att i avsnitt 3.2 fylla i vilken information som omfattas av sekretess. I informationssäkerhetsklassificering klargörs även andra applicerbara lagar som ligger till grund för ifyllnad i senare stycken.

Informationssäkerhetsklassificering genomförd med följande resultat:

Klassificering

Nedan informationsmängder har identifierats och klassificeras enligt följande. Siffrorna visar konsekvenserna om kraven inte kan efterlevas.

Informationstillgång	**K**	**R**	**T**
Personuppgifter Region Skåne anställda	3	3	3
Administratörskonto (Region Skåne anställda)	3	3	3
Personuppgifter om patienter Region Skåne	4	4	3
Personuppgifter om patienter Extern Vårdgivare	4	4	3
Loggad information Region Skåne	3	3	3
Total bedömning	**4**	**4**	**3**

3.2 Beskrivning av sekretessbelagd information

i

Uppgifternas art och känslighet bör finnas med i inventeringen, viktigt när man prövar olämplighet. Gäller även om uppgifterna kommer från en samhällsbärande verksamhet (tänk NIS)

I tabellen nedan ska det inventeras vilka uppgifter som är aktuella samt vad de innehåller.

Förklaring:

Beskrivning av information: En kortfattad beskrivning av den sekretessbelagda informationen, t.ex. personuppgifter, information om upphandling eller medicinsk journal

Mottagare: De personer, företag eller organisationer som är auktoriserade att få tillgång till den sekretessbelagda informationen

Geografisk räckvidd: Den geografiska omfattningen där den sekretessbelagda informationen kan hanteras eller delas, t.ex. bara inom ett specifikt land eller internationellt

Kategori av sekretessbelagd information: Vilken typ av information som omfattas av sekretess, välj i drop-down listan

Typ av sekretess: Nivå av sekretess eller skydd som krävs, välj i dropdown

Antal uppgifter: Det totala antalet uppgifter som omfattas av sekretess inom den specifika informationen

Informationsägare: Den individ, företag eller organisation som äger den sekretessbelagda informationen och har rätt att bestämma hur den ska användas och delas

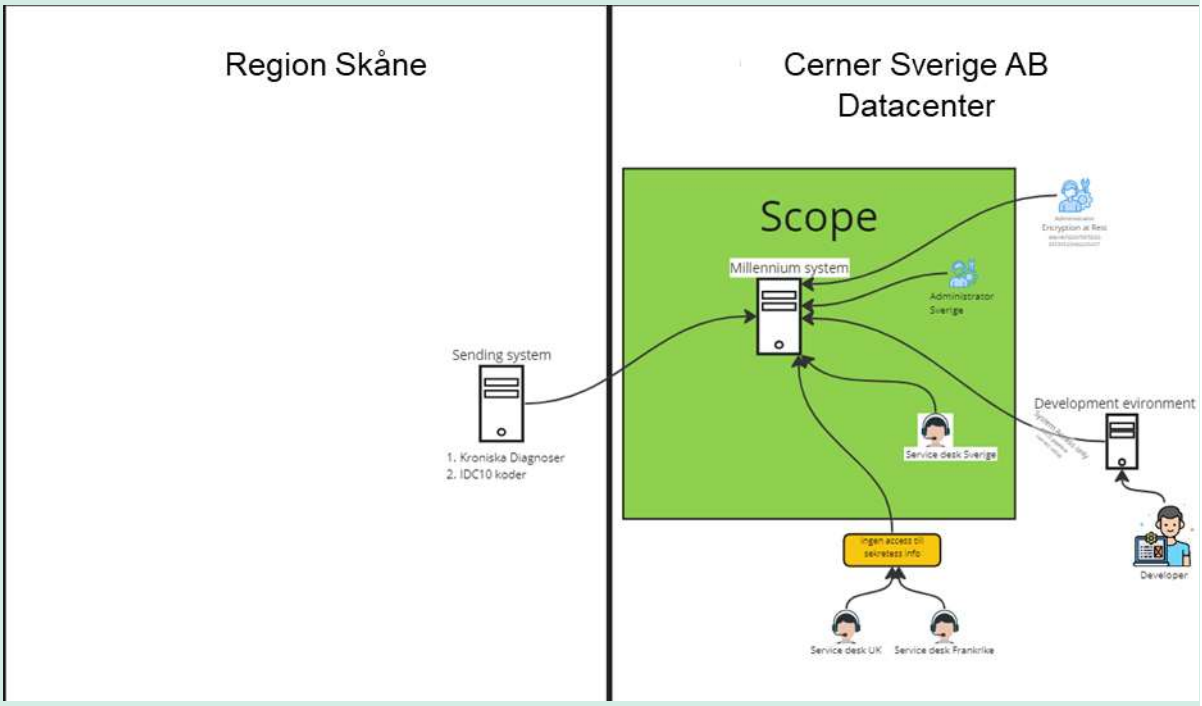
Roll med access hos tjänsteleverantören: Beskriv vilken roll hos tjänsteleverantören som har tillgång samt vilken nivå av tillgång dem har, t.ex. fullständig läs, begränsad läs, fullständig läs och skriv etc

