Informationssikkerhedsbilag til kontrakter i Beskæftigelses-, Integrations-, og Erhvervsforvaltningen

UDKAST

Henvisninger til 'Leverandøren' svarer til nedenstående oplysninger.

Leverandørens navn	
CVR-nummer	
Formål	
Kontraktansvarlig (Leverandør) Navn, titel, e-mail, telefon	

Nedenstående boks udfyldes af forvaltningen.

eDoc-sagsnummer	
Ansvarligt kontor	

UDKAST

Indhold

1. Formål og gyldighed 4
2. Definitioner 4
   2.1 Ordregiver 4
   2.2 Leverandøren 4
   2.3 Underleverandør 4
   2.4 Kontrakten 4
   2.5 Ydelsen 5
   2.6 Kritisk infrastruktur 5
   2.7 Kritiske værdioplysninger 5
   2.8 Sikkerhedshændelser 5
   2.9 Aktiver 5
   2.10 Fortrolighed 6
   2.11 Integritet 6
   2.12 Tilgængelighed 6
3. Krav til leverandøren 6
   3.1 Overholdelse af lovgivning, interne krav og fortrolighed 6
      3.1.1 Lovgivning og myndighedskrav (1) 7
      3.1.2 Ordregivers interne politikker og retningslinjer 7
      3.1.3 Fortrolighed og tavshedspligt 7
      3.1.4 Acceptabel brug af aktiver (Acceptable Use) 7
   3.2 Leverandørens organisatoriske og tekniske sikkerhedsforanstaltninger 8
      3.2.1 Styring af informationssikkerhed (Governance) 8
      3.2.2 Sikker udvikling og ændringsstyring (Change Management) **Fejl! Bogmærke er ikke defineret.**
      3.2.3 Aktivstyring (Asset Management) ..... **Fejl! Bogmærke er ikke defineret.**
      3.2.4 Funktionsadskillelse (Segregation of Duties) 8
      3.2.5 Fysisk sikkerhed og miljøsikring 8
      3.2.6 Netværkssikkerhed 8
      3.2.7 Dokumentation af efterlevelse ..... **Fejl! Bogmærke er ikke defineret.**
   3.3 Adgangsstyring og beskyttelse af information 8
      3.3.1 Principper for tildeling af rettigheder (Identity & Access Management) 8
      3.3.2 Styring af brugerlivscyklus ..... **Fejl! Bogmærke er ikke defineret.**
      3.3.3 Autentifikation og stærk adgangskontrol 9
      3.3.4 Beskyttelse af data (Kryptering) 9
      3.3.5 Logning og sporbarhed 9

UDKAST

3.4 Personale, kompetencer og baggrundskontrol 10
3.4.1 Faglige kvalifikationer og løbende kompetenceudvikling .... **Fejl! Bogmærke er ikke defineret.**
3.4.2 Sikkerhedsbevidsthed og træning 10
3.4.3 Baggrundskontrol af betroet personale ..... **Fejl! Bogmærke er ikke defineret.**
3.5 Risikostyring og håndtering af trusler 10
3.5.1 Risikostyringsproces ..... **Fejl! Bogmærke er ikke defineret.**
3.5.2 Specifikke risikoområder ..... **Fejl! Bogmærke er ikke defineret.**
3.5.3 Sårbarhedsstyring (Vulnerability Management) **Fejl! Bogmærke er ikke defineret.**
3.5.4 Rapportering og kommunikation ..... **Fejl! Bogmærke er ikke defineret.**
3.6 Hændelseshåndtering og rapportering 10
3.6.1 Underretningspligt og tidsfrister 10
3.6.2 Håndtering af hændelsen 11
3.6.3 Bistand og samarbejde 11
3.6.4 Omkostninger 11
3.7 Kontinuitet, backup og beredskab 12
3.7.1 Forretningskontinuitetsstyring (Business Continuity Management - BCM) ..... **Fejl! Bogmærke er ikke defineret.**
3.7.2 Katastrofegenoprettelse (Disaster Recovery - DR) ..... **Fejl! Bogmærke er ikke defineret.**
3.7.3 Backup og genetablering ..... **Fejl! Bogmærke er ikke defineret.**
3.7.4 Test og gennemgang ..... **Fejl! Bogmærke er ikke defineret.**
3.8 Underleverandører og forsyningskæde 12
3.8.1 Godkendelse af underleverandører 12
3.8.2 Nedlukning af krav (Flow-down requirements) 12
3.8.3 Tilsyn og audit af underleverandører 12
3.8.4 Forsyningskædesikkerhed og sporbarhed ..... **Fejl! Bogmærke er ikke defineret.**
3.8.5 Hændelsesrapportering i forsyningskæden 12
3.9 Tilsyn og revision 13
3.9.1 Form og omfang af tilsyn og revision 13
3.9.2 Leverandørens medvirken 13
3.9.3 Anvendelse af tredjepartsrevisorerklæringer .... **Fejl! Bogmærke er ikke defineret.**
3.9.4 Rapportering af fund og afhjælpning ..... **Fejl! Bogmærke er ikke defineret.**
3.9.5 Omkostninger ved tilsyn og revision 13
3.10 Ophør af kontrakt 13
3.10.1 Sletning, destruktion eller tilbagelevering af data 14

