DATABEHANDLERAFTALE

Brug af TrueLink services jf. Medlemsvilkår (Hovedkontrakten)

indgået mellem

Medlem / Kunde

Der er bruger TrueLink services og har tiltrådt **Medlemsvilkår - TrueLink**, dateret april 2018 eller senere

(den "Dataansvarlige")

og

TrueLink A/S

CVR: 31261430

Havneparken 1, 1

7100 Vejle

("Databehandleren", tilsammen "Parterne" og hver for sig en "Part")

BILAG TIL DATABEHANDLERAFTALEN

Bilag 1	Instruks fra den Dataansvarlige
Bilag 2	Tekniske og organisatoriske sikkerhedskrav og garantier
Bilag 3	Den Dataansvarliges forpligtelser
Bilag 4	Underdatabehandlere
Bilag 5	Overførsel til tredjelande og internationale organisationer

1 BAGGRUND OG FORMÅL

1.1 Parterne har aftalt levering af ydelser fra Databehandleren til den Dataansvarlige, som nærmere beskrevet i Databehandlerens Medlemsvilkår herom (”Hovedkontrakten”) beskrevet i bilag 1 til denne aftale (”Den Dataansvarlige instruks”).

1.2 I den forbindelse behandler Databehandleren personoplysninger på vegne af den Dataansvarlige, hvorfor Parterne har indgået denne aftale med underliggende bilag (”Databehandleraftalen”).

1.3 Databehandleraftalen har til formål at sikre, at Parterne overholder den ved Databehandleraftalens indgåelse gældende persondataretlige regulering, dvs.:

(i) Persondataloven (lov 2000-05-31 nr. 429 med senere ændringer)

(ii) Persondataforordningen (Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016), når denne får virkning 25. maj 2018.

2 OMFANG

2.1 Databehandleren bemyndiges til at foretage behandling af personoplysninger på den Dataansvarliges vegne på vilkårene fastsat i Databehandleraftalen.

2.2 Databehandleren må alene behandle personoplysninger efter dokumenteret instruks fra den Dataansvarlige (”Instruks”). Denne Databehandleraftale inkl. bilag udgør Instruksen på accepttidspunktet for TrueLink Medlemsvilkår.

2.3 Instruksen kan til enhver tid ændres eller konkretiseres nærmere af den Dataansvarlige. Sådanne ændringer foretages i henhold til den mellem Parterne aftalte ændringshåndteringsproces, jf. Hovedkontrakten.

3 VARIGHED

3.1 Databehandleraftalen gælder indtil Hovedkontrakten ophører.

4 DATABEHANDLERENS FORPLIGTELSER

4.1 Tekniske og organisatoriske sikkerhedsforanstaltninger

4.1.1 Databehandleren har ansvaret for at gennemføre fornødne (a) tekniske- og (b) organisatoriske sikkerhedsforanstaltninger. Foranstaltningerne skal gennemføres under hensyntagen til det

aktuelle tekniske niveau, implementeringsomkostningerne, og den pågældende behandlings karakter, omfang, sammensætning og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder, samt typerne af personoplysninger beskrevet i bilag 1.

4.1.2 Databehandleren skal uanset punkt 4.1.1 gennemføre de tekniske og organisatoriske sikkerhedsforanstaltninger som fremgår af bilag 2 til denne Databehandleraftale.

4.1.3 Databehandleren gennemfører de passende tekniske og organisatoriske foranstaltninger på en sådan måde, at Databehandlerens behandling af personoplysninger opfylder kravene i gældende persondataretlige regulering.

4.2 Medarbejderforhold

4.2.1 Databehandleren skal sikre, at medarbejdere, der behandler personoplysninger for Databehandleren, har forpligtet sig til fortrolighed eller er underlagt en passende lovbestemt tavshedspligt.

4.3 Påvisning af overholdelse

4.3.1 Databehandleren stiller efter anmodning alle oplysninger, der er nødvendige for at påvise overholdelse af kravene i Databehandleraftalen, til rådighed for den Dataansvarlige og giver mulighed for og bidrager til revisioner, herunder inspektioner, der foretages af den Dataansvarlige eller en anden revisor, som er bemyndiget af den Dataansvarlige. En sådan anmodning besvares inden rimelig tid.