Beskrivning av informationen	Mottagare	Geografisk räckvidd	Typ av sekretess enligt OSL	Kommentar	Antal uppgifter	Informations-ägare	Roll med access till data hos Tjänsteleverantör
Utlämning av sekretessbelagda personuppgifter om hälsa (patient) för bearbetning och lagring	Cerner Sverige AB med underbiträde och underleverantörer	Sverige	25 kap. 1 § OSL Sekretess till skydd för enskild i verksamhet som avser hälso- och sjukvård och annan medicinsk verksamhet		~1,4 miljoner journaler	HSS	Administratör, Service desk

3.3 Översiktlig beskrivning av uppgiftsflödet

Hur säkerställs det att de intresse som sekretessen avser att skydda tillgodoses av mottagaren? Vilka andra omständigheter måste ytterligare beaktas för att uppgiftshanteringen ska vara förutsebar och säker? Hur skyddar mottagaren uppgifterna mot ytterligare spridning?

Bifoga en schematisk bild över hur informationen vid utkontrakteringen flödar som inkluderar externa mottagare för uppgifterna. Om uppgifter överförs till andra länder ska detta framgå av bilden.



I scopet ingår följande:

Information som utlämnandet omfattar är beskrivna i Konsekvensbedömning avseende dataskydd avsnitt 4-6 daterad 2023-10-16. Utlämnandet kommer att tekniskt bearbetas och lagras av personal inom grönmarkerat område i bilden vilket omfattar driftstjänst, administration och support av Cerner Sverige AB genom underbiträden och underleverantörer.

3.3.1 DEN TEKNISKA BEARBETNINGEN OCH LAGRINGENS GEOGRAFISKA RÄCKVIDD SAMT EVENTUELLA UNDERLEVERANTÖRER

Beskriv var uppgifterna som lämnas ut ska hanteras geografiskt samt om/hur den geografiska räckvidden påverkar skyddet av uppgifterna.

Data är lagrat fysiskt i Sverige, Datahallar ligger i Stockholm

3.4 Tröskelvärde för utlämnade till viss tjänsteleverantör

i *Att man har för mycket data hos en och samma tjänsteleverantör vilket medför större påverkan vid avbrott och en ökad riskexponering (Region Skåne perspektiv).*

Specificera omfattningen av samtliga utkontrakteringar för teknisk bearbetning och lagring till tjänsteleverantören och gör ett utlåtande om tröskelvärde för utkontrakteringar till tjänsteleverantören är under eller över tröskeln. Bedömning av tröskelvärdet görs inom avsnitt Informationssäkerhet i samråd med Regional Informationssäkerhet baserat på gällande riktlinjer.

