INTRANOTE

DATABEHANDLERAFTALE

Standardkontraktsbestemmelser

i henhold til artikel 28, stk. 3, i forordning 2016/679 (databeskyttelsesforordningen) med henblik på Databehandlerens behandling af personoplysninger

mellem

DN_D_KundeEmneNavn

DN_D_KundeEmneGade

DN_D_KundeEmnePostNr DN_D_KundeEmneBy

CVR. nr.: DN_D_KundeEmneCVR

(**"den Dataansvarlige"**)

og

IntraNote a/s

Papirfabrikken 20 A

8600 Silkeborg

CVR-nr. 25797620

(**"Databehandleren"**)

der hver især er en **"Part"** og sammen udgør **"Parterne"**

Har aftalt følgende standardkontraktsbestemmelser med henblik på at overholde databeskyttelsesforordningen og sikre beskyttelse af privatlivets fred og fysiske personers grundlæggende rettigheder og frihedsrettigheder (**"Databehandleraftalen"**).

INDHOLD

1. PRÆAMBEL 4
2. DEN DATAANSVARLIGES RETTIGHEDER OG FORPLIGTELSER 5
3. DATABEHANDLEREN HANDLER EFTER INSTRUKS 5
4. FORTROLIGHED 5
5. BEHANDLINGSSIKKERHED 6
6. ANVENDELSE AF UNDERDATABEHANDLERE 7
7. OVERFØRSEL TIL TREDJELANDE ELLER INTERNATIONALE ORGANISATIONER 7
8. BISTAND TIL DEN DATAANSVARLIGE 8
9. UNDERRETNING OM BRUD PÅ PERSONDATASIKKERHEDEN 9
10. SLETNING OG RETURNERING AF OPLYSNINGER 10
11. REVISION, HERUNDER INSPEKTION 10
12. PARTERNES AFTALE OM ANDRE FORHOLD 10
13. IKRAFTTRÆDEN OG OPHØR 10
14. UNDERSKRIFTER 11

Bilag A - Oplysninger om behandlingen 12

Bilag B – Underdatabehandlere 14

Bilag C – Instruks vedrørende behandling af personoplysninger 15

Bilag D - Bestemmelser vedrørende andre forhold 21

1. PRÆAMBEL

1.1 Databehandleraftalen fastsætter Databehandlerens rettigheder og forpligtelser, når denne foretager behandling af personoplysninger på vegne af den Dataansvarlige. Databehandleraftalen er udformet med henblik på Parternes efterlevelse af artikel 28, stk. 3, i Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (databeskyttelsesforordningen eller **"Forordningen"**).

1.2 Databehandleraftalen supplerer Rammeaftalen og bestemmelserne heri vedr. behandling af personoplysninger.

1.3 I forbindelse med (afhængig af aftalen med den Dataansvarlige) leveringen, udvikling, support, og videreudvikling af intranet-løsning, dokumenthåndtering og elektronisk underskrift i henhold til Parternes kontrakt (Rammeaftalen) behandler Databehandleren personoplysninger på vegne af den Dataansvarlige i overensstemmelse med indholdet af Databehandleraftalen.

1.4 Databehandleraftalen har forrang i forhold til eventuelle tilsvarende bestemmelser i andre aftaler mellem Parterne.

1.5 Der hører fire bilag til Databehandleraftalen, og bilagene udgør en integreret del heraf.

1.6 "Bilag A - Oplysninger om behandlingen" indeholder nærmere oplysninger om behandlingen af personoplysninger, herunder om behandlingens formål og karakter, typen af personoplysninger, kategorierne af registrerede og varighed af behandlingen.

1.7 "Bilag B – Underdatabehandlere" indeholder den Dataansvarliges betingelser for Databehandlerens brug af underdatabehandlere og en liste af underdatabehandlere, som den Dataansvarlige har godkendt brugen af.

1.8 "Bilag C – Instruks vedrørende behandling af personoplysninger" indeholder den Dataansvarliges instruks for så vidt angår Databehandlerens behandling af personoplysninger, en beskrivelse af de sikkerhedsforanstaltninger, som Databehandleren som minimum skal gennemføre, og hvordan der føres tilsyn med Databehandleren og eventuelle underdatabehandlere.

1.9 "Bilag D - Bestemmelser vedrørende andre forhold" indeholder bestemmelser vedrørende andre forhold, herunder erstatningsansvar og honorering.

1.10 Databehandleraftalen frigør ikke Databehandleren fra forpligtelser, som Databehandleren er pålagt efter databeskyttelsesforordningen eller enhver anden lovgivning.

2. DEN DATAANSVARLIGES RETTIGHEDER OG FORPLIGTELSER

2.1 Den Dataansvarlige er ansvarlig for at sikre, at behandlingen af personoplysninger sker i overensstemmelse med databeskyttelsesforordningen (se Forordningens artikel 24), databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes[1] nationale ret og Databehandleraftalen.

2.2 Den Dataansvarlige har ret og pligt til at træffe beslutninger om, til hvilke(t) formål og med hvilke hjælpemidler, der må ske behandling af personoplysninger.

