Bilag 13 - Sikkerhed

Vejledning til Tilbudsgiver vedrørende bilag 13 (Sikkerhed)

Dette bilag indeholder Kundens krav til bilag 13. Hele bilag 13 udgør Minimumskrav (MK).

Ovenstående afsnit slettes ved Kontraktens underskrift.

Indholdsfortegnelse

1. Indledning

Dette bilag indeholder Kundens krav til informationssikkerhed vedrørende Services.

I dette bilag beskriver Kunden kravene til informationssikkerheden hos den kommende Leverandør, herunder efterlevelse af standarder og lovgivning, organiseringen af informationssikkerhed hos Leverandøren, rapporteringer, sikkerhedstest, beredskabsplaner, revision, audit og krav til dokumentation.

Ligeledes beskriver Kunden specifikke sikkerhedskrav til Services.

2. Generelle krav til Leverandørens informationssikkerhed

2.1 Leverandørens efterlevelse af ISO27001 (MK)

Leverandøren skal i kontraktperioden efterleve og levere sine ydelser i overensstemmelse med seneste version af ISO27001 eller tilsvarende international anerkendt standard som fælles rammeværk for Leverandørens sikkerhedsstyring af informationssikkerhed.

2.2 Leverandørens ressourcer til arbejdet med informationssikkerhed (MK)

Leverandøren skal dedikere tilstrækkelige og erfarne ressourcer til arbejdet med Leverandørens informationssikkerhed. Såfremt der opstår tvivl om medarbejdernes kvalifikationer, er Kunden berettiget til vederlagsfrit at rekvirere dokumentation for disse medarbejderes kvalifikationer i forhold til arbejdet med informationssikkerhed. Erfaringer kan blandt andet dokumenteres med sikkerhedscertificeringer.

2.3 Informationssikkerhed i Leverandørens projektstyring (MK)

I forbindelse med større ændringer af den driftsmæssige opsætning skal Leverandøren sikre, at informationssikkerhed indgår i alle etaper af projektforløbet, herunder vurdering af sikkerhedsrisici og sikkerhedstemaer i projektets risikostyring. Kunden skal involveres og konsulteres i alle forhold, som kan påvirke sikkerheden af Services. Dokumentation for risikovurdering af ændringen og påvirkning på den samlede informationssikkerhed

skal fremsendes til Kunden, som kan stille krav om yderligere dokumentation, sikkerhedstest og ekstern vurdering og revision.

2.4 Kundens ændringer af krav i relation til informationssikkerheden (MK)

Kunden gennemfører løbende risikovurderinger af informationssikkerheden i Kundens projekter, processer og it-systemer og justerer på baggrund heraf løbende informationssikkerhedskravene til organisatoriske og tekniske sikkerhedskontroller til Kundens og Tilsluttede Parters aktuelle trusselsniveau. Ændringer af krav i relation til informationssikkerheden til Leverandøren vil blive håndteret i overensstemmelse med Bilag 12 (Ændringsprocedure)

2.5 Leverandørens ansvar for Servicens sikkerhed (MK)

Leverandøren skal løbende og for egne midler holde sig orienteret om Best Practice for at sikre Services mod brud på fortrolighed, integritet og tilgængelighed i overensstemmelse med det krævede sikkerhedsniveau, samt løbende sikre, at sikkerhedskontroller er tilstrækkelige, tidssvarende og relevante for Services.

2.6 Leverandørens forpligtelse til styring af underleverandører (MK)

Leverandøren er forpligtet til at indgå databehandleraftaler med dennes underleverandører.

Leverandøren er forpligtet til at sikre, at dennes underleverandører overholder sikkerhedskravene i indeværende bilag, databehandleraftale og kontrakt. Opfølgning kan blandt andet ske ved gennemførelse af revision og opfølgning på eventuelle observationer/revisionsanmærkninger.

Leverandøren er forpligtet til at sikre, at dennes underleverandørers medarbejdere har underskrevet en virksomhedsfortrolighedsaftale.

Leverandøren skal til en hver tid kunne dokumentere indgåelse af databehandleraftaler og fortrolighedsaftaler.