Leverantören levererar nuvarande journalsystem Melior och Obstetrix som kommer att ersättas av Millennium. Även PMO och PASIS kommer ersättas på sikt tillsammans med ca 27 andra mindre system. Totalt utgör det här systemet en kritisk del men inte helheten från Region Skånes IT system.

Med denna implementation balanserar vi ut risken från Tieto som enda Driftsleverantör. Tieto sköter idag driften av tidigare nämnda system.

Svårt att dela upp data när man går mot en ”delad vård och omsorgsdokumentation” med ett system.

Minskar riskexponeringen

Västragötalandsregionen som kommer att använda samma system bidrar till ett ökat intresse för leverantören att tillhandahålla en bra och stabil tjänsteleverans. Ur ett nationellt perspektiv innebär det inte att tröskelvärdet för nationell vård överskrids

4 Lämplighetsbedömning Informationssäkerhet

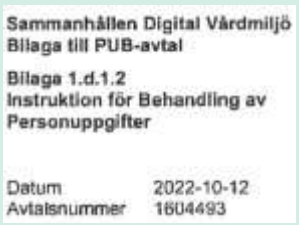
I detta avsnitt dokumenteras om uppgifterna kan tillgängliggörs för tjänsteleverantören på ett säkert och lämpligt sätt, samt om tjänsteleverantören har förmåga att skydda uppgifterna i enlighet med Region Skånes krav på informationshantering.

4.1 Efterlevnad och Informationssäkerhet

i *Innan en uppgift lämnas ut ska det prövas: dels om det finns skäl som talar emot ett utlämnade; dels om tjänsteleverantören kan tillgodose så de intressen beaktas som sekretessen avser att skydda, samt att tjänsteleverantören har förmåga att skydda de utlämnade uppgifterna.*

Med hjälp av frågorna nedan, vars svar kan ingå i en riskanalys, är avsikten att göra en prövning ur ett informationssäkerhetsperspektiv av om uppgifterna får ett ändamålsenligt skydd samt om uppgiftshanteringen är förutsebar och sker i enlighet med gällande rätt.

4.1.1 EFTERLEVNAD

Kravområde	Beskrivning av krav	Kravuppfyllnad	Olämplig
Laglighetsbedömning	Att det finns en dokumenterad laglighetsbedömning: hanteringen är tillåten enligt tillämplig lagstiftning utöver utkontrakteringen och lämplighetsbedömningen.	Ja, utlämningen kan anses följa lagen om ut-kontraktering för bearbetning och lagring	Nej, krav uppfyllt utan anmärkning
Tystnadsplikt för mottagaren	Att det finns en tillämplig lagstadgad tystnadsplikt eller en lämplig avtalsreglerad tystnadsplikt mellan tjänsteleverantören och Region Skåne.	Ja, Avtalet reglerar detta genom att peka ut svensk lagstiftning. Lag (2020:914) om tystnadsplikt vid utkontraktering av teknisk bearbetning eller lagring av uppgifter	Nej, krav uppfyllt utan anmärkning
Avtal om personliga sekretessförbindelser	Att avtalet mellan mottagaren och Region Skåne innehåller krav på att tjänsteleverantörens personal undertecknar personliga sekretessförbindelser.	Verifierat existerar i biträdesinstruktionen 	Nej, krav uppfyllt utan anmärkning
Genomförd bedömning av leverantörens möjlighet till GDPR efterlevnad	Riskanalys utifrån DSF perspektiv och GDPR art 28.1 skall genomföras och vid behov även konsekvensanalys.	Konsekvensbedömning genomförd utan höga risker Artikel 28.1 bedömning Länk: https://sakerlagring.i.skane.se/sites/sdvriskanalyser/Art281/Beslutade	Nej, krav uppfyllt utan anmärkning
Personuppgiftsbiträdesavtal samt Instruktion för behandling	Att det finns ett upprättat personuppgiftsavtal med tillhörande instruktioner om mottagaren ska behandla personuppgifter Att en tydlig instruktion för behandlingen finns framtagen Om det är en utökning av tjänsten ska instruktionen uppdateras	Ja, Undertecknat 2022-10-12	Nej, krav uppfyllt utan anmärkning