4.3.2 For så vidt angår punkt 4.3.1 underretter Databehandleren omgående den Dataansvarlige, hvis en instruks efter Databehandlerens mening er i strid med databeskyttelseslovgivningen eller databeskyttelsesbestemmelser i anden EU-ret eller nationale ret.

4.4 Fortegnelse over behandlingsaktiviteter

4.4.1 Hver af Parterne fører fortegnelser over behandlingsaktiviteter i det omfang det er påkrævet i artikel 30 i Persondataforordningen.

4.5 Sikkerhedsbrud

4.6 Databehandleren underretter uden unødig forsinkelse den dataansvarlige hvis Databehandleren bliver opmærksom på, at der er sket brud på persondatasikkerheden.

4.7 Underretningen skal indeholde de faktiske omstændigheder ved bruddet på persondatasikkerheden, dets virkninger og de trufne og planlagte afhjælpende foranstaltninger.

4.8 Bistand

4.8.1 På den Dataansvarliges anmodning, bistår Databehandleren så vidt muligt den Dataansvarlige ved hjælp af passende tekniske og organisatoriske foranstaltninger, med opfyldelse af den Dataansvarliges forpligtelse til at besvare anmodninger om udøvelse af de registreredes rettigheder.

4.8.2 Under hensyntagen til behandlingens karakter og de oplysninger, der er tilgængelige for Databehandleren bistår Databehandleren den Dataansvarlige med at sikre overholdelse af forpligtelserne vedrørende den Dataansvarliges:

a) Behandlingssikkerhed,

b) Anmeldelse af brud på persondatasikkerheden til tilsynsmyndigheder,

c) Underretning om brud på persondatasikkerheden til registrerede,

d) Konsekvensanalyser vedrørende databeskyttelse, og

e) Forudgående høringer.

5 DEN DATAANSVARLIGES FORPLIGTELSER

5.1 Den Dataansvarlige har de forpligtelser, som fremgår af bilag 5.

6 UNDERDATABEHANDLERE

6.1 Databehandleren må kun gøre brug af en tredjepart til behandlingen af personoplysninger for den Dataansvarlige ("Underdatabehandler") i det omfang det fremgår af (a) bilag 4 til denne Databehandleraftale, eller (b) Instruks fra den Dataansvarlige (bilag 1).

6.2 Databehandleren og Underdatabehandleren skal indgå en skriftlig aftale, som pålægger Underdatabehandleren de samme databeskyttelsesforpligtelser, som påhviler Databehandleren (herunder i medfør af denne Databehandleraftale).

6.3 Underdatabehandleren handler herudover ligeledes alene på Instruks fra den Dataansvarlige.

6.4 Databehandleren er direkte ansvarlig for Underdatabehandlerens behandling af personoplysninger på samme vis, som var behandling foretaget af Databehandleren selv.

7 OVERFØRSEL TIL TREDJELANDE OG INTERNATIONALE ORGANISATIONER

7.1 Databehandleren må kun overføre personoplysninger til i et land uden for den Europæiske Union eller EØS (et "Tredjeland") eller internationale organisationer i det omfang dette fremgår af (a) bilag 5 til denne Databehandleraftale, eller (b) Instruks fra den Dataansvarlige.

7.2 Overførsel af personoplysninger må i alle tilfælde kun ske, hvis Databehandleren har sikret et fornødent overførelsesgrundlag, f.eks. EU Kommissionens Standardkontraktsbestemmelser.

8 DATABEHANDLING UDENFOR INSTRUKSEN

8.1 Databehandleren kan behandle personoplysninger udenfor Instruksen i tilfælde, hvor det kræves af EU-retten eller national ret, som Databehandleren er underlagt.

8.2 Ved behandling af personoplysninger udenfor Instruksen skal Databehandleren underrette den Dataansvarlige om årsagen hertil. Underretningen skal ske, inden behandlingen foretages og skal indeholde en henvisning til de retlige krav, der ligger til grund for behandlingen.

8.3 Underretning skal ikke ske, hvis underretning vil være i strid med EU retten eller den nationale ret.

9 VEDERLAG OG OMKOSTNINGER

9.1 Databehandleren har krav på betaling efter medgået tid samt Databehandlerens øvrige omkostninger herved, for de ydelser der udføres efter Databehandleraftalen på den Dataansvarliges anmodning. Ydelserne kan omfatte, men er ikke begrænset til, ændringer af instruksen, assistance ved anmeldelse af brud på persondatasikkerheden, udlevering og sletning af oplysninger, bistand ved audit, bistand ved ophør, samarbejde med tilsynsmyndigheder og hjælp til efterlevelse af anmodninger fra registrerede.

