

RIGSPOLITIET

POLITI

Bilag 14

Databehandleraftale

Databehandlersaftale

mellem

**Rigspolitiet,
Polititorvet 14,
København V,
CVR-nr. 17143611**

"Kunden"
(som dataansvarlig)

og

**EasyTranslate A/S,
Sundkaj 9,
Pakhus 48,
2150 Nordhavn,
CVR-nr. 33240562**

"Leverandøren"
(som databehandler)

EFTERSOM

- A. Leverandøren udfører visse tjenesteydelser for Kunden i tilknytning til Rameaftale om levering af fremmedsprogstolkning. Disse tjenesteydelser omfatter hvad der i nærmere bestemt omfang er aftalt mellem Parterne (herefter benævnt "Kontrakten"), og
- B. Kunden er Dataansvarlig for de Personoplysninger, som behandles i forbindelse med Leverandørens udførelse af tjenesteydelserne, og
- C. Leverandøren dermed er Databehandler for Kunden

HAR PARTERNE VEDTAGET FØLGENDE:

1 Baggrund og definitioner

- 1.1 Nærværende databehandleraftale ("Aftalen") omfatter enhver nærmere fastsat behandling af personoplysninger som Leverandøren måtte foretage på vegne af Kunden, jf. Kontraktens punkt 2.2.
- 1.2 Begreber i denne Aftale, der skrives med stort forbogstav, skal, medmindre andet er angivet, forstås i overensstemmelse med de definitioner, der fremgår af den til enhver tid gældende persondataretlige regulering i Danmark, jf. punkt 4.1 og 4.2.

2 Aftalens omfang og formål

- 2.1 Omfanget af de tjenesteydelser, som Leverandøren skal udføre er beskrevet i Kontrakten.
- 2.2 Formålet og karakteren med Leverandørens Behandling af Personoplysninger på vegne af Kunden er:

Leverandøren behandler oplysninger om tolke og oversættere med henblik på at kunne levere tolkeydelser og oversættelse til myndighederne, herunder Kunden, som er omfattet af Kontrakten. Formålet med behandlingen af Personoplysninger er at sikre, at myndighedernes, herunder Kundens, behov

kan understøttes ved bestilling af tolkning og i den forbindelse er det nødvendigt at registrere oplysninger om tolke og oversættere, herunder navn, alder og køn.

2.3 Behandlingen omfatter følgende typer af almindelige Personoplysninger:

Leverandøren behandler oplysning om navn, e-mail adresse, telefonnummer, adresse, cpr-nummer, betalingsinformationer, oplysninger om køretøjer, journalnumre, identifikationsnummer, lokaliseringsdata mv.

2.4 Behandlingen omfatter følgende typer af følsomme Personoplysninger:

Leverandøren behandler ikke følsomme Personoplysninger på vegne af Kunden.

2.5 Behandlingen omfatter følgende kategorier af Registrerede:

Leverandøren behandler oplysninger om medarbejdere og eksterne samarbejdspartnere der er oprettet i platformen.

2.6 I denne Aftales Bilag 1 har Leverandøren oplyst den geografiske placering af servere, servicecentre mv. som anvendes til at levere Tjenesteydelserne. Leverandøren forpligter sig til at give skriftligt varsel til Kunden mindst 3 måneder forud for ændringer af den geografiske placering. Dette kræver ikke en formel ændring af Bilag 1, forudgående skriftligt varsel via post eller e-mail er tilstrækkeligt.

3 **Generelle krav til Leverandøren**

3.1 Dette punkt 3 er uden præjudice for strengere krav fastsat i Aftalen.

3.2 Leverandøren er under ingen omstændigheder berettiget til at betinge den fulde og ubegrænsede efterlevelse af Kundens instruks af Kundens betaling af udestående fakturaer mv., og Leverandøren har ingen tilbageholdsret i Personoplysninger, der behandles for Kunden.