4.1.2 INFORMATIONSSÄKERHET

Kravområde	Beskrivning av krav	Kravuppfyllnad	Olämplig
Systematiska säkerhetsarbete: *Certifierad*	En oberoende bedömning från tredje part på efterlevnad av en global säkerhetsstandard (ISO, CSA STAR 2, NIST etc.). Certifieringen ska gälla alla hostning platser och supportinrättningar där Region Skånes information hanteras (lagras, bearbetas, överförs etc.) Audit-rapport kan kunna uppvisas	Försäkransmaterial är inhämtad enligt följande: ISO Certifiering HIPPA Certifiering Privacy Shield Framework certifiering	Nej, krav uppfyllt utan anmärkning
Efterlevnad av informationssäkerhetskrav: *Intyg*	Tillhandahålla ett intyg som är utfärdad av en ackrediterad tredje part som påvisar att man följer ramverk som: AICPA SOC 2 Type II-rapport och CSA CCM Intyg ska kunna uppvisas	Granskning av följande dokument genomfört: SOC 2 typ 1 SOC 2 typ 2	Nej, krav uppfyllt utan anmärkning
Efterlevnad av informationssäkerhetskrav: *Penetrationstest*	Påvisa med intyg att det regelbundet utförts penetrationstester av de tjänster som tjänsteleverantören tillhandahåller Region Skåne, samt påvisa med intyg att eventuella brister som framkommit har åtgärdats	Penetrationstest görs regelbundet 1 gång per år eller vid stora uppdateringar samt delar kvartalsrapport på uppföljning av det som ertappades i penetrationstestet. Egna penetrationstester har gjorts från ett användarperspektiv. Rapport på svagheter som rapporterats finns.	Nej, krav uppfyllt utan anmärkning
Systematiska säkerhetsarbete & Efterlevnad av informationssäkerhetskrav: *Självuppskattning*	Att tjänsteleverantören har gjort en självuppskattning mot gällande internationella ramverk: NIST, CSA, ISO27000, ISO27001, ISO27002 eller motsvarande. Resultatet av självuppskattningen ska kunna tillhandahållas	N/A då leverantören är stor nog att genomgå certifiering varje år	Nej, ej tillämpligt krav
I tjänsteleverantörsavtalet: *Försäkran om efterlevnad*	I tjänsteleverantörsavtalet ska det krävas att tjänsteleverantören tillhandahåller, minst årligen, aktuella rapporter gällande försäkran om efterlevnad av definierade informationssäkerhetskrav:	Ja, finns med i avtalet	Nej, krav uppfyllt utan anmärkning