UDKAST

3.10.2 Krav om ingen kopier 14
3.10.3 Bekræftelse på sletning/destruktion 14
3.10.4 Omkostninger 14
3.10.5 Tilsyn og audit ved ophør 14

UDKAST

Formål og gyldighed

Dette bilag fastlægger Leverandørens forpligtelser vedrørende informationssikkerhed i forbindelse med opfyldelse af Kontrakten.

Bilaget udgør en integreret del af Kontrakten og har til formål at sikre, at Leverandørens ydelser leveres i overensstemmelse med gældende krav til informationssikkerhed, herunder men ikke begrænset til:

- Lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau (NIS2-loven), i det omfang denne finder anvendelse[1].
- Implementering af Cybersikkerhedsforanstaltninger, kapitel 4 (Styrelsen for Samfundssikkerheds vejledning)[2].
- Relevante foranstaltninger i ISO/IEC 27002:2022, herunder specielt A.5.19, A.5.20, A.5.21 og A.8.30.

OBS: Såfremt der indgås en selvstændig Databehandleraftale mellem parterne, vil dette bilag være subsidiært Databehandleraftalens krav til sikkerhedsforanstaltninger.

Definitioner

Ordregiver

Beskæftigelses-, Integrations- og Erhvervsforvaltningen, der indkøber Ydelsen. I relation til persondatalovgivningen agerer Ordregiver typisk som *Dataansvarlig*.

Leverandøren

Den virksomhed eller juridiske enhed, med hvem Ordregiver har indgået Kontrakten. I relation til persondatalovgivningen agerer Leverandøren typisk som *Databehandler*, såfremt denne behandler personoplysninger på vegne af Ordregiver.

Underleverandør

Enhver tredjepart, som Leverandøren benytter til at opfylde dele af sine forpligtelser i henhold til Kontrakten.

Kontrakten

Den, mellem parterne, indgåede hovedaftale om levering af Ydelsen, inklusive alle tilhørende bilag, herunder dette informationssikkerhedsbilag.

UDKAST

[1] https://www.retsinformation.dk/eli/lta/2025/434

[2] https://samsik.dk/wp-content/uploads/2025/08/Vejledning-til-implementering-af-cybersikkerhedsforanstaltninger.pdf

Ydelsen

De produkter, systemer, konsulentydelser eller services, som Leverandøren ifølge Kontrakten skal levere til Ordregiver.

Kritisk infrastruktur

Ved kritisk infrastruktur forstås systemer, netværk, tjenester eller tekniske komponenter, som er nødvendige for Ordregivers drift eller levering af ydelser, og hvor kompromittering, nedbrud eller utilgængelighed kan medføre væsentlig driftsforstyrrelse eller sikkerhedsrisiko.

Kritiske værdioplysninger

Ved kritiske værdioplysninger forstås information eller data, som er væsentlige for Ordregivers drift, sikkerhed eller forretningsmæssige aktiviteter, og hvor uautoriseret adgang, ændring, tab eller offentliggørelse kan medføre væsentlig skade, driftsforstyrrelse eller økonomisk tab.