4 **Behandling af Personoplysninger mv.**

4.1 Leverandøren er instrueret i alene (1) at behandle Personoplysningerne

med det formål at levere Tjenesteydelserne samt (2) behandle Personoplysningerne i overensstemmelse med den til enhver tid gældende persondataretlige regulering i Danmark, herunder for tiden navnlig lov nr. 410 af 27. april 2017 om retshåndhævende myndigheders behandling af personoplysninger og lov nr. 429 af 31. maj 2000 om behandling af personoplysninger med senere ændringer samt de i medfør af loven udstedte administrative forskrifter. Såfremt Leverandøren skønner, at en instruks er i strid med førnævnte lovgivning, skal Leverandøren straks orientere Kunden herom.

- 4.2 Begge Parter forpligter sig til i hele aftaleperioden at indhente og opretholde de registreringer og tilladelser, som Parten er forpligtet til at indhente og opretholde i overensstemmelse med gældende lov eller bestemmelser fastsat i henhold til lov.
- 4.3 Ingen af Parterne kan påberåbe sig Aftalens indhold i et tilfælde, hvor dette ville indebære en overtrædelse af relevant lovgivning.
- 4.4 Leverandøren sikrer, at de personer, der er autoriseret til at behandle Personoplysninger omfattet af Aftalen, har forpligtet sig til fortrolighed eller er underlagt en passende lovbestemt tavshedspligt, jf. også punkt 9.
- 4.5 Leverandøren bistår den dataansvarlige på enhver hensigtsmæssig måde – herunder i et hvilket som helst omfang, som måtte være nødvendigt for at besvare henvendelser fra de kompetente databeskyttelsestilsynsmyndigheder – med at sikre overholdelse af bestemmelser om den registreredes rettigheder indeholdt i den til enhver tid gældende persondataretlige regulering i Danmark. Leverandøren skal deltage i eventuelle drøftelser med Datatilsynet eller andre kompetente myndigheder og implementere eventuelle anbefalinger og/eller påbud mv. fra sådanne myndigheder om behandling af Personoplysninger omfattet af Aftalen.
- 4.6 Leverandøren skal straks underrette Kunden, såfremt en kompetent myndighed retter henvendelse til Leverandøren vedrørende behandlingen af Personoplysninger omfattet af Aftalen.
- 4.7 Leverandøren sletter eller tilbageleverer i overensstemmelse med

Kundens valg alle Personoplysninger til Kunden, efter at leveringen af Tjenesteydelserne er ophørt, og sletter eksisterende kopier, medmindre forpligtelser i henhold til EU-retten eller retten i en EU medlemsstat foreskriver opbevaring af Personoplysningerne.

- 4.8 Leverandøren stiller alle oplysninger, der er nødvendige for at påvise overholdelsen af gældende persondataretlig regulering til rådighed for Kunden.
- 4.9 Leverandøren skal straks assistere Kunden med håndteringen af enhver henvendelse fra en registreret, herunder anmodninger om indsigt, berigtigelse, blokering eller sletning, i det omfang de relevante Personoplysninger behandles af Leverandøren.
- 4.10 Leverandøren forpligter sig til at friholde og forsvare Kunden imod alle krav, retskrav og ethvert ansvar, tab, omkostninger og udgifter forbundet derved som følge af en overtrædelse af Aftalen eller gældende persondataret, hvad enten overtrædelsen er begået af Leverandøren, Leverandørens ansatte, underleverandører (underdatabehandlere) eller repræsentanter i forbindelse med levering af Tjenesteydelserne, gennemførelse af Aftalen eller som i øvrigt aftalt mellem Parterne.

5 Brug af underdatabehandlere

- 5.1 Leverandøren må ikke gøre brug af en anden Databehandler (underdatabehandlere), herunder foretage overførsler eller videregivelse ud af Danmark af Personoplysninger der er omfattet af Aftalen, uden forudgående og specifik skriftlig godkendelse fra Kunden. Kunden er berettiget til at stille vilkår for en sådan godkendelse.
- 5.2 Enhver brug af underdatabehandlere skal være reguleret af en aftale, der – med mindre andet konkret er godkendt af Kunden – binder underdatabehandleren til at efterleve samtlige de forpligtelser, der påhviler Leverandøren i medfør af denne Aftale.