2.3 Den Dataansvarlige er ansvarlig for, blandt andet, at sikre, at der er et behandlingsgrundlag for behandlingen af personoplysninger, som Databehandleren instrueres i at foretage.

3. DATABEHANDLEREN HANDLER EFTER INSTRUKS

3.1 Databehandleren må kun behandle personoplysninger efter dokumenteret instruks fra den Dataansvarlige, medmindre det kræves i henhold til EU-ret eller medlemsstaternes nationale ret, som Databehandleren er underlagt. Denne instruks skal være specificeret i Bilag A og C. Efterfølgende instruks kan også gives af den Dataansvarlige, mens der sker behandling af personoplysninger, men instruksen skal altid være dokumenteret og opbevares skriftligt, herunder elektronisk, sammen med Databehandleraftalen.

3.2 Databehandleren underretter omgående den Dataansvarlige, hvis en instruks efter vedkommendes mening er i strid med denne forordning eller databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret.

4. FORTROLIGHED

4.1 Databehandleren må kun give adgang til personoplysninger, som behandles på den Dataansvarliges vegne, til personer, som er underlagt Databehandlerens instruktionsbeføjelser, som har forpligtet sig til fortrolighed eller er underlagt en passende lovbestemt tavshedspligt, og kun i det nødvendige omfang. Listen af personer, som har fået tildelt adgang, skal løbende gennemgås. På baggrund af denne gennemgang kan adgangen til personoplysninger lukkes, hvis adgangen ikke længere er nødvendig, og personoplysningerne skal herefter ikke længere være tilgængelige for disse personer.

4.2 Databehandleren skal efter anmodning fra den Dataansvarlige kunne påvise, at de pågældende personer, som er underlagt Databehandlerens instruktionsbeføjelser, er underlagt ovennævnte tavshedspligt.

---

1 Henvisninger til "medlemsstat" i disse bestemmelser, skal forstås som en henvisning til "EØS medlemsstater".

5. BEHANDLINGSSIKKERHED

5.1 Databeskyttelsesforordningens artikel 32 fastslår, at den Dataansvarlige og Databehandleren, under hensyntagen til det aktuelle tekniske niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder, gennemfører passende tekniske og organisatoriske foranstaltninger for at sikre et beskyttelsesniveau, der passer til disse risici.

5.2 Den Dataansvarlige skal vurdere risiciene for fysiske personers rettigheder og frihedsrettigheder som behandlingen udgør og gennemføre foranstaltninger for at imødegå disse risici. Afhængig af deres relevans kan det omfatte:

a. Pseudonymisering og kryptering af personoplysninger.

b. Evne til at sikre vedvarende fortrolighed, integritet, tilgængelighed og robusthed af behandlingssystemer og -tjenester.

c. Evne til rettidigt at genoprette tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse.

d. En procedure for regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske foranstaltninger til sikring af behandlingssikkerhed.

5.3 Efter Forordningens artikel 32 skal Databehandleren – uafhængigt af den Dataansvarlige – også vurdere risiciene for fysiske personers rettigheder som behandlingen udgør og gennemføre foranstaltninger for at imødegå disse risici. Med henblik på denne vurdering skal den Dataansvarlige stille den nødvendige information til rådighed for Databehandleren, som gør vedkommende i stand til at identificere og vurdere sådanne risici.

5.4 Derudover skal Databehandleren bistå den Dataansvarlige med vedkommendes overholdelse af den Dataansvarliges forpligtelse efter Forordningens artikel 32, ved bl.a. at stille den nødvendige information til rådighed for den Dataansvarlige vedrørende de tekniske og organisatoriske sikkerhedsforanstaltninger, som Databehandleren allerede har gennemført i henhold til Forordningens artikel 32, og al anden information, der er nødvendig for den Dataansvarliges overholdelse af sin forpligtelse efter Forordningens artikel 32.

Hvis imødegåelse af de identificerede risici – efter den Dataansvarliges vurdering – kræver gennemførelse af yderligere foranstaltninger end de foranstaltninger, som Databehandleren allerede har gennemført, skal den Dataansvarlige angive de yderligere foranstaltninger, der skal gennemføres, i Bilag C.

6. ANVENDELSE AF UNDERDATABEHANDLERE

6.1 Databehandleren skal opfylde de betingelser, der er omhandlet i databeskyttelsesforordningens artikel 28, stk. 2, og stk. 4, for at gøre brug af en anden databehandler (en underdatabehandler).

6.2 Databehandleren må således ikke gøre brug af en underdatabehandler til opfyldelse af Databehandleraftalen uden forudgående specifik skriftlig godkendelse fra den Dataansvarlige.

6.3 Databehandleren har den Dataansvarliges generelle godkendelse til brug af underdatabehandlere. Databehandleren skal skriftligt underrette den Dataansvarlige om eventuelle planlagte ændringer vedrørende tilføjelse eller udskiftning af underdatabehandlere med mindst 30 (tredives) dages varsel og derved give den Dataansvarlige mulighed for at gøre indsigelse mod sådanne ændringer inden brugen af de(n) omhandlede underdatabehandler(e). Længere varsel for underretning i forbindelse med specifikke behandlingsaktiviteter kan angives i Bilag B. Listen over underdatabehandlere, som den Dataansvarlige allerede har godkendt, fremgår af Bilag B.