Sikkerhedshændelser

En informationssikkerhedshændelse defineres som enhver hændelse, der medfører eller potentielt kan medføre brud på fortrolighed, integritet eller tilgængelighed af Ordregivers data, systemer eller tjenester, herunder hændelige eller ulovlige handlinger, der fører til tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til data eller systemer. Dette inkluderer, men er ikke begrænset til, malware-angreb, uautoriseret adgang, databrud, phishing-kampagner, systemnedbrud forårsaget af sikkerhedsbrister og leverandørkædeangreb.

Aktiver

Et aktiv defineres som enhver ressource, der har værdi for Leverancen, og som derfor kræver beskyttelse for at sikre den fortsatte drift og troværdighed. Aktiver udgør fundamentet for organisationens virke, og en kompromittering af disse kan medføre tab, driftsforstyrrelser eller skade på omdømmet.

Aktiver kan kategoriseres bredt og kan for eksempel være (listen er ikke udtømmende):

- **Tekniske aktiver:**
  - Software, herunder it-systemer, AI-funktioner og robotter
  - Databaser og andre lagringssystemer
  - Virtuelle maskiner og cloudtjenester
  - Computere, tablets og telefoner
  - Alarm- og adgangssystemer
  - Servere, krydsfelter og UPS'er (nødstrøm)
- **Organisatoriske aktiver:**
  - Software, herunder it-systemer, AI-funktioner og robotter
  - Databaser og andre lagringssystemer
  - Virtuelle maskiner og cloudtjenester
  - Computere, tablets og telefoner

UDKAST

    - Alarm- og adgangssystemer
    - Servere, krydsfelter og UPS'er (nødstrøm)
- **Fysiske aktiver:**
    - Kontorfaciliteter og bygninger
    - Indgangsfaciliteter og sikring heraf
    - Borgerområder og betjeningszoner

Fortrolighed

Fortrolighed handler om at beskytte data mod uautoriseret indsigt og sikre, at information kun er tilgængelig for de personer, systemer eller processer, der har en legitim ret og autorisation til at tilgå den. Formålet med dette princip er at holde personlige og følsomme oplysninger private, så de kun kan ses af dem, der ejer dem eller skal bruge dem i deres arbejde. I praksis opnås dette blandt andet gennem kryptering og adgangsstyring, der forhindrer, at for eksempel personoplysninger eller kommunens værdidata falder i forkerte hænder.

Integritet

Integritet sikrer, at informationen er korrekt, komplet og troværdig, samt at den ikke er blevet ændret utilsigtet eller af uautoriserede parter. Det centrale formål er at garantere dataens nøjagtighed og pålidelighed, så man altid kan stole på, at systemerne leverer valid information, og at der for eksempel ikke er manipuleret med logfiler. Det handler om at opretholde dataens kvalitet og sikre, at ændringer – hvad enten de er tilsigtede eller utilsigtede – ikke kompromitterer informationens gyldighed.

Tilgængelighed

Tilgængelighed garanterer, at autoriserede brugere har adgang til information og tilhørende systemer, når de har brug for det. Formålet er at sikre oppetid og driftsstabilitet gennem robuste systemer, backup-løsninger og beredskabsplaner. Derved kan organisationen opretholde centrale funktioner og fortsætte driften, selv i tilfælde af tekniske fejl, strømsvigt eller cyberangreb.

Krav til leverandøren

Leverandøren garanterer, at der opretholdes et højt informationssikkerhedsniveau gennem hele kontraktperioden. Sikkerhedsniveauet skal løbende tilpasses det aktuelle trusselsbillede samt den teknologiske udvikling. Leverandøren er forpligtet til proaktivt at sikre Ordregivers data og systemer mod kompromittering af fortrolighed, integritet og tilgængelighed.

Overholdelse af lovgivning, interne krav og fortrolighed

Leverandøren er forpligtet til at sikre, at leverancen og den tilhørende behandling af data sker i fuld overensstemmelse med gældende lovgivning, rammeværk samt Ordregivers interne regler.

UDKAST

Lovgivning og myndighedskrav

Leverandøren skal overholde al relevant dansk og EU-lovgivning, herunder men ikke begrænset til:

1. **Databeskyttelsesforordningen (GDPR)** og **Databeskyttelsesloven**, såfremt løsningen behandler personoplysninger.
2. **NIS2-lovgivningen** (Lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau).
3. **Forvaltningsloven** og **Offentlighedsloven**, i det omfang Leverandøren udfører opgaver, der indebærer forvaltningsmyndighed eller behandling af sager på vegne af Ordregiver.
4. Relevant faglovgivning.