2.7 Leverandørens organisering af informationssikkerheden (MK)

Leverandøren skal iværksætte og opretholde de organisatoriske, administrative og informationssikkerhedsmæssige kontroller, som gælder ifølge databeskyttelseslovgivningen, til sikring af, at personoplysninger ikke hændeligt eller ulovligt tilintetgøres, fortabes, forringes, kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med databeskyttelsesforordningens og databeskyttelseslovens krav.

2.8 Leverandørens interne retningslinjer for informationssikkerhed (MK)

Leverandøren skal fastsætte og gennemføre interne retningslinjer for informationssikkerhed. Leverandøren skal have retningslinjer for organisatoriske forhold, logisk og fysisk sikring, herunder administration af adgangskontroller og autorisationsordninger samt kontrol af autorisationer.

2.9 Leverandørens instrukser for ind- og uddata og it-udstyr (MK)

Leverandøren skal sikre, at der er fastsat instrukser, som fastlægger ansvaret for og beskriver retningslinjer for behandling og destruktion af ind- og uddatamateriale.

Leverandøren skal ligeledes sikre, at der er fastsat instrukser, som fastlægger ansvaret for og beskriver retningslinjer for anvendt it-udstyr.

2.10 Leverandørens medarbejdersikkerhed og sikkerhedsfaglige niveau (MK)

Leverandøren skal sikre, at medarbejdere, der arbejder med Services, og som har adgang til Kundens og/elers Tilsluttede Parters data autoriseres forud for tildeling af rettigheder til Services.

Leverandøren skal underskrive en virksomhedsfortrolighedsaftale, som omfatter medarbejdere, der arbejder inden for rammerne af denne Kontrakt.

Personoplysninger må ikke videregives til uvedkommende, eller uden at der er indgået en databehandleraftale, eller anvendes til formål som ikke er specificeret i databehandleraftalen indgået med Leverandøren og Kunden. Alle personoplysninger skal behandles fortroligt.

Leverandøren skal stille tekniske specialister til rådighed, som har indgående kendskab til metoder til identifikation, tolkning og mitigering af sikkerhedsrelaterede hændelser. Såvel kendskabet til ISO 27001 eller tilsvarende og evnerne til at håndtere sikkerhedsrelaterede hændelser skal vedligeholdes i aftaleperioden, så den afspejler aktuelle sikkerhedsrisici, metoder og afhjælpninger.

Leverandøren er ansvarlig for at give den fornødne instruktion til medarbejdere, herunder af sikker håndtering af Kundens Service.

2.11 Adskillelse af Leverandørens udviklings- og testmiljø fra produktionsmiljø (MK)

Leverandørens udviklings- og testmiljøer skal være adskilte fra produktionsmiljøer, såvel Kundens som Leverandørens, for at sikre funktionsadskillelse mellem miljøerne og reducere risikoen for uautoriseret adgang til eller ændringer af produktionsmiljøet.

2.12 Brug af testdata (MK)

Leverandøren er ansvarlig for at anvende anonymiseret testdata, som ikke indeholder personhenførbare oplysninger.

2.13 Krav til sikker behandling og adgang til data (MK)

Leverandøren skal efterleve vejledninger og anbefalinger fra Datatilsynet, herunder vejledningen om behandlingssikkerhed og databeskyttelse gennem design og standardindstillinger. Leverandøren er herunder forpligtet til at konsultere Kunden og indhente skriftlig accept i alle forhold vedrørende Leverandørens ændring i behandling af Kundens data, jf. Bilag 14 (Databehandleraftale).

Leverandøren skal aktivt medvirke til at sikre mod uautoriseret og uvedkommendes adgang til Services – såvel fysisk som logisk, herunder også beskyttelse mod skadelig software – i henhold til internationalt anerkendte metoder og teknikker for adgangskontrol og personlig identifikation. Det skal som minimum omfatte etablering og review af firewalls og opsætning af sikkerhedsindstillinger i systemmiljøer, herunder vedligeholdelse af software/firmware og konfigurationer - samt i relevant omfang vedligeholdelse af anti-malware og antivirus.

Leverandøren er forpligtet til at beskytte mod uautoriseret og uvedkommendes adgang til og ændring af kildekode eller data.