6.4 Når Databehandleren gør brug af en underdatabehandler i forbindelse med udførelse af specifikke behandlingsaktiviteter på vegne af den Dataansvarlige, skal Databehandleren, gennem en kontrakt eller andet retligt dokument i henhold til EU-retten eller medlemsstaternes nationale ret, pålægge underdatabehandleren de samme databeskyttelsesforpligtelser som dem, der fremgår af Databehandleraftalen, hvorved der navnlig stilles de fornødne garantier for, at underdatabehandleren vil gennemføre de tekniske og organisatoriske foranstaltninger på en sådan måde, at behandlingen overholder kravene i Databehandleraftalen og databeskyttelsesforordningen.

Databehandleren er derfor ansvarlig for at kræve, at underdatabehandleren som minimum overholder Databehandlerens forpligtelser efter Databehandleraftalen og databeskyttelsesforordningen.

6.5 Underdatabehandleraftale(r) og eventuelle senere ændringer hertil sendes – efter den Dataansvarliges anmodning herom – i kopi til den Dataansvarlige, som herigennem har mulighed for at sikre sig, at tilsvarende databeskyttelsesforpligtelser som følger af Databehandleraftalen er pålagt underdatabehandleren. Bestemmelser om kommercielle vilkår, som ikke påvirker det databeskyttelsesretlige indhold af underdatabehandleraftalen, skal ikke sendes til den Dataansvarlige.

6.6 Hvis underdatabehandleren ikke opfylder sine databeskyttelsesforpligtelser, forbliver Databehandleren fuldt ansvarlig over for den Dataansvarlige for opfyldelsen af underdatabehandlerens forpligtelser. Dette påvirker ikke de registreredes rettigheder, der følger af databeskyttelsesforordningen, herunder særligt Forordningens artikel 79 og 82, over for den Dataansvarlige og Databehandleren, herunder underdatabehandleren.

7. OVERFØRSEL TIL TREDJELANDE ELLER INTERNATIONALE ORGANISATIONER

7.1 Enhver overførsel af personoplysninger til tredjelande eller internationale organisationer må kun foretages af Databehandleren på baggrund af dokumenteret instruks herom fra den Dataansvarlige og skal altid ske i overensstemmelse med databeskyttelsesforordningens kapitel V.

7.2 Hvis overførsel af personoplysninger til tredjelande eller internationale organisationer, som Databehandleren ikke er blevet instrueret i at foretage af den Dataansvarlige, kræves i henhold til EU-ret eller medlemsstaternes nationale ret, som Databehandleren er underlagt, skal Databehandleren underrette den Dataansvarlige om dette retlige krav inden behandling, medmindre den pågældende ret forbyder en sådan underretning af hensyn til vigtige samfundsmæssige interesser.

7.3 Uden dokumenteret instruks fra den Dataansvarlige kan Databehandleren således ikke inden for rammerne af Databehandleraftalen:

a. overføre personoplysninger til en Dataansvarlig eller databehandler i et tredjeland eller en international organisation,
b. overlade behandling af personoplysninger til en underdatabehandler i et tredjeland, eller
c. behandle personoplysningerne i et tredjeland

7.4 Den Dataansvarliges instruks vedrørende overførsel af personoplysninger til et tredjeland, herunder det eventuelle overførselsgrundlag i databeskyttelsesforordningens kapitel V, som overførslen er baseret på, skal angives i Bilag C.6.

7.5 Databehandleraftalen skal ikke forveksles med standardkontraktsbestemmelser som omhandlet i databeskyttelsesforordningens artikel 46, stk. 2, litra c og d, og Databehandleraftalen kan ikke udgøre et grundlag for overførsel af personoplysninger som omhandlet i databeskyttelsesforordningens kapitel V.

8. BISTAND TIL DEN DATAANSVARLIGE

8.1 Databehandleren bistår, under hensyntagen til behandlingens karakter, så vidt muligt den Dataansvarlige ved hjælp af passende tekniske og organisatoriske foranstaltninger med opfyldelse af den Dataansvarliges forpligtelse til at besvare anmodninger om udøvelsen af de registreredes rettigheder som fastlagt i databeskyttelsesforordningens kapitel III.

Dette indebærer, at Databehandleren så vidt muligt skal bistå den Dataansvarlige i forbindelse med, at den Dataansvarlige skal sikre overholdelsen af:

a. oplysningspligten ved indsamling af personoplysninger hos den registrerede,
b. oplysningspligten, hvis personoplysninger ikke er indsamlet hos den registrerede,
c. indsigtsretten,
d. retten til berigtigelse,
e. retten til sletning (retten til at blive glemt),
f. retten til begrænsning af behandling,
g. underretningspligten i forbindelse med berigtigelse eller sletning af personoplysninger eller begrænsning af behandling,
h. retten til dataportabilitet,
i. retten til indsigelse, og

j. retten til ikke at være genstand for en afgørelse, der alene er baseret på automatisk behandling, herunder profilering.