Leverandøren skal proaktivt holde sig orienteret om relevante udviklinger inden for informationssikkerhed, herunder ændret lovgivning, anerkendte standarder, det aktuelle trusselsbillede og teknologisk udvikling, der kan påvirke Ydelsen og dennes forsyningskæde. Nødvendige sikkerhedsforanstaltninger, der udspringer heraf, og som omfatter både Leverandørens egne operationer og eventuelle underleverandørers ydelser, skal implementeres uden meromkostning for Ordregiver. Leverandøren er forpligtet til at orientere Ordregiver forud for ændringer, der kan påvirke Ydelsens informationssikkerhed, og skal derudover som minimum opretholde det sikkerhedsniveau, der er beskrevet i dette Bilag.

Ordregivers interne politikker og retningslinjer

Leverandøren og dennes medarbejdere skal respektere og efterleve Ordregivers gældende politikker for informationssikkerhed og IT-anvendelse.

1. Ordregiver fremsender relevante politikker og retningslinjer forud for kontraktindgåelse.
2. Leverandøren er ansvarlig for at instruere sit personale i disse regler, inden adgang etableres.

Fortrolighed og tavshedspligt

Leverandøren skal iagttage ubetinget tavshed med hensyn til alle oplysninger vedrørende Ordregivers forhold, herunder forretningshemmeligheder, fortrolige data og personoplysninger, som Leverandøren måtte få kendskab til under kontraktforholdet.

1. Tavshedspligten er tidsubegrænset og gælder også efter Kontraktens ophør.
2. Leverandøren skal sikre, at alle medarbejdere og underleverandører, der arbejder på Kontrakten, har underskrevet en fortrolighedserklæring eller er underlagt lovbestemt tavshedspligt.

Acceptabel brug af aktiver (Acceptable Use)

Leverandøren må alene anvende Ordregivers informationer, data, licenser og IT-udstyr til opfyldelse af Kontrakten. Enhver anden brug, herunder kommerciel udnyttelse af data (for eksempel til træning af AI-modeller, statistik eller videresalg), er strengt forbudt uden eksplicit skriftlig aftale, som allonge til kontrakten.

UDKAST

Leverandørens organisatoriske og tekniske sikkerhedsforanstaltninger

Leverandøren skal etablere, implementere, dokumentere og vedligeholde passende organisatoriske og tekniske foranstaltninger baseret på anerkendte internationale standarder (for eksempel ISO/IEC 27001, ISO/IEC 27002 eller NIST). Foranstaltningerne skal sikre et sikkerhedsniveau, der står mål med risikoen ved behandlingen og de leverede ydelser.

Leverandørens foranstaltninger skal som minimum omfatte følgende områder:

Styring af informationssikkerhed (Governance)

Leverandøren skal have en forankret sikkerhedsorganisation, det vil sige en systematiseret tilgang til sikkerhed med definerede roller og ansvar. Der skal foreligge en opdateret sikkerhedspolitik, som er godkendt af ledelsen og kommunikeret til alle relevante medarbejdere.

Funktionsadskillelse (Segregation of Duties)

Hvor det er praktisk muligt, skal Leverandøren implementere funktionsadskillelse for at reducere risikoen for fejl og misbrug. Det betyder, at kritiske funktioner (blandt andet udvikling og drift eller anmodning og godkendelse af rettigheder) ikke bør udføres af samme person.

Fysisk sikkerhed og miljøsikring

Leverandøren skal sikre, at faciliteter, hvorfra Ydelsen leveres eller data opbevares (datacentre, serverrum, kontorer), er beskyttet mod uautoriseret adgang, brand, vandskade og strømsvigt. Dette inkluderer:

1. Fysisk adgangskontrol (nøglekort, alarmer).
2. Miljøkontrol (køling, brandslukning).
3. Sikring af strømforsyning (UPS/nødstrøm).

Netværkssikkerhed

Leverandøren skal anvende anerkendte teknologier til beskyttelse af netværk, herunder segmentering af netværk, anvendelse af firewalls og beskyttelse mod DDoS-angreb.