2.14 Fysisk sikkerhed på Leverandørens lokationer (MK)

Leverandøren skal med udgangspunkt i en informationssikkerhedsrisikovurdering træffe de nødvendige foranstaltninger og kontroller til hindring af uvedkommendes adgang til Kundens og de Tilsluttede Parters data, herunder personoplysninger.

Leverandørens fysiske kontrolforanstaltninger skal omfatte, men ikke nødvendigvis være begrænset til, følgende områder:

- Fysisk adgangskontrol med det formål at sikre at kun autoriseret personer med et arbejdsbetinget behov har adgang til Services
- Logning af enhver adgang
- Overvågning af gæster
- Indbrudssikring, herunder alarmsystemer
- Logisk adskillelse mellem Leverandørens informationsbehandlingsudstyr og eventuelle service- og underleverandørers udstyr
- Serverrum, krydsfelter og tilsvarende områder skal på forsvarlig vis sikres mod miljømæssige hændelser som brand, vand, eksplosion og tilsvarende påvirkninger
- Et brandsikringsanlæg der bl.a. tager hensyn til omfanget af elektronisk udstyr
- Overvågning af pålæsningsområder, hvor offentligheden har adgang
- Udstyr skal placeres så risici for skader og uautoriseret adgang minimeres

Udstyr skal sikres mod forsyningssvigt på baggrund af en risikovurdering, der afdækker hvor kritisk udstyret er. Nødstrømsanlæg skal være dimensioneret til at kunne overtage driften af de services, som skal videreføres i tilfælde af strømsvigt. Eksempelvis et nødstrømsanlæg, der sikrer hurtig og korrekt nedlukning i tilfælde af strømsvigt.

Brud på ovenstående fysisk sikring vil blive betragtet som en sikkerhedsmæssig hændelse og skal som følge behandles som en sikkerhedsmæssig hændelse.

2.15 Transmission af oplysninger over internettet, herunder Sundhedsdatanettet og andre lukkede net (MK)

Leverandøren skal implementere foranstaltninger, som sikrer imod uvedkommende trafik og forhindrer adgang fra det åbne net til Leverandørens interne net.

For transmission af personoplysninger skal følgende opfyldes af Leverandøren:

- Alle personoplysninger skal behandles fortroligt. Transmission af personoplysninger af fortrolig karakter skal sikres ved forsvarlig kryptering. Kryptering skal ske på basis af en anerkendt krypteringsalgoritme.
- Sikkerhed for afsenders og modtagers identitet (autenticitet) skal sikres ved anvendelse af f.eks. digital signatur eller andre individuelle, fortrolige og stærke adgangskoder med 2-faktorautentifikation.

2.16 Overdragelse af data til ny leverandør (MK)

Leverandøren er forpligtet til at medvirke ved overdragelse af data til ny leverandør ved kontraktens ophør.

2.17 Sletning af data (MK)

Leverandøren er forpligtet til at slette Kundens og Tilsluttede Parters data, herunder personoplysninger, således at det ikke er muligt at genskabe data, når Leverandøren ikke længere har et arbejdsmæssigt behov for disse data, herunder i forbindelse med reparation, service eller destruktion af udstyr og medier. Sletning af data skal ske på en sådan måde, at de uigenkaldeligt fjernes fra alle lagringsmedier. Det anbefales, at der til overskrivning af datamedier anvendes et af de dertil beregnede specialprogrammer, som overskriver data flere gange i overensstemmelse med en anerkendt specifikation (f.eks. DOD 5220.22-M). Alternativt kan sletning af data gennemføres ved destruktion af anvendte lagringsmedier.

Alle Kundens data skal slettes ved Kontraktens ophør efter, at Kunden har bekræftet, at der må foretages sletning. Leverandøren er ansvarlig for at dokumentere, at sletning er sket i overensstemmelse med indeværende krav. Dette skal dokumenteres med en ledelseserklæring udstedt til Kunden. Papirdokumentation skal makuleres, når der ikke længere er behov for at opbevare personoplysninger. Makulering skal leve op til Dansk Standard DS/EN 15713.