	AICPA SOC2 Type II-rapport eller liknade		
I tjänsteleverantörsavtalet: *Tekniska efterlevnadsskanningar*	Tjänsteleverantören ska kunna på begäran utföra tekniska efterlevnadsskanningar och tillhandahålla adekvata rapporter om resultatet	Månadsvis behörighetsstyrningsrapport för M1912 (migreringsdomän) presenteras månadsvis i SDV security forum	Nej, krav uppfyllt utan anmärkning
I tjänsteleverantörsavtalet: *Frekventa granskningar*	Tjänsteleverantören genomför frekventa granskningar av såväl kvalitetsarbete som säkerhet, samt på åtgärder och förbättringar när sårbarheter och brister upptäcks	Systematiskt säkerhetsarbete har uppvisats genom omfattande dokumentation som SOC2, Certifieringar, Pentest etc.	Nej, krav uppfyllt utan anmärkning
I tjänsteleverantörsavtalet: *Transparens*	Tjänsteleverantören är transparent och delar information så som information avseende kvalitetssäkring, säkerhetsarbete, incidenter, risker, hot och sårbarheter.	Ja, Metod Cerner flash, Exempel finns vid Log4j incidenten	Nej, krav uppfyllt utan anmärkning
I tjänsteleverantörsavtalet: *Incidenthantering*	I avtalet med tjänsteleverantören ska framgå hur man säkerställer ett konsekvent och effektivt tillvägagångsätt för hantering av incidenter inklusive kommunikation om säkerhetshändelser och svagheter.	Ja, finns i avtal, Bilaga 1m	Nej, krav uppfyllt utan anmärkning
I tjänsteleverantörsavtalet: *Avtalad exitstrategi*	Kontroll av nödvändiga uppsägningsmöjligheter och krav på dokumentation av en exitstrategi vid avslut/byte av tjänsteleverantör	Ja, Efter varje genomförd testladdning raderas all Test-data från laddningen. N/A för detta utlämnande	Nej, krav uppfyllt utan anmärkning
I tjänsteleverantörsavtalet: *Rätt till granskning*	Rätten att få granska tjänsteleverantörens processer och säkerhetsåtgärder relaterade till avtalet	Ja, årligen, I första hand granskning av tredjeparts audits,	Nej, krav uppfyllt utan anmärkning
Kontroll över digitala leveranskedjor	Tjänsteleverantören har insyn i och kontroll över sina egna digitala leveranskedjor	Ja, egen infrastruktur, nätverk etc.	Nej, krav uppfyllt utan anmärkning

Åtkomstkontroll	För att säkerställa auktoriserad åtkomst och förhindra obehörig åtkomst till information, och andra tillhörande tillgångar, ska hanteringen av åtkomstkontroll följa internationella ramverk som ISO27002 eller liknade. Krav på dokumenterat behörighetskoncept (innehållande rollbeskrivning, åtkomsträtt, begränsningar etc.) som ska kunna tillhanda hållas	Behörighet beskrivs och regleras genom biträdesinstruktion för migrering testladdning.	Nej, krav uppfyllt utan anmärkning
Åtkomsträttigheter *Priviligierade åtkomsträttigheter*	Följande principer ska följas: *Need-to-use/ Event-by-event* *Least privilege* *Segregation of duties* Guide: Inga rättigheter får ges till anonyma konton Tilldelning ska ske via dokumenterade och verifierade processer. Åtkomständringar ska loggas med periodisk loggranskning Åtkomsträttigheter som inte längre är lämpliga eller redundanta ska återkallas eller justeras	Just in time access för administratörer. Least privilege är en del av den behörighetsstruktur som finns. Segregation of duties sköts igenom systematiskt säkerhetsarbete. Månadsvis möte i SDV Security forum.	Nej, krav uppfyllt utan anmärkning
Säker autentisering	Åtkomst till information, och andra tillhörande tillgångar, ska kontrolleras av en säker inloggningsprocedur med lämpliga autentiseringsmetoder för att styrka användarens påstådda identitet.	Två-faktors autentisering genom bland annat Cisco duo.	Nej, krav uppfyllt utan anmärkning

4.1.3 SUMMERAD BEDÖMNING INOM EFTERLEVNAD OCH INFORMATIONSSÄKERHET

Beskriv den samlade bilden av tjänsteleverantörens förmåga att ge uppgifterna ett ändamålsenligt skydd. Beskriv om det finns tillräckligt med skäl för att uppgifterna ska anses hanteras rättsenligt och förutsebart.

Gör en summerade bedömningen om det är olämpligt/inte olämpligt att genomföra den föreslagna utlämningen för tekniska bearbetning och lagring hos tjänsteleverantören utifrån Informationssäkerhet.

Sammansatt bedömning av inhämtad information i avsnitt 4.1.1 och 4.1.2 är genomförd av SDV programmets Informationssäkerhets och Dataskyddssamordnare.

Efter noggrann granskning av de försäkringsmaterial som samlats in från Cerner Sverige AB, inklusive SOC2 Type 2, ISO 27000-certifikat och räckvidden för tillämpbarheten av ISO 27000-certifieringen, penetrationstestresultaten och GDPR Privacy Shield Framework-certifieringen, är bedömningen att leverantören är väl lämpad att skydda data som klassificeras som Sekretess och att man kan anse att OSL 10:2 Teknisk bearbetning och Teknisk Lagring stödjer den hantering som Region Skåne avtalat med Cerner Sverige AB för SDV och Millennium.