6 Krav til sikkerhed og databeskyttelse

- 6.1 Leverandøren skal træffe de fornødne tekniske og organisatoriske

sikkerhedsforanstaltninger mod, at Personoplysningerne hændeligt eller ulovligt tilintetgøres, fortabes eller forringes, samt mod at de kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med den til enhver tid gældende persondatarettlig regulering.

6.2 Fastsættelsen af fornødne tekniske og organisatoriske sikkerhedsforanstaltninger skal ske under iagttagelse af bl.a.:

i. denne Aftales Bilag 1.

6.3 Hvis Leverandøren er etableret i en anden EU-medlemsstat, skal de bestemmelser om sikkerhedsforanstaltninger, som er fastsat i lovgivningen i den EU-medlemsstat, hvor Leverandøren er etableret, derudover gælde for Leverandøren.

7 Kontrol

7.1 Leverandøren skal på Kundens anmodning give Kunden tilstrækkelige informationer til, at denne kan påse, at Leverandøren har truffet de nødvendige tekniske og organisatoriske sikkerhedsforanstaltninger.

7.2 I forbindelse med opfølgning på Aftalen, skal Leverandøren én gang årligt udarbejde og fremsende en uafhængig revisionserklæring baseret på en anerkendt standard vedrørende generelle it-kontroller til Kunden. Revisionserklæringen skal omfatte en vurdering af Leverandørens efterlevelse af kravene fastlagt i denne aftale samt de krav, der i øvrigt måtte følge af den til enhver tid gældende persondatarettlige regulering i Danmark. Erklæringen skal afgives til udgangen af hvert år, således at erklæringen er Kunden i hænde senest den 31. december. I forbindelse med udfærdigelsen af erklæringen skal enhver information indhentet hos eller modtaget fra Leverandøren behandles fortroligt. Leverandøren og Kunden skal begge modtage en kopi af revisionserklæringen. Udarbejdelse af uafhængige revisionserklæringer er uden vederlag for Kunden.

Kunden kan anmode om fremsendelse af den senest udarbejdede revisionserklæring via:

frp@easytranslate.com

7.3 Kunden kan foretage uanmeldt kontrol af, at Leverandøren samt eventuelle underleverandører overholder deres forpligtelser, herunder kontrol af og eventuel opfølgning på brugeradgange og rettigheder. En betroet tredjepart godkendt af Kunden og Leverandøren skal ligeledes kunne foretage denne kontrol.

7.4 I det omfang Kunden instruerer Leverandøren herom, er Leverandøren forpligtet til at give myndigheder, der efter den til enhver tid gældende danske lovgivning har adgang til Kundens og Leverandørens faciliteter, eller repræsentanter, der optræder på myndighedens vegne, adgang til Leverandørens fysiske faciliteter mod behørig legitimation. I det omfang myndigheder, der efter gældende danske lovgivning er tillagt tilsynskompetence mv. over for Kunden, stiller krav herom, skal Leverandøren give adgang til det fulde revisionsspor indeholdt i enhver revisionserklæring mv. udarbejdet om Leverandørens efterlevelse af persondataretlige krav og it-sikkerhedsstandarder, herunder erklæringer omfattet af punkt 7.2.

8 Informationssikkerhedsbrud og Brud På Persondatasikkerheden

8.1 Leverandøren skal have dokumenterede og fungerende procedurer for håndtering af informationssikkerhedsbrud samt mistanke om Brud På Persondatasikkerheden. Procedurerne skal sikre, at Kunden underrettes om sikkerhedshændelser.