8.2 I tillæg til Databehandlerens forpligtelse til at bistå den Dataansvarlige i henhold til punkt 5.4, bistår Databehandleren endvidere, under hensyntagen til behandlingens karakter og de oplysninger, der er tilgængelige for Databehandleren, den Dataansvarlige med:

a. den Dataansvarliges forpligtelse til uden unødig forsinkelse og om muligt senest 72 timer, efter at denne er blevet bekendt med det, at anmelde brud på persondatasikkerheden til den kompetente tilsynsmyndighed, Datatilsynet, medmindre at det er usandsynligt, at bruddet på persondatasikkerheden indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder,
b. den Dataansvarliges forpligtelse til uden unødig forsinkelse at underrette den registrerede om brud på persondatasikkerheden, når bruddet sandsynligvis vil medføre en høj risiko for fysiske personers rettigheder og frihedsrettigheder,
c. den Dataansvarliges forpligtelse til forud for behandlingen at foretage en analyse af de påtænkte behandlingsaktiviteters konsekvenser for beskyttelse af personoplysninger (en konsekvensanalyse), og/eller
d. den Dataansvarliges forpligtelse til at høre den kompetente tilsynsmyndighed, Datatilsynet, inden behandling, såfremt en konsekvensanalyse vedrørende databeskyttelse viser, at behandlingen vil føre til høj risiko i mangel af foranstaltninger truffet af den Dataansvarlige for at begrænse risikoen.

8.3 Parterne skal i Bilag C angive de fornødne tekniske og organisatoriske foranstaltninger, hvormed Databehandleren skal bistå den Dataansvarlige samt i hvilket omfang og udstrækning. Det gælder for de forpligtelser, der følger af punkt 8.1 og 8.2.

9. UNDERRETNING OM BRUD PÅ PERSONDATASIKKERHEDEN

9.1 Databehandleren underretter uden unødig forsinkelse den Dataansvarlige efter at være blevet opmærksom på, at der er sket et brud på persondatasikkerheden.

9.2 Databehandlerens underretning til den Dataansvarlige skal om muligt ske senest 24 timer efter, at denne er blevet bekendt med bruddet, sådan at den Dataansvarlige kan overholde sin forpligtelse til at anmelde bruddet på persondatasikkerheden til den kompetente tilsynsmyndighed, jf. databeskyttelsesforordningens artikel 33.

9.3 I overensstemmelse med punkt 8.2.a skal Databehandleren bistå den Dataansvarlige med at foretage anmeldelse af bruddet til den kompetente tilsynsmyndighed. Det betyder, at Databehandleren skal bistå med at tilvejebringe nedenstående informationer, som ifølge artikel 33, stk. 3, skal fremgå af den Dataansvarliges anmeldelse af bruddet til den kompetente tilsynsmyndighed:

a. karakteren af bruddet på persondatasikkerheden, herunder, hvis det er muligt, kategorierne og det omtrentlige antal berørte registrerede samt kategorierne og det omtrentlige antal berørte registreringer af personoplysninger,
b. de sandsynlige konsekvenser af bruddet på persondatasikkerheden, og
c. de foranstaltninger, som den Dataansvarlige har truffet eller foreslår truffet for at håndtere bruddet på persondatasikkerheden, herunder, hvis det er relevant, foranstaltninger for at begrænse dets mulige skadevirkninger.

9.4 Parterne skal i Bilag C angive den information, som Databehandleren skal tilvejebringe i forbindelse med sin bistand til den Dataansvarlige i dennes forpligtelse til at anmelde brud på persondatasikkerheden til den kompetente tilsynsmyndighed.

10. SLETNING OG RETURNERING AF OPLYSNINGER

10.1 Der henvises til Bilag C. pkt. 4, hvor forhold vedr. sletning er særskilt behandlet.

11. REVISION, HERUNDER INSPEKTION

11.1 Databehandleren stiller alle oplysninger, der er nødvendige for at påvise overholdelsen af databeskyttelsesforordningens artikel 28 og 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.

11.2 Procedurerne for den Dataansvarliges revisioner, herunder inspektioner, med Databehandleren og underdatabehandlere er nærmere angivet i Bilag C.7. og C.8.

11.3 Databehandleren er forpligtet til at give tilsynsmyndigheder, som efter gældende lovgivningen har adgang til den Dataansvarliges eller Databehandlerens faciliteter, eller repræsentanter, der optræder på tilsynsmyndighedens vegne, adgang til Databehandlerens fysiske faciliteter mod behørig legitimation.

12. PARTERNES AFTALE OM ANDRE FORHOLD

12.1 Parterne kan aftale andre bestemmelser vedrørende tjenesten vedrørende behandling af personoplysninger om f.eks. erstatningsansvar, så længe disse andre bestemmelser ikke direkte eller indirekte strider imod Databehandleraftalen eller forringer den registreredes grundlæggende rettigheder og frihedsrettigheder, som følger af databeskyttelsesforordningen.