9.2 Databehandleren har krav på betaling efter medgået tid samt Databehandlerens øvrige omkostninger herved, for de ydelser der udføres efter Databehandleraftalen som følger af ændringer i den Dataansvarliges forhold. Ydelserne kan omfatte, men er ikke begrænset til, bistand til ændringer der følger af nye risikovurderinger og konsekvensanalyser samt ændringer nødvendiggjort af ændringer i lovgivningen.

10 ØVRIGE BESTEMMELSER

10.1 Generelt

10.2 Misligholdelse

10.2.1 Misligholdelse er reguleret i TrueLink Medlemsvilkår.

10.3 Ansvar og ansvarsbegrænsninger

10.3.1 Ansvar og ansvarsbegrænsninger er reguleret i TrueLink Medlemsvilkår.

10.4 Force Majeure

10.4.1 Force majeure er reguleret i TrueLink Medlemsvilkår.

10.5 Fortrolighed

10.5.1 Fortrolighed er reguleret i TrueLink Medlemsvilkår.

11 OPHØR

11.1 Opsigelse og ophævelse

11.1.1 Databehandleraftalen kan alene opsiges eller ophæves i overensstemmelse med bestemmelserne om opsigelse og ophævelse i Medlemsvilkår i relation til bilag 1- Instruks fra den Dataansvarlige.

11.1.2 Opsigelse eller ophævelse af denne Databehandleraftale kan alene ske ved – og berettiger til - samtidig opsigelse eller ophævelse af dele af aftale(r)n(e) om levering af Hovedydelserne, der vedrører behandling af personoplysninger i medfør af Databehandleraftalen.

11.1.3 Når aftale(r)n(e) om levering af Hovedydelserne ophører, vil Databehandleren fortsat have virkning, indtil disse personoplysninger er slettet eller tilbageleveret som beskrevet i punkt 11.3.

11.2 Virkning af ophør

11.2.1 Reguleringen af virkning af ophør er reguleret i Hovedkontrakten.

11.3 Databehandleren og dennes Underdatabehandlere skal tilbagelevere alle personoplysninger, som Databehandleren har behandlet under denne Databehandleraftale, til den Dataansvarlige ved Databehandleraftalens ophør, i det omfang den Dataansvarlige ikke allerede er i besiddelse af personoplysningerne. Databehandleren er herefter forpligtet til at slette alle personoplysninger fra den Dataansvarlige med mindre andet fremgår af Hovedkontrakten. Den Dataansvarlige kan anmode om fornøden dokumentation for, at dette er sket.

11.4 Databehandleren er berettiget til at anonymisere personoplysningerne på en sådan måde, at de ikke senere kan de anonymiseres igen, og herefter anvende den anonyme data til egne formål både i denne Databehandleraftales løbetid og fremadrettet.

12 TVISTLØSNING

12.1 Reguleringen af tvistløsning i Hovedkontrakten finder anvendelse også for denne Databehandleraftale, som om denne Databehandleraftale var en integreret del heraf.

13 FORRANG

13.1 Såfremt der er modstrid mellem denne Databehandleraftale og aftale(r)n(e) om levering af Hovedydelserne, har denne Databehandleraftale forrang, med mindre andet følger direkte af Databehandleraftalen.

14 UNDERSKRIFTER

Vejle, den 1. april 2019

For den Dataansvarlige	For Databehandleren
Accept af TrueLink Medlemsvilkår logget i TrueLink services	Navn: Per Hedeboe Jensen Titel: Adm. direktør

BILAG 1
INSTRUKS FRA DEN DATAANSVARLIGE

1 FORMÅL OG HOVEDKONTRAKT

1.1 Med Hovedkontrakten menes: TrueLink Medlemsvilkår https://www.truelink.dk/medlemsvilkaar

2 PERSONOPLYSNINGER

2.1 Typer af personoplysninger, der behandles i sammenhæng med levering af Hovedydelsen:

a) Almindelige personoplysninger

b) Følsomme personoplysninger, herunder oplysninger om helbredsmæssige forhold (hvis relevant)

c) Cpr-numre (hvis relevant)