8.2 I tilfælde af Brud På Persondatasikkerheden eller mistanke herom skal Leverandøren uden unødigt forsinkelse orientere Kunden herom skriftligt, jf. også punkt 8.1. Leverandøren skal herefter uden unødigt ophold, dog senest 24 timer efter Bruddet På Persondatasikkerheden eller en mistanke herom, rapportere til Kunden. Rapporteringen skal som minimum indeholde følgende:

- En beskrivelse af karakteren af Bruddet, herunder kategorierne og det omtrentlige antal berørte Registrerede samt kategorierne og det omtrentlige antal berørte registreringer af Personoplysninger
- en beskrivelse af de sandsynlige konsekvenser af Bruddet
- en beskrivelse af de foranstaltninger, som Leverandøren foreslår truffet for at håndtere Bruddet, herunder

foranstaltninger for at begrænse dets mulige skadevirkninger.

Leverandøren må alene underrette tredjemand om et Brud På Persondatasikkerheden efter forudgående skriftlig tilladelse fra Kunden.

- 8.3 Når og for så vidt som det ikke er muligt at give oplysningerne samlet, kan oplysningerne omfattet af punkt 8.2 meddeles trinvist uden unødigt yderligere forsinkelse.

9 Tavshedspligt

- 9.1 Leverandøren skal holde alle Personoplysningerne og enhver oplysning om Aftalen fortrolige, og er således alene berettiget til at anvende Personoplysningerne som led i opfyldelsen af sine forpligtelser i henhold til Kontrakten, herunder Aftalen.

- 9.2 Leverandøren og dennes medarbejdere skal iagttage ubetinget tavshed for så vidt angår de Personoplysninger, som de får kendskab til i forbindelse med opfyldelse af Kontrakten. Leverandøren skal pålægge eventuelle underleverandører (underdatabehandlere), deres medarbejdere og andre, der bistår Leverandøren i forbindelse med opfyldelse af Kontrakten, en tilsvarende forpligtelse.

10 Erstatningsansvar

- 10.1 Leverandøren (eller eventuelle underdatabehandlere) hæfter kun for skade, der er forvoldt ved behandling af Personoplysninger, hvis de pågældende ikke har overholdt de forpligtelser, der i forhold til den til enhver tid gældende persondataretlige regulering i Danmark, jf. bl.a. punkt 4.1, gælder for Databehandlere, eller hvis de pågældende har undladt at følge eller handlet i strid med den Kundens lovlige instrukser.

- 10.2 Hvis Kunden, i en situation, hvor både Kunden og Leverandøren (eller en eller flere underdatabehandlere) er involveret i den samme behandling, har betalt fuld erstatning for den forvoldte skade, har Kunden ret til at kræve den del af erstatningen, der svarer til de øvrige parter del af ansvaret for skaden, tilbage fra de øvrige parter.

11 Ændringer i Aftalen

- 11.1 Parterne kan til enhver tid ændre databehandleraftalen, jf. Kontraktens punkt 2.2.

12 Varighed og ophør af Aftalen

- 12.1 Aftalen træder i kraft ved Parternes underskrift og er gældende så længe Leverandøren behandler Personoplysninger på vegne af Kunden eller til Kontraktens ophør, alt efter hvilket tidspunkt, der indtræder senest.
- 12.2 Uanset Aftalens formelle aftaleperiode skal Aftalen vedblive at gælde, så længe Leverandøren behandler de personoplysninger, som Kunden er dataansvarlig for.
- 12.3 I tilfælde af ophør af Aftalen, uanset det juridiske grundlag herfor, skal Leverandøren yde de fornødne overgangsydelser til Kunden, jf. Kontraktens punkt 23.
- 12.4 De fornødne overgangsydelser omfatter bl.a., at Leverandøren skal handle efter instruks fra Kunden, herunder instruks om straks at tilbagelevere eller slette samtlige Personoplysninger, uanset opbevaringsmedie.
- 12.5 Leverandøren er forpligtet til loyalt og hurtigst muligt at medvirke til, at udførelse af ydelserne overgår til en anden databehandler eller tilbageføres til Kunden. Leverandøren skal straks efter anmodning fra Kunden ændre, overføre eller slette Personoplysninger, som Leverandøren behandler for Kunden.

13 Forrang

- 13.1 I ethvert tilfælde af konflikt eller fortolkningstvivl mellem bestemmelserne i denne Aftale og bestemmelserne i andre skriftlige eller mundtlige aftaler indgået mellem Parterne – herunder Kontrakten – skal bestemmelserne i denne Aftale have forrang.