Adgangsstyring og beskyttelse af information

Leverandøren skal sikre, at adgang til Ordregivers informationer, data, systemer og øvrige aktiver begrænses til det absolut nødvendige omfang, samt at data beskyttes effektivt gennem hele deres livscyklus.

Principper for tildeling af rettigheder (Identity & Access Management)

Leverandøren skal styre adgange efter følgende principper:

UDKAST

1. **Need-to-know:** Adgang gives kun til medarbejdere, der har et arbejdsmæssigt behov for adgangen for at kunne løse opgaven.
2. **Least Privilege:** Brugeren tildeles kun de rettigheder, der er strengt nødvendige (for eksempel læseadgang frem for skriveadgang), og aldrig administratorrettigheder, medmindre det er påkrævet.
3. **Personlige brugere:** Alle adgange skal være personlige og unikt identificerbare. Brug af fælleskonti (for eksempel "admin" eller "root" delt mellem flere personer) er ikke tilladt, medmindre det undtagelsesvist og tidsbegrænset er teknisk nødvendigt og ledsaget af streng, kompenserende overvågning.

Autentifikation og stærk adgangskontrol

1. Leverandøren skal anvende Multi-Faktor Autentifikation (MFA) ved al fjernadgang (remote access) til systemer, der behandler Ordregivers data, samt ved al adgang til privilegerede konti (administratoradgang).
2. Der skal håndhæves en stærk adgangskodepolitik (krav til længde, kompleksitet og udløb), såfremt MFA undtagelsesvist ikke kan anvendes.

Beskyttelse af data (Kryptering)

Leverandøren skal anvende effektiv kryptering af kommunens værdidata og personoplysninger under transport (in transit) og i hvile (at rest). Niveauet af kryptering skal på baggrund af risikovurderingen være passende for at effektivt forhindre uvedkommende i at få adgang til personoplysninger.

Følsomme data og personoplysninger skal opbevares krypteret i databaser, på servere, backups samt på mobile enheder (laptops, tablets og telefoner).

Kryptering af transportlaget (TLS) skal som minimum være TLS 1.2 med opdaterede cyber suites. Alle ældre TLS-protokoller skal være slået fra.

Leverandøren skal definere og implementere regler for effektiv anvendelse af kryptografi, herunder administration af krypteringsnøgler. Krypteringsnøgler skal opbevares sikkert og adskilt fra de data, de beskytter.

Al datatrafik mellem medarbejderens hjemmearbejdsplads og Leverandørens netværk skal foregå via krypterede kommunikationsforbindelser. Dette sikrer, at information er beskyttet mod uautoriseret aflytning under transit og dermed opretholder datafortroligheden.

Leverandøren er forpligtet til at sikre, at al fjernadgang for både egne og Ordregivers medarbejdere til Leverandørens netværk udelukkende sker via en Virtual Private Network (VPN) forbindelse. Adgangen til denne VPN-forbindelse skal være beskyttet med flerfaktorautentifikation (MFA), der kræver anvendelse af mere end én form for identitetsbekræftelse. Dette krav skal sikre mod uautoriseret adgang, selv i tilfælde af kompromitterede adgangskoder.

Logning og sporbarhed

For at sikre opklaring ved sikkerhedshændelser og misbrug skal Leverandøren logge aktiviteter i systemerne.

UDKAST

1. **Hvad skal logges:** Som minimum logges alle login-forsøg (både succesfulde og fejlede), tildeling af rettigheder, samt adgang til og ændring/sletning af følsomme data.
2. **Beskyttelse af logfiler:** Logfiler skal beskyttes mod sletning og manipulation. De skal opbevares i en periode på minimum 6 måneder (eller længere, hvis lovgivningen kræver det), hvorefter de skal slettes.
3. **Gennemgang:** Leverandøren skal have procedurer for regelmæssig gennemgang af logfiler for at identificere mistænkelig adfærd.

Personale, kompetencer og baggrundskontrol

Leverandøren skal sikre, at alt personale, der er involveret i leverancen af Ydelsen, er pålideligt, kompetent og informeret om gældende sikkerhedskrav og forpligtelser.