Personoplysninger, der opbevares digitalt, skal slettes i overensstemmelse med ovenstående sletningskrav efter behandlingsbehovet er ophørt. Dette gælder ikke data, som er nødvendige at opbevare for at opfylde lovgivningsmæssige krav vedrørende regnskabsaflæggelse og revision. Disse oplysninger skal opbevares i overensstemmelse med gældende lovgivning for bogføring mm.

Leverandøren forpligter sig til at sikre, at data, der skal slettes, rent faktisk bliver slettet, og at sletningen forekommer for alle eventuelle kopier og backups af data.

Kunden kan til en hver tid kræve dokumentation for at retmæssig sletning eller destruktion er forekommet.

2.18 Funktionsadskillelse (MK)

Leverandøren skal opretholde funktionsadskillelse med det formål at opretholde den krævede integritet og fortrolighed og begrænse muligheden for fejlagtig eller bevidst misbrug af Leverandørens systemer og Services. Leverandøren skal have beskrevet, hvor og hvordan funktionsadskillelse bliver opretholdt.

2.19 Leverandørens egen adgangsstyring (MK)

Leverandøren skal have implementeret retningslinjer for adgangsstyring hos Leverandøren. Kunden kan til en hver tid bede om en kopi af Leverandørens fastsatte retningslinjer for adgangsstyring.

Kun de personer hos Leverandøren, som er autoriseret hertil, må have adgang til Kundens data, herunder personoplysninger. Der må ikke gives adgangsrettigheder til personoplysninger i videre omfang, end den pågældende bruger har et arbejdsbetinget behov for.

Leverandøren skal sikre, at al adgang for Leverandørens medarbejdere til Kundens og Tilsluttede Parters data og de systemer, hvor data lagres, er personhenførbar, blandt andet vha. personlige brugernavne og password.

Passwords skal konstrueres i overensstemmelse med best practice og skal udover at være personlige også være fortrolige. Leverandøren skal tilse, at adgangskontrollens sværhedsgrad afstemmes med fortroligheden og følsomheden af Kundens og Tilsluttede Parters data.

Administratorpasswords bør jf. Center for Cybersikkerheds anbefalinger være sikret med 2-faktor autentifikation.

Leverandøren skal implementere og dokumentere formelle procedurer for registrering og afmelding af brugere. I forbindelse med ophør, fratrædelse og omplacering til anden funktion skal Leverandøren sikre, at brugerens adgang blokeres.

Tilsvarende skal Leverandøren med jævne mellemrum og særligt i forbindelse med ændringer i ansættelsesforholdet gennemgå brugernes adgangsrettigheder. Brugeradgange til fortrolige personoplysninger skal revurderes halvårligt for at sikre, at autoriserede personer fortsat opfylder betingelserne for adgang. Dette skal dokumenteres hos Leverandøren.

Der skal implementeres sikkerhedskontroller for at sikre, at kun autoriserede brugere kan få adgang til behandling af personoplysninger.

Leverandøren skal sikre, at medarbejdere, der varetager brugersupport, kun tildeles de privilegier, og at der kun gives adgang til de dele af Services, der er nødvendige for at varetage opgaven.

Leverandøren skal træffe særlige foranstaltninger for at sikre, at der kun tildeles privilegier til anvendelse af ressourcer, der indeholder personoplysninger på administratorniveau, når der er et arbejdsbetinget behov.

Leverandøren skal til enhver tid kunne dokumentere, hvem der er autoriseret til at have adgang til data, hvilke privilegier, medarbejderne har fået tildelt i forhold til Services, hvilket adgangsniveau samt oplysninger om, hvem der som ressourceejer har tildelt privilegierne.

Hvis der behandles personoplysninger, skal Leverandøren hvert halve år fremsende dokumentation for gennemgang af brugerkonti og tildelte privilegier hos Leverandøren og eventuelle underleverandører.

Leverandøren skal løbende overvåge, om der sker ændringer i administratorers privilegier og adgangsniveau med henblik på at sikre, at der ikke uforvarende eller med forsæt sker en eskalation af privilegierne, som muliggør misbrug af privilegiet.

Der skal føres kontrol med afviste adgangsforsøg.