13. IKRAFTTRÆDEN OG OPHØR

13.1 Databehandleren har mulighed for at opdatere Databehandleraftalen, eventuelt på baggrund af ændringer i lovgivning, markedsforhold eller interne processer hos Databehandleren.

13.2 Den til enhver tid gældende version af Databehandleraftalen er tilgængelig på Databehandlerens hjemmeside www.intranote.dk/compliance/databehandleraftale

13.3 Begge Parter kan kræve Databehandleraftalen genforhandlet, hvis lovændringer eller uhensigtsmæssigheder Databehandleraftalen giver anledning hertil.

13.4 Databehandleraftalen er gældende, så længe tjenesten vedrørende behandling af personoplysninger varer. I denne periode kan Databehandleraftalen ikke opsiges, medmindre andre bestemmelser, der regulerer levering af tjenesten vedrørende behandling af personoplysninger, aftales mellem Parterne.

13.5 Hvis levering af tjenesterne vedrørende behandling af personoplysninger ophører, og personoplysningerne er slettet eller returneret til den Dataansvarlige i overensstemmelse med punkt 10 og Bilag C.4, kan Databehandleraftalen opsiges med et skriftligt varsel på 30 dage af begge Parter.

14. UNDERSKRIFTER

Underskrevet på vegne af den Dataansvarlige
DN_D_KundeEmneNavn



af

DN_D_Kontraktansvarlig_Navn
DN_D_Kontraktansvarlig_Stilling

Underskrevet på vegne af Databehandleren
IntraNote A/S



af

DN_D_Underskriver_Navn
DN_D_Underskriver_Stilling

Bilag A - Oplysninger om behandlingen

A.1. Formålet med Databehandlerens behandling af personoplysninger på vegne af den Dataansvarlige

Behandlingen af den Dataansvarliges oplysninger sker i henhold til formålet i Rammeaftalen.

A.2. Databehandlerens behandling af personoplysninger på vegne af den Dataansvarlige drejer sig primært om (karakteren af behandlingen)

Behandlingen vil – afhængigt af Rammeaftalen med den Dataansvarlige og de ydelser, Databehandleren skal levere – ske i forbindelse med følgende aktiviteter:

- Konsulentbistand efter aftale
- Produktsupport og fejlfinding efter aftale
- Udviklingsopgaver efter aftale
- Hosting af løsningen, såfremt dette fremgår af Rammeaftalen
- IntraNote Signing, hvis dette tages i brug.

A.3. Behandlingen omfatter følgende typer af personoplysninger om de registrerede

A.3.1. Almindelige personoplysninger

Databehandleren vil behandle almindelige personoplysninger på vegne af den Dataansvarlige. De specifikke oplysninger, som behandles, afhænger af aftalen med den Dataansvarlige og de ydelser, Databehandleren skal levere, herunder den Dataansvarliges anvendelse heraf. Personoplysninger kan (ikke udtømmende) f.eks. være:

- Navn, køn, stillingsbetegnelse, fødselsdato, brugernavn, initialer, kontaktoplysninger, korrespondance i mails, support tickets og lignende, IP-adresse og andet metadata tilhørende signerede dokumenter, underskrifter i signerede dokumenter og andre typer af personoplysninger, som kunden eller de registrerede registrerer i den relevante løsning.

A.3.2. Følsomme personoplysninger (jf. Databeskyttelsesforordningens artikel 9):

Databehandleren kan efter omstændighederne behandle særlige kategorier (følsomme) personoplysninger på vegne af den Dataansvarlige. De specifikke følsomme personoplysninger, som behandles, afhænger af aftalen med den Dataansvarlige og de ydelser, Databehandleren skal levere, herunder den Dataansvarliges anvendelse heraf.

Særlige kategorier af personoplysninger (følsomme personoplysninger) omfattet af databeskyttelsesforordningens artikel 9 udgør racemæssig eller etnisk baggrund, politisk overbevisning, religiøs overbevisning, filosofisk overbevisning, fagforeningsmæssigt tilhørsforhold, helbredsforhold eller seksuelle forhold.

A.3.3. Oplysninger om strafbare forhold (jf. Databeskyttelsesforordningens artikel 10):

Databehandleren kan efter omstændighederne behandle personoplysninger om strafbare forhold på vegne af den Dataansvarlige. De specifikke personoplysninger, som behandles, afhænger af aftalen med den Dataansvarlige og de ydelser, Databehandleren skal levere, herunder den Dataansvarliges anvendelse heraf.

A.3.4. Oplysninger om CPR-nummer (jf. Databeskyttelsesloven § 11, stk. 2, nr. 3):

Databehandleren kan efter omstændighederne behandle CPR-numre på vegne af den Dataansvarlige. Om dette konkret er tilfældet, afhænger af aftalen med den Dataansvarlige og de ydelser, Databehandleren skal levere, herunder den Dataansvarliges anvendelse heraf.