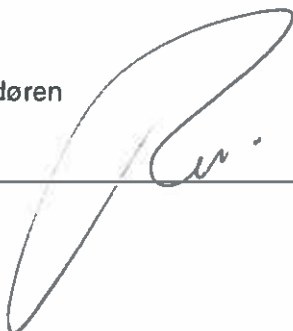
14 Underskrift

Ovenstående tiltrædes hermed med virkning fra databehandleraftalens underskrift.

København, den 14/11-2018

Frederik R. Pedersen
Direktør

For Leverandøren



København, den 15/11-2018

Thomas Østrup Møller
Koncernstyringsdirektør

For Rigspolitiet



BILAG 1 – ARBEJDSORDRE OG SIKKERHEDSKRAV

Dette dokument ("Arbejdsordre"/"Arbejdsordren") er aftalt i tilknytning til databehandleraftalen (tidligere defineret som "Aftalen").

Begreber defineret i Aftalen skal have den samme betydning, når de anvendes i denne Arbejdsordre.

1 Behandlingen af Personoplysninger

Lokation(er) for behandlingen:

EasyTranslate har data hosted på en sikker centraliseret storage service (S3) i EU, nærmere betegnet Dublin, Irland på Amazons to datacentre.

Amazon Web Services (AWS)

- **South Dublin Data Center**
Parkview, Greenhills Rd, Tymo Noth, Dublin 24, Ireland
- **Clonshaugh Data Center**
Saint Joseph, Clonshaugh Rd, Clonshaugh, Dublin 17, Ireland

2 Minimumskrav til de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger

- i. Leverandøren skal som minimum træffe de nedenfor beskrevne tekniske og organisatoriske sikkerhedsforanstaltninger i forbindelse med behandlingen af Personoplysningerne beskrevet i denne Arbejdsordre. Hvis mere omfattende tekniske og organisatoriske sikkerhedsforanstaltninger er nødvendige for at sikre efterlevelse af Aftalens punkt 8, skal sådanne mere omfattende foranstaltninger altid træffes.
- ii. Leverandøren skal behandle Personoplysningerne i overensstemmelse med gældende lov og i overensstemmelse med gældende vejledninger og politikker hos Kunden, herunder Kundens IT sikkerhedspolitik samt underliggende politikker.
- iii. Leverandøren skal udpege et fast kontaktpunkt, som over for

Kunden skal varetage ethvert forhold i relation til behandlingen af Personoplysninger for Kunden.

- iv. Leverandøren skal udarbejde og vedligeholde en informationssikkerhedspolitik, der er godkendt af Leverandørens ledelse, hvori der – som minimum – er en beskrivelse af:
 - a. Ledelsens overordnede retningslinjer for informationssikkerhed
 - b. Krav om, opbakning til og engagement i opfyldelsen af alle relevante lovkrav om databeskyttelse samt aftalte krav fra Kunden
 - c. Regler og retningslinjer for fastlæggelse af et acceptabelt risikoniveau
- v. Parterne er herunder enige om, at Leverandøren skal træffe følgende tekniske og organisatoriske sikringsforanstaltninger, der må anses for at være fornødne, jf. ovenfor:
- vi. Den fysiske adgang til lokaliteter, hvor der behandles Personoplysninger, sikres mod uvedkommendes adgang til oplysningerne, og kan eksempelvis omfatte aflåsning af lokaler, brug af adgangskort, alarmsystemer og vagter, samt særlig begrænsning i adgangen til serverrum.
- vii. Der må udelukkende ske behandling af data i eller fra godkendte lokaler eller fra godkendte, sikrede fjernadgange. Dette gælder ligeledes ved anvendelse af mobile enheder. Al administration af systemer skal foregå via krypterede forbindelser, herunder skal det være muligt at tilbyde differentieret login eventuelt ved krav om to logins ved anvendelse af særlige rettigheder.
- viii. I forbindelse med reparation og service af dataudstyr, der indeholder Personoplysninger skal der træffes de fornødne foranstaltninger for at sikre mod, at Personoplysninger hændeligt eller ulovligt tilintetgøres, fortabes eller forringes samt mod, at de kommer til uvedkommendes kendskab, misbruges eller i øvrigt