2.20 Yderlig sikkerhedstest (MK)

Leverandøren skal ved Kundens anmodning foretage yderligere sikkerhedstest af Services. Ved yderligere sikkerhedstest er Leverandøren berettiget til særskilt vederlag baseret på det faktiske timeforbrug med udgangspunkt i de timepriser, der er anført i Bilag 4A Tilbudsliste.

Leverandøren skal ligeledes ved Kundens anmodning give ekstern part adgang til at gennemføre de af Kunden krævede sikkerhedstest. Hvis leverandøren kan begrunde, hvorfor den valgte eksterne part ikke vil være hensigtsmæssig at anvende (f.eks. at der er tale om et konkurrenceforhold), skal Kunden så vidt muligt tage hensyn hertil. Den eksterne part skal underskrive en fortrolighedserklæring, før denne gives den beskrevne adgang.

2.21 Håndtering af advarsler fra Center for Cybersikkerhed (CFCS) og Sundhedssektorens decentrale Cyber- og informationssikkerhedsenhed (DCIS Sund) (MK)

Leverandøren er forpligtet til at håndtere advarsler fra CFCS samt DCIS, såfremt de er relevante for Servicens sikkerhed.

3. Logning

3.1 Logningskrav (MK)

Leverandøren skal etablere og vedligeholde logning på alt aktivt netværksudstyr, som anvendes for Servicen hos Leverandøren. Logningen skal omfatte en log over anvendelsen af privilegerede konti på aktivt netværksudstyr, herunder navn, start og slut tidspunkt, samt formålet med brugen af den privilegerede konto.

Leverandøren skal foretage overvågning af og reagere på uautoriserede forespørgsler i Leverandørens log, samt foretage overvågning af Leverandørens log i forhold til identificering af misbrug af Services og Kundens og Tilsluttede Parters data.

Alle logs skal beskyttes mod uautoriseret adgang og manipulation.

3.2 Efterlevelse af Center for Cybersikkerhed (CFCS) vejledning om god logning (MK)

Leverandøren skal som minimum efterleve vejledningen fra CFCS om logning.

3.3 Opbevaring af log (MK)

Leverandøren skal opbevare transaktionsloggen på Leverandørens adgang til personoplysninger i 2 år.

Driftslog uden personoplysninger opbevares i 5 år til brug ved opfølgning/undersøgelse af evt. ulovlige eller kriminelle handlinger.

3.4 Import af log til Kundens Logmanagementsystem (MK)

Loggen skal kunne eksporteres til Kundens Logmanagementsystem.

4. Backup af Kundens data

4.1 Backup (MK)

Backup skal opbevares på en anden lokation end Driftsmiljøet. Leverandøren skal sikre, at backups transmitteres og opbevares i overensstemmelserne med sikkerhedskravene i dette bilag.

Test af restore af data fra backuppen skal foretages mindst 2 gange årligt for at sikre at det er muligt at genskabe data fra backuppen.

5. Håndtering af sikkerhedshændelser og beredskabsplaner

5.1 Leverandørens rapportering af sikkerhedshændelser (MK)

Ved konstateret brud på informationssikkerheden eller ved mistanke herom skal Leverandøren rapportere dette til Kunden.

Leverandørens afrapportering af sikkerhedshændelser, herunder i hvilke tilfælde rapporteringen skal ske uden unødigt ophold, skal sammen med Leverandørens øvrige statusrapportering fastlægges sammen med Kunden ved Projektets opstart, jf. Bilag 9 Samarbejdsorganisation.

Dog skal Leverandøren, såfremt der konstateres brud på personoplysninger eller der er mistanke herom, altid uden unødigt ophold, og senest 24 timer efter konstatering, rapportere dette til Kunden.

Rapporteringen til Kunden skal ske i så rimelig tid, og med tilstrækkelig information, til at Kunden kan leve op til sine forpligtelser til rapportering af brud på personoplysninger jf. til alle tider gældende lovgivning.

Leverandøren skal sikre, at Leverandørens organisation og medarbejdere tager ved lære at indtrufne sikkerhedshændelser og anvender læren til at

etablere kontroller som reducerer risikoen for at en lignende sikkerhedshændelse indtræffer igen. Mitigerende tiltag og forbedringer som følge af sikkerhedshændelser skal rapporteres til kunden.