2.2 Kategorien af registrerede identificerede eller identificerbare fysiske personer omfattet af Databehandleraftalen:

a) Brugernavn, fornavn, efternavn, e-mail og telefonnr.
b) Oprettelse af egne kunder, med information om navn, adresse, telefon og e-mailadresse
c) Oprettelse af egne leverandører med navn, adresse, telefon og e-mailadresse
d) Dokumentdata med information om afsender / modtager persondata, samt indhold i dokumentet i form af ydelsesmodtager, CPR nr.
e) Det er den Dataansvarliges ansvar, at personfølsomme data er placeret korrekt i dokumenterne

TrueLink A/S vil i forbindelse med indførsel af Persondataforordningen den 25. maj 2018 begrænse adgang til data i TrueLink servicen:

- Visningsformular for faktura og kreditnota, hvor der fremgår et CPR nr. i indholdet af visningsformularen, vil dette indhold være markeret med xxxxxx-xxxx
- Adgang til 3-level log, hvor det er muligt at vise / downloade rå-data, som XML, CSV m.fl., hvor personfølsomme data kan ses
- Administrator kan ændre denne begrænsning på Kundens konto i TrueLink for alle brugere med adgang til Kundens konto. En sådan ændring vil blive logget i TrueLink persondata-log.

BILAG 2
TEKNISKE OG ORGANISATORISKE SIKKERHEDSKRAV

Generelle sikkerhedsforanstaltninger

TrueLink har udarbejdet og implementeret informationspolitikker med udgangspunkt i ISO 27001:2013 og ISO 27002:2017 standarder. I nedenstående er afsnit fra TrueLinks informationssikkerhedspolitikker kopieret ind, i.ht. TrueLinks informationssikkerhedspolitikker vil der minimum 1 gang årligt ske en review af informationssikkerhedspolitikkerne for at sikre at politikkerne tager højde for ændringer i trusselsbilledet, ændringer hos TrueLink m.m. TrueLink stiller til hver en tid sine informationssikkerhedspolitikker til gennemsyn for kunder og samarbejdspartnere.
Af hensyn til reference til TrueLinks interne dokumentation af informationssikkerhedspolitikker har vi i nedenstående valg at bruge samme afsnitsnumre, som der er i den interne dokumentation

Autorisation og adgangskontrol
Adgangsstyring
9.1 Forretningsmæssige krav til adgangsstyring
TrueLinks systemer er beskyttet af autorisationssystemer, som har til formål at sikre mod uautoriseret adgang, TrueLinks brugere medvirker til beskyttelse af informationsaktiverne gennem korrekt brug af autorisationssystemerne.

9.1.1 Politik for adgangsstyring
Kun adgang til relevant information
Brugers autorisation til systemer og systemers data begrænses, så kun adgang gives til systemer og data i det omfang, at brugerne har et arbejdsrelateret behov for adgangen.

9.1.2 Adgang til netværk og netværkstjenester
Opdeling af netværk
TrueLinks netværk er opdelt i virksomhedsnetværk og gæste netværk. Kun TrueLinks medarbejdere og eksterne konsulenter har adgang til virksomhedsnetværket og gæster kan få adgang til gæste netværk.

Forbindelse til hosting - andre outsourcing partnere
Alle forbindelser mellem TrueLinks kontor, hosting centre, outsourcing partnere og kunder etableres ved sikre VPN-forbindelser eller certifikat forbindelse, og hvor forbindelser kun giver adgang til nødvendige tjenester.

9.2 Administration af brugeradgang
TrueLink har en fast procedure for start -, ændre – og ophør af samarbejdsforhold, som foreskriver, at opdatering af dokumentation for tildelte rettigheder til brugere på TrueLinks systemer. Proceduren og fortegnelsen inkluderer almindelige brugers adgang og rettigheder samt tildeling af privilegerede brugerrettigheder samt brugeradgang til privilegerede systemprogrammer.

Det er systemejeren som giver bruger adgangen og rettigheder, i.h.t. ”09.02 procedure for start -, ændre – og ophør af samarbejdsforhold” samt sikre at ”09 Fortegnelse over brugere og -rettigheder” opdateres ved ændringer.