behandles i strid med lovgivningen. Ved reparation og service af udstyr, skal Leverandøren, hvis ikke oplysningerne kan fjernes fra udstyret, sikre sig, at reparations- og servicepersonalet vil behandle oplysninger, som de måtte blive bekendt med under deres arbejde, som fortroligt materiale, der under ingen omstændigheder må videregives eller anvendes. Ved kassation af lagringsmedier og udstyr, som indeholder Personoplysninger, skal lagringsmedierne destrueres eller afmagnetiseres, så der ikke er mulighed for at læse indholdet. It-udstyr og lagermedier, som har været anvendt til lagring eller behandling af politiets data og som ikke skal anvendes mere, må ikke bortsælge men skal destrueres ved fysisk destruktion. Lagret information skal slettes forud for reparation af it-udstyr. Slettemetoden skal være godkendt af Koncern IT.

- ix. Kun de personer, som autoriseres hertil, må have adgang til de Personoplysninger, der behandles. Der må kun autoriseres personer, der er beskæftiget med de formål, hvortil Personoplysningerne behandles. De enkelte brugere må ikke autoriseres til anvendelser, som de ikke har behov for. Der må endvidere autoriseres personer, for hvem adgang til oplysninger er nødvendig med henblik på revision eller drifts- og systemtekniske opgaver. Leverandøren skal træffe foranstaltninger for at sikre, at kun autoriserede brugere kan få adgang, og at disse kun kan få adgang til de Personoplysninger og anvendelser, som de er autoriserede til.
- x. Der skal foretages den fornødne uddannelse/instruktion af medarbejderne i brugeradministrationen for at sikre disse reglers overholdelse.
- xi. Det skal være muligt for Leverandøren at generere oversigter over brugere og tildelte rettigheder samt grupper og roller, herunder disse brugeres brug af konti, særligt med henblik på kontrol og opfølgning. Oversigten skal dokumentere grupperinger af rettigheder, tilføjede, ændrede eller slettede rettigheder samt tidsstempling herfor. Oversigten skal udleveres til Kunden på Kundens forlangende. Systemet skal kunne foretage automatisk låsning af konti efter en periode uden aktivitet.

- xii. Inddatamateriale må alene anvendes af personer, som er beskæftiget med inddatering. Ved inddatamateriale forstås det grundmateriale (papirbaseret eller elektronisk), hvorfra der hentes oplysninger til videre elektronisk behandling. Inddatamateriale, som indeholder fortrolige eller følsomme Personoplysninger, skal opbevares aflåst, når det ikke anvendes. Inddatamateriale skal slettes eller tilintetgøres, når det ikke længere skal anvendes til de formål, som behandlingen varetager, eller til kontrol med de inddaterede Personoplysninger. Ved tilintetgørelse af inddatamateriale skal Leverandøren træffe de fornødne sikkerhedsforanstaltninger mod, at materialet misbruges eller kommer til uvedkommendes kendskab. Disse foranstaltninger skal omfatte opsamling af materiale i aflåste containere med efterfølgende anvendelse af en pålidelig makuleringservice for fortroligt materiale.
- xiii. Uddatamateriale må kun anvendes af personer, der er beskæftiget med de formål, til hvilke behandlingen af Personoplysningerne foretages. Ved uddatamateriale forstås det resultat af en elektronisk databehandling, som foreligger på papirbaseret eller elektronisk form. Herudover må uddatamateriale anvendes af personer, der er beskæftiget med revision eller drifts- og systemtekniske opgaver vedrørende systemet hos Leverandøren. Leverandøren skal opbevare uddatamateriale på en sådan måde, at uvedkommende ikke kan gøre sig bekendt med Personoplysningerne deri. Uddatamateriale skal slettes eller tilintetgøres, når det ikke længere skal anvendes til de formål, som behandlingen varetager, og senest efter **5 dage**. Ved tilintetgørelse af inddatamateriale skal Leverandøren træffe de fornødne sikkerhedsforanstaltninger mod, at materialet misbruges eller kommer til uvedkommendes kendskab. Disse foranstaltninger skal omfatte opsamling af materiale i aflåste containere med efterfølgende anvendelse af en pålidelig makuleringservice for fortroligt materiale.
- xiv. Udveksling af Personoplysninger mellem Kunden og Leverandøren samt mellem Leverandøren og eventuelle underleverandører skal ske gennem den løsning, Kunden har