Leverantören har etablerat en omfattande uppsättning organisatoriska, logiska och fysiska kontroller i linje med branschstandarder. Deras efterlevnad av SOC2 Type 2-kraven, ISO 27000-certifikatet och GDPR Privacy Shield Framework-certifieringen visar på en hög nivå av datasäkerhet och följsamhet.
Dessa certifikat och insatser bekräftar leverantörens dedikation till att skydda konfidentiell information. Penetrationstestresultaten visar också att de aktivt identifierar och åtgärdar sårbarheter. GDPR Privacy Shield Framework-certifieringen visar att de följer europeiska dataskyddsförordningar och skyddar personlig data.

Slutsatsen är därför att Cerner Sverige AB inte kan anses vara Olämplig för det angivna utlämnandet och Region Skåne bör på dessa grunder kunna känna sig trygga med att Cerner Sverige AB som partner kan upprätthålla den sekretessnivå som avtalet innebär. Min rekommendation är härmed att godkänna denna lämplighetsbedömning och därmed tillåta den utökade datamängd - 20231109 Michael Rasmusson, Informationssäkerhet och Dataskydd SDV.

4.2 Fysisk säkerhet

Om utkontrakteringen innebär att teknisk bearbetning och/eller lagring av information ska ske utanför Region Skånes miljö och/eller lokaler behöver införandeprojektet ta fram en kravställning avseende fysisk säkerhet för leveransen.

4.2.1 BEDÖMNING AV FYSISK SKYDD AV TJÄNSTELEVERANTÖRENS DATAHALLAR

i

Gör en bedömning mot framtagen kravställning för fysisk säkert enligt riktlinjer från Område Säkerhet Beredskap Hållbarhet och Miljö. Granskning av leverantörens SOC2-rapport eller motsvarande bör genomföras om det är tillämpligt. Beakta placering, skalskydd, byggnationer, försörjning och andra faktorer kring fysiskt skydd utifrån informationsklassning för den tilltänkta utlämningen av information. Beakta även systematiskt säkerhetsarbete hos leverantören utifrån fysisk säkerhet

Summera bedömning av Fysiskt skydd av tjänsteleverantörens datahallar och gör en rekommendation om det är/inte är olämpligt att genomföra lagring i tjänsteleverantörens datahallar i samråd med Säkerhetschef/ Område Säkerhet Beredskap Hållbarhet och Miljö.

Primär datahall godkänd 2020-10-26 signerad Jan Svensson, verksamhetschef.

Den primära datahallen uppfyller Region Skånes kravställning och utlämnandet för teknisk bearbetning och lagring i den primära datorhallen kan därför inte anses vara olämplig

5 SAMMANSATT BEDÖMNING

5.1 Summering från delområden

Summera bedömningar gjorda per delområde till en sammansatt bedömning

Område	Bedömning
Tröskelvärde för utlämnade till leverantör	Utlämnandet för teknisk bearbetning och lagring är inte olämpligt
Informationssäkerhet	Utlämnandet för teknisk bearbetning och lagring är inte olämpligt
Fysisk säkerhet	Utlämnandet för teknisk bearbetning och lagring är inte olämpligt

5.2 Rekommendation till beslut

Gör en summerade bedömningen om det är olämpligt/inte olämpligt att genomföra den föreslagna utlämningen för tekniska bearbetning och lagring hos tjänsteleverantören.

Baserat på rekommendationerna från samtliga analyserade delområden rekommenderar SDV programmet att det fastställs att utlämnandet för teknisk bearbetning och lagring enligt avsnitt 3 och Konsekvensbedömning avseende dataskydd avsnitt 4-6 daterad 2023-10-16 inte är olämpligt