9.2.1 Brugerregistrering og -afmelding

Identifikation, autentifikation og autorisation af brugere

Alle brugere får tildelt en unik identitet i TrueLinks systemer, som kun er til personlig brug. Der er opsat passende autentifikationsteknik til verifikation af brugernes identitet. For at have fuld sporbarhed af en brugers aktiviteter på TrueLinks systemer, er det ikke tilladt at benyttes fælles bruger identiteter på TrueLinks systemer.

Nedlæggelse af bruger ved samarbejdsophør

I forbindelse md samarbejdsophør, hvor brugere skal nedlægges i TrueLinks systemer, har TrueLink en fast procedure for nedlæggelse af brugere.

Henvisning: ”09.02 Procedure for start -, ændre - og ophør af samarbejdsforhold” og dokumentation af ”09 Fortegnelse over brugere og -rettigheder”.

9.2.2 Tildeling af brugeradgang

I forbindelse med start – og ændring af samarbejdsforhold, har TrueLink en procedure for tildeling/fjernelse af rettigheder, proceduren foreskriver også opdatering af bruger- og -rettighedsfortegnelse.

Bruger rettigheder skal stemme overens med det forretningsmæssige behov, hvilket skal kontrolleres efter, at en bruger er oprettet.

Henvisning: ”09.02 Procedure for start -, ændre - og ophør af samarbejdsforhold” og dokumentation af ”09 Fortegnelse over brugere og -rettigheder”.

9.2.3 Styring af privilegerede adgangsrettigheder

Privilegerede / administrator adgangsrettigheder

Tildeling af privilegerede adgangsrettigheder, tildeles kun når der er et forretningsmæssig behov og tildeles kun ved forudgående godkendelse fra TrueLinks ledelse, TrueLink har en fast procedure for tildelingen af adgang til privilegerede adgangsrettigheder.

Henvisning: ”09.02 Procedure for start -, ændre - og ophør af samarbejdsforhold” og dokumentation af ”09 Fortegnelse over brugere og -rettigheder”.

Privilegerede systemprogrammer

Tildeling af afgang til privilegerede systemprogrammer, tildeles kun når der er et forretningsmæssig behov og tildeles kun ved forudgående godkendelse fra TrueLinks ledelse, TrueLink har en fast procedure for tildelingen af adgang til privilegerede systemprogrammer.

Henvisning: ”09.02 Procedure for start -, ændre - og ophør af samarbejdsforhold” og dokumentation af ”09 Fortegnelse over brugere og -rettigheder”.

Skift af systemadministrator passwords

Systemadministrator passwords skal ændres efter højest 60 dage. Systemadministrator passwords skal ændres, hvis der er den mindste mistanke om, at udenforstående har kendskab til passwordet og det

skal endvidere straks ændres, når der sker samarbejdsophør med en bruger/person, som har kendskab til systemadministrator passwords.

Generelle systemadministrator brugerprofiler, som kan benyttes på TrueLinks systemer, benyttes kun i nødsituationer og derfor aldrig i det daglige arbejde hos TrueLink.

Henvisning: "09.02.03 Procedure og log over ændring af Administrator – og system passwords" og "09 Fortegnelse over administrator - og system passwords"

9.2.4 Styring af hemmelig autentifikationsinformation om brugere

Krav til password/kodeord

Brugere skal ændre deres password/kodeord efter maksimum 90 dage, password/kodeord skal være af en minimumslængde på 8, indeholde tal, store og små bogstaver.

Retningslinjer for password/kodeord

Ved oprettelse af brugere skal disse tildeles en sikker midlertidig kodeord/password som skal ændres ved første login.

Opbevaring af password/kodeord

Adgangskoder må ikke opbevares i klar tekst, hverken i en digital form eller på papir.

Administrator password/kodeord, opbevares elektronisk i dokument, som er password beskyttet, og passwordet er kun kendt af TrueLinks ledelse.

Henvisning: "09 Fortegnelse over administrator - og system passwords"

Overdragelse af password/kodeord

Kodeord må aldrig overdrages eller deles med andre, eneste undtagelse er når en bruger skal logge ind første gang med midlertidige password/kodeord, hvor systemejere kan overdrage det midlertidige password/kodeord til brugeren.

