SPØRGSMÅL & SVAR – SIKKERHEDSBILAG

02.17 & 02.15

SPØRGSMÅL & SVAR:
VEDR SIKKERHEDSBILAGET B.3

01052025

Indholdsfortegnelse

Oftest stillede spørgsmål

Her finder du svar på en række forskellige spørgsmål, vedr. Sikkerhedsbilaget B.3 og krav til revisionserklæringer.

Bliver kravene til sikkerhed angivet i opgavebeskrivelsen ift. leverancen eller i forhold til de enkelte konsulenter?

Kravene i sikkerhedspakken gælder for hele leverancen. Kunden kan dog præcisere, at der gælder forskellige sikkerhedspakker, for særskilte leverancer. Det er vigtigt at eventuelt differentierede sikkerhedspakker er velbeskrevet i kundens opgavebeskrivelse, ellers vil revisor give anmærkning på at der er sikkerhedskrav der ikke er overholdt.

Det bemærkes, at svaret ikke er givet forhold til den enkelt konsulent, men (del)-leverancen, fordi de skal være velbeskrevet og gennemsigtigt hvad del-leverancen går ud på og den sikkerhedspakke som netop delleverancen er omfattet af.

Husk på, at det er kunden der vurderer hvilken sikkerhedspakke der er passende og nødvendig for en leverance og om det er hensigtsmæssigt at målrette forskellige sikkerhedspakker til del-leverancer.

Hvis der ikke er forskel på del-leverance og den del som en bestemt konsulent (underleverandør) har ansvar for, er der naturligvis sammenfald mellem underleverandør og den pågældende del-leverance, som er omfattet af en given sikkerhedspakke med sikkerhedskrav.

Hvornår skal ISAE 3000 type 1 fremsendes første gang?

Sendes senest 1/9 og skal dække kravene i sikkerhedsbilaget.

Revisionserklæringen kan være dateret før Rammeaftalens ikrafttræden, men skal dække de krav og kontroller der fremgår af sikkerhedsbilaget.

Er støttende enheder (ifm. Prækvalifikation) omfattet af krav til revisionserklæring?

Nej, så længe de alene er støttende enheder, der ikke udfører leverancer under 02.15 og 02.17 leveringskontrakt. Hvis en støttende enhed bliver udførende underleverandør, så er de dog alligevel omfattet af krav til revisionserklæring.

Skal hovedleverandørens revisionserklæring indeholde underleverandørerne?

Det er hovedleverandørens **revisors** opgave at inkludere underleverandørers revision i sin revisionserklæring. Dette udelukker ikke at underleverandøren har fået foretaget sin revision af en anden revisor, som hovedleverandørens revisor forholder sig til i sin samlede revision.

Konsortier kan vælge samlet revision af hele konsortiet (inkl. Underleverandører), eller særskilt revision af det enkelt konsortiemedlem (og dennes underleverandører). Hvornår og hvordan skal jeg håndtere problemer med leverandøren?

Spørgsmål angående gyldighedsperiode for revisionserklæring?

Revisionserklæring skal (naturligvis) angå perioden forud for at den fremsendes. For den første type 2- erklæring kan dette være for en periode der er kortere end 12 måneder. Efterfølgende type 2 erklæring må ikke have en udækket periode siden sidst fremsendte type 2 erklæring.

ISAE 3000 Type 1 erklæring -> Kan vi selv vælge skæringsdato, så længe den ligger i perioden fra 01.06.2025 til 31.08.2025?

Ja, I kan selv vælge skæringsdatoen for type 1 erklæring, og en type 1 erklæring kan principielt også være dateret før 01.06.2025

Skal den første Type 2 erklæring gælde fra skæringsdatoen fra Type 1?

Ja, hvis også revisor mener det giver mening, kan type 2 erklæringen dække en periode der er kortere end 12 måneder. Der må ikke være udækkede perioder.