A.4. Behandlingen omfatter følgende kategorier af registrerede

Databehandleren kan efter omstændighederne behandle personoplysninger om en række forskellige typer af registrerede på vegne af den Dataansvarlige. De specifikke registrerede, der behandles personoplysninger om, afhænger af aftalen med den Dataansvarlige og de ydelser, Databehandleren skal levere, herunder den Dataansvarliges anvendelse heraf. De registrerede kan f.eks. være (ikke udtømmende):

- Kunder
- Leverandører
- Kontaktoplysninger på ansatte hos kunder og leverandører
- Ansøgere
- Personer, hvis personoplysninger fremgår af signede dokumenter
- Andre typer af registrerede, som den Dataansvarlige behandler personoplysninger om afhængig af ydelsen til den Dataansvarlige og den Dataansvarliges virksomhed mv.

A.5. Databehandlerens behandling af personoplysninger på vegne af den Dataansvarlige kan påbegyndes efter Databehandleraftalens ikrafttræden. Behandlingen har følgende varighed:

Behandlingen vil forestå indtil ydelsen ophører i henhold til Rammeaftalen.

Bilag B – Underdatabehandlere

Den Dataansvarlige har ved databehandleraftalens ikrafttræden specifikt godkendt anvendelse af de linkede underdatabehandlere. Listen med godkendte underdatabehandlere forefindes her: www.intranote.dk/compliance/databehandleraftale-bilag-b

Bilag C – Instruks vedrørende behandling af personoplysninger

C.1. Behandlingens genstand/instruks

Databehandlerens behandling af personoplysninger på vegne af den Dataansvarlige sker ved, at Databehandleren udfører følgende:

- Behandlingen vil ske i forbindelse med aktiviteterne, som beskrevet i Bilag A.2.

Særligt i forbindelse med support har den Dataansvarlige og Databehandleren aftalt, at den Dataansvarlige skal anonymisere personoplysninger, som ikke er nødvendige for opgaveløsningen, i forbindelse med indgivelse af support tickets til Databehandleren, således der ikke er personoplysninger på f.eks. skærmbilleder, som ikke er nødvendige. Hvis den Dataansvarlige overlader personoplysninger til Databehandleren, som ikke er nødvendige for, at Databehandleren kan udføre support, anonymiserer Databehandleren oplysningerne efter bedste evne, jf. pkt. C.4 nedenfor.

C.2. Behandlingssikkerhed

Sikkerhedsniveauet skal afspejle:

Behandlingen kan omfatte en større mængde personoplysninger, herunder (afhængig af den ydelse, Databehandleren leverer til den Dataansvarlige og den Dataansvarliges anvendelse heraf) oplysninger omfattet af databeskyttelsesforordningens artikel 9 og 10, hvorfor der skal etableres et højt sikkerhedsniveau.

Databehandleren er herefter berettiget og forpligtet til at træffe beslutninger om, hvilke tekniske og organisatoriske sikkerhedsforanstaltninger, der skal gennemføres for at etablere det nødvendige (og aftalte) sikkerhedsniveau.

Foranstaltningerne gennemføres for at undgå, at personoplysninger:

- tilintetgøres, mistes, ændres eller forringes,
- kommer til uvedkommendes kendskab eller misbruges,
- eller i øvrigt behandles i strid med lovgivningen.

Databehandleren har derfor implementeret følgende foranstaltninger:

Generelle sikkerhedsforanstaltninger:

Databehandleren yder support og vedligehold på Databehandlerens produkter i henhold til Rammeaftalen og på baggrund af interne politikker og forretningsgange.

I forbindelse med opgaveløsningen kan supportmedarbejdere og konsulenter få adgang til persondata. Support- og konsulentopgaver udføres kun efter direkte instruks fra den Dataansvarlige (Oprettelse af supportsag eller konsulentopgave).

Slutbrugersupport vil altid kræve brugerens medvirken og accept. Ved support og konsulentopgaver på den Dataansvarliges (hostede) servermiljø kontaktes den Dataansvarlige altid i forvejen.

Autorisation og adgangskontrol

- Kun autoriseret personale har adgang til kundens systemer. Navne på autoriserede medarbejdere oplyses på anfordring og fremgår af det til enhver tid gældende organisationsdiagram og reguleres i rettighedsgrupper i Databehandlerens AD.

Inddatamateriale som indeholder personoplysninger

- Databehandleren kan komme i besiddelse af inddata i form af skærmprints, der anvendes til fejlbeskrivelser i forbindelser med løsning af supportsager eller konfiguration af systemet. Sådanne data tilknyttes den enkelte sag og slettes når sagen lukkes.

Uddatamateriale som indeholder personoplysninger

- Databehandleren kan komme i besiddelse af uddata i form af skærmprints, der anvendes til fejlbeskrivelser i forbindelser med løsning af support sager eller test af konfigurationer. Sådanne data tilknyttes den enkelte sag og slettes når sagen lukkes.

Kontrol med afviste adgangsforsøg

- Bruger-login og forsøg herpå logges maskinelt. Der er opsat regler for spærring af brugeren ved gentagne mislykkede forsøg.