9.2.5 Gennemgang af brugeradgangsrettigheder

Intern audit af brugerprofiler og rettigheder

Der er beskrevet procedure for gennemgang af bruger profiler og rettigheder i TrueLinks systemer, proceduren foreskriver, at samtlige brugerprofiler og brugergrupper gennemgås for, at sikre, at der ikke eksisterer inaktive brugere eller brugergrupper. Endvidere skal samtlige brugers rettigheder kontrolleres inklusive privilegerede rettigheder samt adgang til privilegerede systemprogrammer så det sikres at rettighedstildelingen er i overensstemmelse med brugernes forretningsmæssige behov.

Henvisning: "09.02.05 Procedure og log over intern audit af brugere og -rettigheder".

9.2.6 Inddragelse eller justering af adgangsrettigheder

Inddragelse af adgangsrettigheder

Ved ophør af et samarbejdsforhold skal brugeren som minimum deaktiveres, så adgang til TrueLinks systemer forhindres. Efter maksimum 30 dage skal brugeren fysisk slettet fra TrueLinks systemer.

Justering af adgangsrettigheder

Ved ændring af et samarbejdsforhold, skal adgangsrettigheder revurderes så rettighederne afspejler forretningsmæssige behov.

Henvisning: ”09.02 Procedure for start -, ændre - og ophør af samarbejdsforhold” og dokumentation af ”09 Fortegnelse over brugere og -rettigheder”.

9.3 Brugerens ansvar

9.3.1 Brug af hemmelig autentifikationsinformation

Brug af ens password/kodeord

Det er tilladt at benytte samme password/kodeord i TrueLinks systemer, det er ikke tilladt at benytte samme TrueLink password/kodeord på internettet som benyttes på TrueLinks system(er), f.eks. ved adgang til Facebook, privat netbank m.m. Stort genbrug af kodeord/password øger risikoen for, at fortroligheden omkring password/kodeord kan blive krænket.

Indhold i kodeord/password

Det er brugerens ansvar at gøre password så sikre som muligt, dvs. undgå fødselsdatoer, navne på venner/familie/kæledyr m.m.

Adgangskoder til TrueLinks systemer skal minimum være 8 tegn lang og skal være en kombination følgende:

- store bogstaver
- små bogstaver
- tal

Skift af kodeord/password

Adgangskoder skal skiftes minimum efter 90 dage.

”Auto Login”

Det er ikke tilladt at benytte systemer, hvor adgangskoder gemmes i genveje, funktionstaster, macroer eller lign. form for automatisk gemmefunktion.

Opbevaring af kodeord/password

Brugerens kodeord/password må aldrig forefindes i klartekst på noget medie, som f.eks. papir, i Word dokument, i Notepad dokument eller lign.

9.4 Styring af system- og applikationsadgang

9.4.1 Begrænset adgang til informationer

TrueLinks systemer giver kun adgang til information i det omfang, der er givet brugeren rettigheder til dette. Dvs. at adgang til data som er klassificeret som fortrolig eller højere begrænses adgangen i videst mulige omfang.

9.4.2 Procedurer for sikkert log-on

Adgang til TrueLinks systemer er beskyttes af sikker log-on procedure, hvor brugernavn bliver anvendt til at identificere personen som logger ind. Personen er ansvarlig for de aktiviteter, der bliver udført af personen på systemet for det pågældende log-on.

9.4.4 Brug af privilegerede systemprogrammer

Brugen af privilegerede systemprogrammer begrænses i størst muligt omfang, og tildeles kun når det er forretningsrelevant at give adgangen. Rettigheder tildeles i proceduren for start -, ændring – og ophør af samarbejdsforhold.

Henvisning: ”09.02 Procedure for start -, ændre - og ophør af samarbejdsforhold” og dokumentation af ”09 Fortegnelse over brugere og -rettigheder”.

9.4.5 Styring af adgang til kildekoder til programmer
Udviklers og brugers adgang til kildekode begrænses ved at der kun gives adgang til kildekoden for de systemer der foretages udvikling på. Rettigheder tildeles i proceduren for start -, ændring – og ophør af samarbejdsforhold

Henvisning: ”09.02 Procedure for start -, ændre - og ophør af samarbejdsforhold” og dokumentation af ”09 Fortegnelse over brugere og -rettigheder”.