I krav 4.c.4 er der en ufuldstændig sætning, kan I oplyse ordlyden af kravet?

4.c.4 Kravet i sin fulde længde:

Medarbejdere som har udvidede adgangsrettigheder skal:

• kun bruge deres udvidede adgangsrettigheder med et særligt bruger-id som ikke benyttes almindeligt dagligt arbejde

Således at kravet *opfyldes ved levering af Ydelser.*

Skal vi også dokumentere efterlevelsen af tillægspakkerne?

Revisorerklæringen skal dække hele sikkerhedsbilaget, dvs. både sikkerhedspakker og tillægspakker

Er det muligt i teknisk afklaringsmøde, efter dialog med kunden at ændre kundens valg af sikkerhedspakke?

Det vil forudsætte at ikke andre leverandører har afslået opgaven.

Hvad sker der hvis man ikke lever op til sikkerhedspakkerne?

Manglende efterlevelse af kravene til informationssikkerhed, herunder kravene i bilag B.3 jf. Rammeaftalens punkt 11.4 i Rammeaftalen, udgør væsentlig misligholdelse, såfremt forholdet ikke er afhjulpet senest 30 dage efter SKI's skriftlige påkrav, jf. punkt 15.2, litra j. En sådan misligholdelse kan berettige SKI til helt eller delvist at ophæve Rammeaftalen med fremadrettet

Skal erklæringen være udformet på dansk, eller må den gerne være på engelsk?

ISAE-erklæringerne må godt fremsendes på engelsk, i den forbindelse præcisere vigtigheden af at udfylde "Findingsarket" som skal vedlægges erklæringerne i udfyldt stand (det ark får I fremsendt så snart aftalen er trådt i kraft).

Uafhængigt af Leveringskontrakter skal vi aflevere ISAE3000 type 1 erklæring senest 1. september og igen 1 gang årligt ISAE3000 type 2)

Skal der leveres ydelser, der er omfattet af ISAE 3402, er den korrekte erklæring ISAE 3402.

Er det korrekt at i perioden fra 1. juni til 1. september gælder at den nødvendige ISAE-erklæring skal være på plads inden påbegyndelse af en opgave? -og således bekræftes 1 gang årligt?

Der skal leveres en erklæring, når leverandøren begynder at udføre handlinger i rollen som databehandler, og herefter hver 12. måned.

Kan I bekræfte at der ikke skal præsenteres noget i relation til de enkelte Leveringskontrakter?

Det fremgår af pkt. 11.4.3, at revisionserklæringen omfatter: ”…Leverandørens korrekte opfyldelse af Rammeaftalen og Leveringskontrakterne”.

Kan I bekræfte at erklæringer skal fremsendes til SKI og ikke til SKI’s kunder.

Det fremgår af Rammeaftalens pkt. 11.4.3, at ” ”Leverandøren skal fremsende revisionserklæringen til SKI og alle berørte Kunder, der leveres til i henhold til en Leveringskontrakt. Fremsendelsen kan gennemføres ved at Leverandøren stiller revisionserklæringen elektronisk til rådighed.”

Persondata 11.4.3 - Hvem afholder udgiften til denne erklæring? Og skal der laves en erklæring pr. leverings-kontrakt? Hvornår finder den anvendelse:

2) Persondata 11.4.3:

”Såfremt der i forbindelse med levering af 02.17 IT-konsulentydelser leveres ydelser, der er omfattet af ISAE 3402, fx i forhold til regnskabsbærende systemer, eller når ydelserne understøtter eller indgår til kundens regnskabsaflæggelse, er den korrekt erklæring ISAE 3402 el. tilsvarende.

I alle andre tilfælde er den korrekte erklæring ISAE (revised) 3000 el. tilsvarende.