6. Rapportering, revision og audit af Leverandørens informationssikkerhedskontroller

6.1 Leverandørens rapportering om Services informationssikkerhed til Kunden (MK)

Leverandøren skal i rimeligt omfang deltage i møder med Kunden om Leverandørens efterlevelse af indeværende krav til informationssikkerhed. Frekvensen for møder om rapportering af Services informationssikkerhed skal fastlægges i Afklaringsfasen i samarbejde mellem Kunden og Leverandør.

Leverandøren skal afgive en månedlig statusrapport for Services informationssikkerhed. Indholdet af Leverandørens statusrapport skal fastlægges i Afklaringsfasen i samarbejde mellem Kunden og Leverandør.

6.2 Leverandørens kontrol med retningslinjer (MK)

Leverandøren skal føre kontrol med, at sikkerhedskrav overholdes. Leverandørens retningslinjer herfor skal revideres årligt for at sikre, at de til stadighed er tilstrækkelige og relevante.

Kunden kan til enhver tid kræve at få indblik i Leverandørens interne retningslinjer for informationssikkerhed.

6.3 Kundens informationssikkerhedsrisikovurdering af Servicen og Leverandøren (MK)

Leverandøren er forpligtet til, som minimum, årligt og i forbindelse med større ændringer, at medvirke til i samarbejde med Kunden, de dataansvarlige og/eller Kundens eller de dataansvarliges revisor at gennemføre og dokumentere en risikovurdering af den eller de services der leveres til kunden. Risikovurderingen skal baseres på en anerkendt metodik, som f.eks. ISO 27005 eller tilsvarende.

Leverandøren skal i den forbindelse vedligeholde en proces for løbende identifikation af sikkerhedsrisici.

Leverandøren er endvidere forpligtet til at deltage i og afgive oplysninger i forbindelse med Kundens konsekvensvurdering vedr. databeskyttelse og informationssikkerhedsrisikovurdering af Services og Leverandøren. I den henseende er Leverandøren forpligtet til i rimeligt omfang at stille ressourcer og oplysninger til rådighed for Kunden.

6.4 Leverandørens it-sikkerhedsauditering (MK)

Leverandørens eksterne revisor skal mindst 1 gang om året udarbejde en erklæring om kontrollernes design, implementering og operationelle effektivitet, baseret på enten revisionsstandarden ISAE3000 type 2 såfremt der behandles personoplysninger, eller ISAE 3402 (Generelle it-kontroller), såfremt der ikke behandles personoplysninger.

Leverandøren er forpligtet til at orientere Kunden om resultater fra egne interne og eksterne it-revisioner, it-audits og sikkerhedstest, hvor disse resultater omfatter Services.

6.5 Kundens it-sikkerhedsauditering (MK)

Leverandøren forpligtiger sig til at medvirke til, at Kundens eksterne revisor årligt gennemfører og afgiver en revisionserklæring baseret på revisionsstandarden ISAE 3000 type 2.

Leverandøren forpligter sig til at stille de nødvendige vidensressourcer til rådighed, som er nødvendige for at kunne gennemføre it-revisionen af Servicen.

Kunden kan desuden medtage en audit af de sikkerhedskrav som stilles i nærværende bilag og Underdatabehandleraftale.

6.6 Leverandørens afhjælpningspligt (MK)

Leverandøren skal uden ugrundet ophold foretage anbefalet afhjælpning af alle alvorlige og kritiske forhold påpeget af en it-revision, it-audit, risikovurdering og ved sikkerhedstest, samt forelægge og få accept fra Kunden for afhjælpningen af alle alvorlige og kritiske forhold.

Leverandøren skal endvidere sikre gentagelse af sikkerhedstest eller revisionstest, fra ekstern revisor, for at påvise effektivitet af de mitigerende tiltag.

Dokumentation herfor skal fremsendes til Kunden.

Leverandøren skal udbedre identificerede risici, som er påpeget af Kunden, i forbindelse med Kundens risikovurderinger af Services. Såfremt der er væsentlige omkostninger forbundet med risikohåndteringen, skal disse håndteres i overensstemmelse med ændringshåndtering jf. Bilag 12.