Sikkerhedsbevidsthed og træning

Leverandøren skal etablere og opretholde et program for sikkerhedsbevidsthed og -træning, der som minimum omfatter:

1. **Introduktionstræning:** Obligatorisk sikkerhedstræning ved ansættelse og inden medarbejdere får adgang til Ordregivers data eller systemer.
2. **Løbende awareness-træning:** Årlig, obligatorisk træning for alt relevant personale, der dækker emner som informationssikkerhedspolitik, phishing, social engineering, håndtering af personoplysninger og rapportering af sikkerhedshændelser.
3. **Dokumentation:** Leverandøren skal kunne dokumentere, at relevant personale har gennemført den påkrævede træning.

Risikostyring og håndtering af trusler

Leverandøren skal etablere, implementere og vedligeholde en systematisk og dokumenteret proces for risikostyring af informationssikkerhed i relation til de ydelser, der leveres til Ordregiver. Dette skal sikre, at relevante risici identificeres, vurderes og behandles proaktivt.

Hændelseshåndtering og rapportering

Leverandøren skal have etableret en robust, dokumenteret og testet proces for håndtering af informationssikkerhedshændelser (Incident Management), som er i stand til at identificere, vurdere, afhjælpe og forebygge gentagelse af sikkerhedshændelser.

Underretningspligt og tidsfrister

Leverandøren skal proaktivt underrette Ordregiver om alle sikkerhedshændelser, der påvirker, potentielt kan påvirke eller på anden måde berører Ordregivers data, drift og ydelse, uanset omfang. Underretning skal ske via e-mail til systemejer på det pågældende it-system og Informationssikkerhedskoordinator i BIF.

Vær opmærksom på, at der i forbindelse med brud på persondatasikkerheden, følger særskilte underretningsregler, som er nævnt i en eventuel Databehandleraftale.

Såfremt der er tale om sikkerhedshændelser jævnfør NIS 2, skal følgende tidsfrister overholdes:

UDKAST

1. **Første underretning (varsel):** Senest **24 timer** efter, at Leverandøren er blevet opmærksom på hændelsen. Denne underretning skal som minimum angive hændelsens karakter og Leverandørens første vurdering af dens potentielle alvorlighed, årsag og sandsynlige konsekvenser for Ydelsen og Ordregiver.
2. **Opdateret underretning:** Senest **72 timer** efter den første underretning, og efter behov herefter. Denne skal give en status på hændelsen, yderligere oplysninger om årsag, konsekvenser, iværksatte afhjælpende foranstaltninger, og eventuel information om, hvorvidt hændelsen er anmeldt til relevante myndigheder.
3. **Endelig underretning:** Ved hændelsens afslutning eller senest **én måned** efter den første underretning, skal Leverandøren fremsende en endelig rapport med en detaljeret beskrivelse af hændelsen, dens årsag, de endelige konsekvenser, alle iværksatte foranstaltninger og planer for at forhindre gentagelse.

Håndtering af hændelsen

Leverandøren skal have en klar og dokumenteret proces for håndtering af sikkerhedshændelser, der omfatter:

1. **Identifikation og analyse:** Hurtig identifikation, analyse og klassificering af hændelsen, herunder vurdering af omfang og konsekvens.
2. **Inddæmning (Containment):** Isolering af hændelsen for at begrænse dens spredning og skade.
3. **Udryddelse (Eradication):** Fjernelse af den primære årsag til hændelsen.
4. **Genopretning (Recovery):** Gendannelse af berørte systemer og data, så de igen er operationelle og sikre.
5. **Post-incident analyse:** Efter hændelsen skal Leverandøren gennemføre en grundig analyse (Root Cause Analysis) for at identificere årsagen og de underliggende sårbarheder, samt udarbejde en plan for at forhindre lignende hændelser i fremtiden.

Bistand og samarbejde

Leverandøren skal yde fuld bistand og samarbejde med Ordregiver i forbindelse med håndtering af sikkerhedshændelser, herunder:

1. **Informationsdeling:** Stille alle relevante oplysninger, logfiler og teknisk ekspertise til rådighed for Ordregiver eller en af Ordregiver udpeget tredjepart.
2. **Deltagelse i kriseteams:** På anmodning deltage i møder og koordineringsindsatser med Ordregivers sikkerhedspersonale.
3. **Korrektive handlinger:** Efterleve Ordregivers anvisninger vedrørende afhjælpende foranstaltninger, hvor hændelsen påvirker Ordregivers data eller systemer.