Det fremgår af pkt. 11.4.3, at revisionserklæringen omfatter: ”…Leverandørens korrekte opfyldelse af Rammeaftalen og Leveringskontrakterne”. Og senere at ”herefter skal Leverandøren, så længe databehandlingstjenesterne leveres under en Leveringskontrakt, løbende levere revisionserklæringer af type 2…”

Og endelig:

”Leverandøren skal fremsende revisionserklæringen til SKI og alle berørte Kunder, der leveres til i henhold til en Leveringskontrakt. Fremsendelsen kan gennemføres ved at Leverandøren stiller revisionserklæringen elektronisk til rådighed.”

Da kravet om revisionserklæring følger af Rammeaftalen er der tale om en erklæring ift. leverandørens efterlevelse af kravene til databehandling iht. rammeaftalen og på kontrakter der indgås på rammeaftalen. Der skal leveres en erklæring, når leverandøren begynder at udføre handlinger i rollen som databehandler, og herefter hver 12. måned.

Der er dermed ikke tale om en erklæring pr. leveringskontrakt, men ift. rammeaftalen.

Det er leverandøren der afholder udgiften til erklæringen.
Bemærk at revisionserklæring i henhold til pkt. 11.4.3 ikke henviser ned i bilag B3. (Sikkerhedsbilaget).

Pkt. 11.4.3 handler alene om GDPR og der er ikke fra SKIs side i Pkt 11.4.3 givet specifikke krav til GDPR. For at overholde **databeskyttelsesforordningen (GDPR)**, skal en leverandør implementere en række **tekniske og organisatoriske foranstaltninger**, der sikrer et passende sikkerhedsniveau i forhold til de risici, der er forbundet med behandlingen af personoplysninger.
I pkt. 11.4.3.

Hvis kunden vælger Basis pakke, vil der så udløbe et krav om revisionserklæring?

Kundens B (Basis) er ikke omfattet af revisionserklæring. Kunden har dog mulighed for at lave sin egen audit i forhold til om kundens krav er overholdt af leverandøren, hvis Kunden finder det relevant. Revisor skal ikke foretage revision af krav B (Basis).

Krav: 2.a.1 screening af medarbejdere - hvilke medarbejdere er omfatter af screening?

Alle medarbejdere hos leverandøren, som direkte arbejder på eller er involveret i levering af ydelser til SKI-leveringskontrakten er omfattet af krav 2.a.1.

Det inkluderer:

- Konsulenter, der udfører arbejde for SKI-kunder.
- Projektledere, teknikere og andre med adgang til kundedata, systemer eller lokationer i forbindelse med opgaver under kontrakten.
- Midlertidigt personale eller underleverandører, hvis de indgår i leverancen.

Det inkluderer ikke:

- Øvrige medarbejdere hos leverandøren, som ikke har nogen rolle i leverancen (f.eks. administration, HR, marketing mv.), medmindre de får adgang til informationer eller systemer relateret til leverancen.

I praksis:
Når der i kontrakten står, at medarbejdere skal være screenet, er det et krav, at alle personer, der aktivt arbejder på leveringskontrakten (og dermed også konsulenter), skal være baggrundstjekket før arbejdet påbegyndes.

Det betyder, at både fastansatte medarbejdere hos leverandøren og eksterne konsulenter, som arbejder med at levere ydelser under SKI-kontrakten, omfattes af screening-kravet.

Sikkerhedskrav: 2.a.4 - Hvad betyder: Screeningsprocessen i henhold til krav-id 2.a.1 skal understøttes af eksterne agenturer, hvor en rolle kræver nationale sikkerhedsgodkendelser eller kontrol af strafferegistre?

Kravet kan uddybes således:

Med hensyn til : "...hvor en rolle kræver nationale sikkerhedsgodkendelser..."

Det henviser til særligt følsomme roller, hvor medarbejderen f.eks. skal:
Have adgang til klassificerede oplysninger (hemmelig, fortrolig eller til tjenestebrug).
Arbejde på kritisk infrastruktur, fx i forsvarssektoren, politi, eller visse offentlige myndigheder.