Logning

- For enhver opgave føres der en intern log, der beskriver:
  - Opgavens formål
  - Hvem, der har haft adgang
  - Hvilket tidsrum, der er har været adgang
  - (Herudover logges aktivitet på serverniveau (maskinelt)).

Organisatoriske sikkerhedsforanstaltninger (overordnet)

- Interne politikker og procedurer, der sikrer beskyttelse af personoplysninger og IT-sikkerhed
- Fortegnelse over behandlingsaktiviteter
- Løbende awareness træning af medarbejdere
- Beredskabsplan og plan for håndtering af brud og log ved databrud
- Plan for kontroller af organisatoriske og tekniske foranstaltninger til overholdelse af databeskyttelsesforordningen og best-practice (vedr. IT-sikkerhed)
- Kontrol med underdatabehandlere.

Særligt om hjemmearbejdspladser

- Databehandlerens behandling af personoplysninger sker helt eller delvist ved anvendelse af hjemmearbejdspladser.
- Ved arbejde fra hjemmet anvender Databehandlerens ansatte vpn-forbindelser og "fjernskrivebord", hvorfra interaktion med den Dataansvarliges systemer foregår. Derved er adgangen underlagt samme rutiner som ovenfor beskrevet. Der anvendes kun PC'ere, der er stillet til rådighed af Databehandleren. PC'en er krypteret og har det nødvendige sikkerhedsniveau ift. patch af styresystem og opdaterede antivirus suiter.

Sikkerhed hos Creative Quarter Inc.

- Som det fremgår ovenfor, anvender Databehandleren Creative Quarters Inc. som databehandler. Der overføres dog ingen personoplysninger til USA, jf. afsnit C.5 nedenfor. De personer hos Creative Quarters Inc, som foretager supportering, fejlfinding, og opdatering mv. som beskrevet i Bilag B.1 ovenfor hos Creative Quarters Inc. (inklusive selskabets underdatabehandlere) anvender alene it-udstyr udleveret af Databehandleren til at behandle personoplysninger på vegne af den Dataansvarlige, herunder ved brug af VPN-forbindelse. Med andre ord er Creative Quarter Inc. underlagt samme sikkerhedsforanstaltninger som Databehandleren selv. Den Dataansvarlige har mulighed for at fravælge anvendelsen af Creative Quarter Inc. I den forbindelse accepterer den Dataansvarlige, at de ydelser, som skulle have leveret fra den pågældende Databehandler, ikke kan leveres af Databehandleren.

Øvrige sikkerhedsforanstaltninger på løsninger fra Databehandleren:

Databehandleren har – ud over ovenstående sikkerhedsforanstaltninger – implementeret følgende tekniske foranstaltninger vedr. enhver løsning, som Databehandleren – i overensstemmelse med Parternes aftale kan levere til den Dataansvarlige:

IntraNote Signing (altid hostet)

- AES 256 bit-kryptering for personoplysninger "at rest"
- HTTPS med TLS 1.2-kryptering for personoplysninger "in transit"
- SQL er altid krypteret (personoplysninger i databasen er altid krypteret)
- SQL IP Whitelisting

IntraNote WorkSpace (Ved hosting hos IntraNote)

- TLS 1.2-kryptering for personoplysninger "in transit"

DocuNote (Ved hosting hos IntraNote)

- TLS 1.2-kryptering for personoplysninger "in transit"

DocuNote Web (Ved hosting hos IntraNote)

- TLS 1.2-kryptering for personoplysninger "in transit"
- Two factor authentification (hvis tilvalgt af kunden)

FreshDesk (support)

- AES 256 bit-kryptering for personoplysninger "at rest"
- HTTPS med TLS 1.2-kryptering for personoplysninger "in transit"
- Virtual Private Cloud
- Malware- and spam-beskyttelse
- Flere oplysninger tilgængelige her: https://www.freshworks.com/security/

TeamViewer (support)

- RSA private-/public key exchange og AES (256 bit) sessionskryptering

C.3 Bistand til den Dataansvarlige

Databehandleren skal så vidt muligt – inden for det nedenstående omfang og udstrækning – bistå den Dataansvarlige i overensstemmelse Databehandleraftalens punkt 8.1 og 8.2 ved at gennemføre følgende tekniske og organisatoriske foranstaltninger:

Databehandleren bistår, under hensyntagen til behandlingens karakter, så vidt muligt den Dataansvarlige ved hjælp af passende tekniske og organisatoriske foranstaltninger med opfyldelse af den Dataansvarliges forpligtelse til at besvare anmodninger om udøvelsen af de registreredes rettigheder som fastlagt i databeskyttelsesforordningens kapitel III.

Databehandleren skal videresende anmodninger i henhold til databeskyttelsesforordningens kapitel III til den Dataansvarlige uden unødig forsinkelse med henblik på den Dataansvarliges besvarelse af anmodningen, med mindre den Dataansvarlige specifikt giver en anden instruks.

Omfanget af Databehandlerens assistance i forbindelse med håndtering af brud på persondatasikkerheden vil afhænge af til, hvilken grad at Databehandleren har adgang til de personoplysninger, som den Dataansvarlige behandler og som bruddet vedrører.