Inddatamateriale som indeholder personoplysninger

4 Retningslinjer for opbevaring og sletning af data
TrueLinks systemer stilles til rådighed for kunder, hvor kunderne har inddata materiale som inddateres i TrueLinks systemer.

Opbevaring af uddata og inddata sker i TrueLinks systemer, indtil kunder giver instruks til at slette ind og/eller uddata, eller dele heraf.

Det betyder at TrueLinks retningslinje er at inddata og uddata opbevares, indtil den dataansvarlig give instruks til at der skal slettes i inddata og/eller uddata

Al data er beskyttet i.h.t. TrueLinks Informationspolitikkerne.

Uddatamateriale som indeholder personoplysninger

4 Retningslinjer for opbevaring og sletning af data
TrueLinks systemer stilles til rådighed for kunder, hvor kunderne har inddata materiale som inddateres i TrueLinks systemer.

Opbevaring af uddata og inddata sker i TrueLinks systemer, indtil kunder giver instruks til at slette ind og/eller uddata, eller dele heraf.

Det betyder at TrueLinks retningslinje er at inddata og uddata opbevares, indtil den dataansvarlig give instruks til at der skal slettes i inddata og/eller uddata

Al data er beskyttet i.h.t. TrueLinks Informationspolitikkerne.

Eksterne kommunikationsforbindelser

10.1.1 Politik for anvendelse af kryptografi.
Kommunikationsforbindelser

TrueLinks forbindelser til samarbejdspartnere foregår altid på sikre linjer enten som VPN-tunneler, HTTPS kommunikation og privat/public key, dette for at beskytte fortrolig/hemmelig/meget hemmelig information, som bliver transmitteret mellem TrueLink og samarbejdspartnere.

10.1.2 Administration af nøgler
Der er etableret et administrationssystem til nøgler, som indeholder information om alle etablerede nøgler og mellem hvilke samarbejdspartnere/points.

Kontrol med afviste adgangsforsøg

9.4.3 System for administration af adgangskoder
Ved mere end 3 på hinanden forgæves forsøg på login, lukker TrueLink systemerne brugeren ude, indtil systemejeren lukker brugeren op igen.

Såfremt en bruger er lukket ude, uden brugeren selv er skyld i dette, skal hændelsen logges i TrueLinks hændelseslog. Henvisning til: "16 TrueLinks procedure for styring af hændelser".

Logning

12.4 Logning og overvågning
12.4.1 Hændelseslogning
Logning af hændelser sker i "Registrerede hændelser", hvor TrueLink logger hændelser som observeres eller indrapporteres fra f.eks. outsourcing partnere, kunder m.m.

Henvisning til: "16 TrueLinks procedure for styring af hændelser"

Applikationslogning / logning af bruger aktivitet
TrueLinks systemer logger i applikationsloggen når brugere foretager visning, oprettelse -, ændring - eller sletning af data.

Log historik opbevares indtil TrueLinks kunder, giver instruks til, at log historik skal slettes.

12.4.2 Administrator- og operatørlog
Der foretages logning af alle handlinger udført af brugere med administratorrettigheder i forbindelse med systemkomponenter, DB, server administration m.m.

Hjemmearbejdspladser

Leverandørens behandling af personoplysninger sker helt eller delvist ved anvendelse af hjemmearbejdspladser.

6.2 Mobilt udstyr og fjernarbejdspladser
6.2.2 Fjernarbejdspladser
Kun TrueLink ejede PC'er må kobles op til TrueLink via VPN.
Udskrivning af fortrolig/hemmelig/meget hemmelig information på printere uden for TrueLinks domæne skal i størst mulige omfang undgås. I situationer, hvor det er nødvendigt, skal udskrifterne opbevares sikkert indtil makulering kan foretages på TrueLinks kontor.

BILAG 3
DEN DATAANSVARLIGES FORPLIGTELSER

1 FORPLIGTELSER

1.1 Den Dataansvarlige har følgende forpligtelser

1.1.1 Den Dataansvarlig er ansvarlig for at overholde den til enhver tid gældende persondatalovgivning i forhold til de personoplysninger, som overlades til Databehandlerens behandling. Dataansvarlig er herunder navnlig ansvarlig for og indestår for, at:

- Angivelsen i bilag 1 er udtømmende, og at Databehandleren kan agere herefter, bl.a. i forhold til fastsættelse af nødvendige sikkerhedsforanstaltninger.
- Den Dataansvarlige har fornøden hjemmel til at behandle og til at overlade det til Databehandleren at behandle de personoplysninger, der behandles i forbindelse med levering af Hovedydelserne.
- Den afgivne Instruks, i henhold til hvilken Databehandleren skal behandle personoplysninger på vegne af den Dataansvarlige, er lovlig.