Omkostninger

Såfremt en sikkerhedshændelse skyldes Leverandørens fejl, forsømmelse eller manglende overholdelse af Kontraktens bestemmelser, afholdes alle omkostninger til håndtering af hændelsen (herunder Ordregivers egne og eksterne omkostninger) af Leverandøren.

UDKAST

Kontinuitet, backup og beredskab

Leverandøren skal etablere, implementere, dokumentere og regelmæssigt teste passende foranstaltninger for at sikre forretningskontinuitet (Business Continuity) og genopretning (Disaster Recovery), der minimerer afbrydelser i leverancen af Ydelsen i tilfælde af større hændelser, naturkatastrofer eller sikkerhedsbrud..

Underleverandører og forsyningskæde

Leverandøren er og forbliver fuldt ud ansvarlig for opfyldelsen af Kontrakten og alle forpligtelser i dette Bilag, uanset om Leverandøren benytter underleverandører til at levere dele af Ydelsen.

Godkendelse af underleverandører

1. Leverandøren skal oplyse Ordregiver om alle underleverandører, der agerer som databehandlere eller behandler Ordregivers data og/eller har adgang til kritiske systemer i forbindelse med Ydelsen, inden de tages i brug.
2. Ordregiver skal godkende alle nye underleverandører, der har adgang til ordregivers data eller varetager kritiske funktioner. Leverandøren skal fremlægge den nødvendige dokumentation for at Ordregiver kan træffe en informeret beslutning. Leverandøren er forpligtet til at orientere Ordregiver forud for ændringer leverandørlandskabet.
3. En liste over godkendte underleverandører, der anvendes til levering af Ydelsen, skal være en del af Kontrakten eller vedlægges som bilag.

Nedlukning af krav (Flow-down requirements)

Leverandøren skal sikre, at samtlige krav fastsat i dette Bilag, samt alle relevante forpligtelser fra hovedkontrakten, nedarves kontraktuelt til alle underleverandører, der medvirker til opfyldelsen af Ydelsen. Dette gælder for hele underleverandørkæden.

1. Leverandøren skal indgå skriftlige aftaler med sine underleverandører, der pålægger dem tilsvarende forpligtelser vedrørende informationssikkerhed og databeskyttelse.
2. Leverandøren skal på anmodning kunne fremlægge disse aftaler for Ordregiver.

Tilsyn og audit af underleverandører

Leverandøren er ansvarlig for at føre løbende tilsyn med sine underleverandørers efterlevelse af de nedarvede sikkerhedskrav.

1. Dette tilsyn kan inkludere gennemgang af underleverandørens sikkerhedsdokumentation, auditrapporter (for eksempel ISAE 3402/3000), interne procedurer og eventuelt fysiske audits.
2. Ordregiver har, gennem Leverandøren, ret til at foretage tilsyn hos underleverandører i samme omfang som hos Leverandøren selv.

Hændelsesrapportering i forsyningskæden

Leverandøren skal omgående informere Ordregiver, hvis Leverandøren bliver opmærksom på en informationssikkerhedshændelse hos en underleverandør, der påvirker eller potentielt

UDKAST

kan påvirke Ydelsen, Ordregivers data eller drift. Rapporteringen skal følge tidsfristerne og proceduren angivet i afsnit 0, side 10.

Tilsyn og revision

Ordregiver er berettiget til at føre tilsyn med og gennemføre revision af Leverandørens efterlevelse af Kontrakten, herunder specielt bestemmelserne i dette Bilag. Formålet er at sikre et tilstrækkeligt informationssikkerhedsniveau og fuld overholdelse af gældende lovgivning.

Form og omfang af tilsyn og revision

Tilsyn og revision kan foregå som:

1. **Dokumentgennemgang:** Ordregiver kan anmode om at modtage og gennemgå relevant dokumentation fra Leverandøren, herunder sikkerhedspolitikker, procedurer, risikovurderinger, auditrapporter, logfiler og bevis for træning.
2. **Fysisk revision:** Ordregiver (eller en af Ordregiver udpeget uafhængig tredjepart) kan gennemføre en fysisk revision på Leverandørens faciliteter, hvorfra Ydelsen leveres. Dette vil typisk ske efter skriftligt varsel på minimum 14 arbejdsdage.
3. **Teknisk verifikation:** I særlige tilfælde, og efter forudgående aftale, kan Ordregiver anmode om adgang til at verificere tekniske sikkerhedsforanstaltninger.