Leverandøren kan ikke selv foretage denne godkendelse. Den skal gennemføres af relevante myndigheder:

PET (Politiets Efterretningstjeneste) for civil sikkerhedsgodkendelse.
FE (Forsvarets Efterretningstjeneste) for militære eller forsvarsrelaterede formål.

Med hensyn til "...eller kontrol af strafferegistre"

Her handler det om at kunne dokumentere, at en medarbejder ikke har en straffeattest, der er uforenelig med det arbejde, vedkommende skal udføre.
Det kan være et krav i opgaver med personfølsomme oplysninger, økonomisk ansvar, mv.
Dette kan ske ved:

Politiets online selvbetjening, hvor medarbejderen henter og afleverer sin straffeattest (kræver samtykke).
Eller gennem et autoriseret firma, der indhenter og verificerer straffeattester som en del af en samlet baggrundstjekpakke.

Skal der foreligge en ISAE 3000 på alle tre niveauer, hhv. niveau 1, 2 og 3?

I 02.17 & 02.15, Rammeaftalens punkt 11.4.4 IT-sikkerhedsrevision, skal ISAE 3000 dække sikkerhedskravene i pakkerne 1, 2, 3 og tillægspakkerne.

Hvordan vil SKI sikre at revisorerklæringen og alle de andre sikkerhedsspørgsmål vil være opfyldt for alle i marked?

De krav, der er til sikkerhed, i sikkerhedsbilaget bilag B3, er underlagt revision. Revisionen omfatter Konsortiemedlemmer, hovedleverandør og anvendte underleverandører. Hvis revisor har anmærkninger i forhold til, at der er sikkerhedskrav der ikke er overholdt, følger SKI op, indtil forholdet er bragt i orden. SKI har mulighed for at pålægge bod (pr. tilfælde) og kan også opsige Rammeaftalen. Kunderne har indsigt i revisionsrapporterne. Herudover har en kunde i sin leveringskontrakt de almindelige misligholdelsesbeføjelser.

Med det nye kædeansvar vil alle underleverandører fremover skulle opfylde alle krav til NIS2, revisorerklæring og øvrige krav?

I forhold til hvad en underleverandør reelt kan overholde i forhold til sikkerhedskrav i konkrete leverancer og hvordan en hovedleverandørkan arbejde med dette, (se svaret under første spørgsmål) ” Kravene i sikkerhedspakken gælder for hele leverancen. Kunden kan præcisere, at der gælder forskellige sikkerhedspakker, for særskilte leverancer. Det er vigtigt at eventuelt differentierede sikkerhedspakker er velbeskrevet i kundens opgavebeskrivelse, ellers vil revisor give anmærkning på at der er sikkerhedskrav der ikke er overholdt…”

Det er i en teknisk afklaring af kundes tildeling, at hovedleverandøren kan afdække om hele leverancen eller blot dele af leverancen er omfattet af en sikkerhedspakke eller sikkerhedspakke med mere skærpede krav

Kan leverandørens nuværende processer og efterlevelse af krav i henhold til ISAE 3402 dække "tilsvarende" ifm. rammeaftalens krav i punkt 11.4.1 om at overholde informationssikkerhedsstandarden ISO/IEC 27001 eller tilsvarende?

Det vil forudsætte at jeres nuværende erklæring dækker kravene i sikkerhedsbilaget B.3.

Mere information

Find mere information om aftalen på ski.dk. Her finder du andre dokumenter, der kan hjælpe dig med at bruge aftalen.

Du er også altid velkommen til at kontakte SKI's kundeservice på telefon 33 42 70 00, hvis du har spørgsmål til aftalen.

Staten og Kommunernes Indkøbsservice
Montagehallen ▪ Pakkerivej 6 ▪ 2500 Valby ▪ Telefon +45 33 42 70 00