autoriseret eller stillet til rådighed, og som indeholder kryptering.

- xv. Der skal kunne opsættes sletterutiner (automatisk håndtering af sletning af data) efter lovgivningens regler således, at data kan slettes på bestemte tidspunkter efter de opsatte regler. Personoplysninger skal under alle omstændigheder slettes eller tilintetgøres, når de ikke længere skal anvendes til de formål, som behandlingen varetager.
- xvi. Der skal foretages maskinel registrering (logning) af alle behandlinger af Personoplysninger. Registreringen skal mindst indeholde oplysning om tidspunkt, bruger, type af behandling og angivelse af den person, de anvendte oplysninger vedrørte, eller det anvendte søgekriterium.
- xvii. Der til enhver tid foreligger en aktuel risikovurdering for Kundens it-miljø hos Leverandøren. Leverandøren skal således løbende foretage risikoanalyse og risikobedømmelse af alle hændelser og handlinger, der potentielt kan påvirke den aktuelle risikovurdering. Leverandøren skal på baggrund af risikovurderingen identificere og vurdere mulighederne for risikohåndtering.
- xviii. Leverandøren skal løbende gennemføre test af, at det etablerede sikkerhedsniveau overholdes.

3 Kontrol med informationssikkerhed og databeskyttelse

- i. Leverandøren skal på Kundens anmodning give Kunden tilstrækkelige informationer til, at denne kan påse, at Leverandøren har truffet de nødvendige tekniske og organisatoriske sikkerhedsforanstaltninger.
- ii. Hvis Leverandøren er etableret i en anden EU-medlemsstat, skal de bestemmelser om sikkerhedsforanstaltninger, som er fastsat i lovgivningen i den EU-medlemsstat, hvor Leverandøren er etableret, derudover gælde for Leverandøren. Hvis Leverandøren er etableret i en anden EU-medlemsstat, skal Leverandøren

således overholde såvel sikkerhedskrav omfattet af gældende lovgivning i Danmark som sikkerhedskrav i Leverandørens hjemland.

- iii. Leverandøren (og enhver eventuel underleverandør) skal hvert år i december for egen regning indhente en erklæring fra en uafhængig ekspert angående Leverandørens overholdelse af kravene til sikkerhedsforanstaltninger fastsat i Aftalen. Erklæringen skal udarbejdes på grundlag af en anerkendt standard for sådanne erklæringer. Erklæringen skal sendes til Kunden senest den 31. december det pågældende år.
- iv. Derudover har Kunden ret til, for egen regning, at udpege en uafhængig ekspert, som skal have adgang til Leverandørens (og enhver eventuel underleverandørs) fysiske faciliteter for behandling af Personoplysninger samt modtage de nødvendige informationer til udførelsen af undersøgelsen af, hvorvidt Leverandøren har truffet de nævnte tekniske og organisatoriske sikkerhedsforanstaltninger.
- v. Leverandøren er forpligtet til at give oplysninger i relation til udførelsen af Tjenesteydelserne til myndigheder og Kundens eksterne rådgivere, i det omfang det er nødvendigt i forhold til deres opgavevaretagelse.
- vi. Leverandøren er endvidere forpligtet til at give myndigheder, der efter lovgivningen har adgang til Kundens og Kundens leverandørers faciliteter, eller repræsentanter, der optræder på myndighedens vegne, adgang til Leverandørens fysiske faciliteter mod behørig legitimation.