Leverandørens medvirken

Leverandøren skal uden ugrundet ophold og vederlagsfrit:

1. Stille relevant dokumentation til rådighed for Ordregiver i forbindelse med tilsyn og audit.
2. Give Ordregiver (eller dennes repræsentant) adgang til relevante faciliteter og personale i overensstemmelse med de aftalte rammer for revision.
3. Bidrage med den nødvendige faglige ekspertise for at besvare spørgsmål og klarlægge forhold af betydning for revisionen.

Omkostninger ved tilsyn og revision

1. Almindeligt tilsyn og gennemgang af dokumentation afholdes af Ordregiver.
2. Såfremt en fysisk revision afdækker væsentlige afvigelser eller mangler i Leverandørens overholdelse af dette Bilag, afholdes alle omkostninger forbundet med revisionen (herunder Ordregivers egne omkostninger og omkostninger til eventuel ekstern revisor) af Leverandøren.
3. Endvidere afholdes omkostninger til eventuel opfølgende revision af Leverandøren, hvis dette er nødvendigt for at verificere afhjælpning af væsentlige mangler.

Ophør af kontrakt

Ved Kontraktens ophør, uanset årsag, skal Leverandøren sikre en struktureret og sikker afvikling af alle opgaver og forhold relateret til Ordregivers data og systemer.

UDKAST

Sletning, destruktion eller tilbagelevering af data

Leverandøren skal, i henhold til Ordregivers anvisninger og senest inden 30 kalenderdage efter Kontraktens ophør:

1. **Tilbagelevere** alle Ordregivers data i et aftalt, struktureret og almindeligt anvendt format til Ordregiver.
2. **Slette** alle Ordregivers data og kopier heraf permanent fra alle systemer (inklusive test-, udviklings- og backup-miljøer), fysiske lagermedier og hos eventuelle underleverandører. Sletning skal ske på en måde, der gør dataene irreversibelt/uigenkaldeligt utilgængelige og uanvendelige. Sletning skal ske i overensstemmelse med en eventuel databehandleraftale imellem Ordregiver og Leverandør.
3. **Destruere** eventuelle fysiske dokumenter, der indeholder Ordregivers fortrolige informationer eller personoplysninger, på en sikker måde (for eksempel makulering).

Krav om ingen kopier

Leverandøren skal sikre, at der efter tilbagelevering og sletning ikke opbevares nogen kopier af Ordregivers data hos Leverandøren eller dennes underleverandører, medmindre:

1. Opbevaring er påkrævet i henhold til anden lovgivning (for eksempel bogføringslovgivning). I sådanne tilfælde skal data opbevares i krypteret form, isoleret fra produktionsdata og efter de sikkerhedskrav, der er fastsat i dette Bilag, og meddeles skriftligt til Ordregiver.
2. Ordregiver udtrykkeligt og skriftligt har givet tilladelse til fortsat opbevaring med et specifikt formål.

Bekræftelse på sletning/destruktion

Leverandøren skal, senest inden for 14 kalenderdage efter den aftalte frist for sletning/destruktion, fremsende en skriftlig bekræftelse til Ordregiver. Bekræftelsen skal:

1. Angive, at alle Ordregivers data er slettet/destrueret i overensstemmelse med dette Bilag.
2. Specificere, hvis der undtagelsesvist er data, der opbevares i henhold til afsnit 00, og give en begrundelse herfor.

Omkostninger

Alle omkostninger forbundet med tilbagelevering, sletning og destruktion af data, samt udarbejdelse af bekræftelse herpå, afholdes af Leverandøren.

Tilsyn og audit ved ophør

Ordregiver er berettiget til at føre tilsyn med, eller anmode om audit af, Leverandørens efterlevelse af forpligtelserne i dette afsnit, herunder om data er slettet korrekt. Leverandøren skal give fuld medvirken til dette.

UDKAST