1.1.2 Den Dataansvarlige orienterer skriftligt Databehandleren om eventuelt gennemførte konsekvensanalyser, der er relevante for de overladte behandlingsaktiviteter, og den Dataansvarlige giver samtidig Databehandleren fornøden indsigt i analysen med henblik på at Databehandleren kan opfylde sine forpligtigelser under Databehandleraftalen.

1.1.3 Den Dataansvarlige orienterer i øvrigt Databehandleren om forhold af betydning for Databehandleren udførelse af sine forpligtigelser under Databehandleraftalen, herunder blandt andet den Dataansvarliges løbende risikovurdering, i det omfang de er relevante for Databehandleren.

1.1.4 Den Dataansvarlige orienterer desuden Databehandleren, hvis den til enhver tid gældende persondatalovgivning i forhold til de personoplysninger, som overlades til Databehandlerens behandling, omfatter andet end lov nr. 429 af 31/05/2000 med senere ændringer om behandling af personoplysninger (Persondataloven) eller Europa-Parlamentets og Rådets forordning (EU) 2016/679 (inkl. efterfølgende tilpasninger af dansk ret, der sker som konsekvens af denne forordning).

1.1.5 Den Dataansvarlige bistår Databehandleren med at indgå aftaler med Underdatabehandlere, i det omfang det er nødvendigt, herunder for at sikre overførselsgrundlag til tredjelande.

BILAG 4
UNDERDATABEHANDLERE

1 GENERELT

1.1 Den Dataansvarlige giver hermed sin forudgående generelle godkendelse til, at Databehandleren kan gøre brug af Underdatabehandlere. Databehandleren skal skriftligt underrette den Dataansvarlige om tilføjelse eller erstatning af en Underdatabehandler forud for anvendelsens påbegyndelse. Tilsvarende skal Databehandleren underrette den Dataansvarlige om ophør af brug af en Underdatabehandler.

1.2 Databehandleren benytter følgende Underdatabehandlere:

1) A/S ScanNet.dk (CVR: 29 41 20 06)
   Drift af TrueLink A/S' løsninger
   Adresse: Højvangen 4, 8660 Skanderborg

2) TrueDevelop Sp. z o. o., PL (KRS number 0000754117, NIP 5272868353)
   Udviklingsafdeling og last level support for TrueLink A/S' løsninger
   ul. Mazowiecka 11 app. 49,00-052 Warszawa, Poland

3) Interoperabilty partner
   a) TrueCommerce ApS (VANS/EDIFACT forsendelser og modtagelser)
   b) mySupply A/S (forsendelse til Norge og andre PEPPOL lande)
   c) Inexchange AB (forsendelse og modtagelser fra Sverige og Finland)
   d) Pagero AB (forsendelse og modtagelser fra Sverige og Finland)
   e) Basware AB (forsendelse og modtagelser fra Sverige og Finland)
   f) Crediflow AB (forsendelse og modtagelser fra Sverige og Finland)

4) Microsoft Corporation – Office 365 og Driftsplatform (AZURE) for hosting og opbevaring af data. Data vil blive opbevaret indenfor EU
   Adresse: Dept. 551, Volume Licensing, 6100 Neil Road, Suite 210, Reno, Nevada 89511-1137, USA

BILAG 5
OVERFØRSEL TIL TREDJELAND OG INTERNATIONALORGANISATION

1 GENERELT

1.1 Den Dataansvarlige giver gennem accept af **TrueLink Medlemsvilkår** hermed sin bemyndigelse til, at Databehandleren kan indgå EU Standardkontraktbestemmelser eller anden form for lovligt overførselsgrundlag for overførsel af personoplysninger til et Tredjeland eller international organisation på vegne af Dataansvarlig med underleverandøren.

1.2

Virksomhed	Land eller lokation
Microsoft Gyldigt overførselsgrundlag: EU-U.S. Privacy Shield	USA