C.4 Opbevaringsperiode/sletterutine

Generelt

Den Dataansvarlige træffer beslutning om, hvorvidt der skal ske sletning eller tilbagelevering af personoplysningerne efter, at behandlingen af personoplysningerne er ophørt i medfør af Rammeaftalen.

Den Dataansvarlige skal senest 45 dage inden Rammeaftalens ophør skriftligt meddele Databehandleren, hvorvidt alle personoplysningerne skal slettes eller tilbageleveres til den Dataansvarlige. Såfremt Databehandleren ikke modtager en sådan skriftlig meddelelse, skal Databehandleren af egen drift slette personoplysningerne hurtigst muligt efter Rammeaftalens ophør.

I det tilfælde, hvor personoplysningerne tilbageleveres til den Dataansvarlige, skal Databehandleren ligeledes slette eventuelle kopier. Databehandleren skal sikre, at eventuelle underdatabehandlere ligeledes efterlever

den Datasvarliges meddelelse. Evt. omkostninger forbundet med tilbageleveringen betales af den Dataansvarlige.

- Særligt vedr. uddatamateriale som indeholder personoplysninger
    - Databehandleren kan komme i besiddelse af uddata i form af skærmprints, der anvendes til fejlbeskrivelser i forbindelser med løsning af support sager eller test af konfigurationer. Sådanne data tilknyttes den enkelte sag og slettes når sagen lukkes.
- Anden sletning og anonymisering
    - Hvis Databehandleren modtager personoplysninger, som ikke (længere) er nødvendige for, at Databehandleren kan udføre sin ydelse til den Dataansvarlige, sletter eller anonymiserer Databehandleren personoplysningerne så hurtigt som muligt og efter "best practice". Dette gælder f.eks. personoplysninger i tickets eller om tidligere brugere. Support tickets slettes senest 5 år efter lukningen af den relevante ticket. I særlige tilfælde kan en ticket opbevares længere, f.eks. af hensyn til en verserende sag mv.

C.5 Lokalitet for behandling

Behandling af de af Databehandleraftalen omfattede personoplysninger kan ikke uden den Dataansvarliges forudgående skriftlige godkendelse ske på andre lokaliteter end følgende:

- IntraNote A/S, Papirfabrikken 20 A, 8600 Silkeborg
- IntraNote Polen, Generation Park Z, Towarowa 28, 00-839 Warszawa
- HAL7, Hørskætten 5, 2630 Taastrup (hvis hosting anvendes)
- Behandlingslokationer anvendt af Databehandlerens underdatabehandlere og disses egne underdatabehandlere, jf. Bilag B.1.

Efter anmodning skal Databehandleren udlevere dokumentation om behandlingsfaciliteter, datacentre mv. anvendt af Databehandlerens underdatabehandlere.

C.6 Instruks vedrørende overførsel af personoplysninger til tredjelande

Hvis den Dataansvarlige ikke i Databehandleraftalen eller efterfølgende giver en dokumenteret instruks vedrørende overførsel af personoplysninger til et tredjeland, er Databehandleren ikke berettiget til inden for rammerne af Databehandleraftalen at foretage sådanne overførsler.

Den Dataansvarlige har autoriseret Databehandleren til at overføre personoplysninger til Databehandlerens underdatabehandleren som angivet i Bilag B.1 i det omfang sådanne underdatabehandlere (eller underdatabehandlerens underdatabehandlere) behandler personoplysninger i tredjelande.

Den Dataansvarliges evt. instruks vedr. yderligere overførsler til tredjelande skal følge processen i Databehandleraftalens punkt 6.3 og Bilag B.2.

Databehandleren indestår for overførslers lovlighed, herunder at sikre et gyldigt overførselsgrundlag og foretage alle nødvendige vurderinger i forbindelse med overførsler.

C.7 Procedurer for den Dataansvarliges revisioner, herunder inspektioner, med behandlingen af personoplysninger, som er overladt til Databehandleren

Databehandleren indhenter med rimelige mellemrum og mindst én gang årligt en revisionserklæring fra en uafhængig tredjepart angående Databehandlerens overholdelse af databeskyttelsesforordningens artikel 28. Erklæringen skal mindst leve op til ISAE 3000-standarden. Databehandleren skal efter anmodning fra den Dataansvarlige fremsende den seneste udgave af sådan revisionserklæring til den Dataansvarlige.

Den Dataansvarlige kan endvidere for egen regning udpege en uafhængig tredjepart, som skal have adgang til Databehandlerens behandlingsfaciliteter og modtage den fornødne information med henblik på at vurdere, om Databehandleren overholder databeskyttelsesforordningens artikel 28 og Databehandleraftalen. Denne uafhængige tredjepart skal efter Databehandlerens anmodning underskrive en fortrolighedsaftale, hvorefter denne forpligter sig til at behandle al information modtaget fra Databehandleren fortroligt og alene videregive oplysninger til den Dataansvarlige.

Ønsker den Dataansvarlige i øvrigt at føre tilsyn med Databehandleren på måder, som ikke fremgår af ovenstående, herunder f.eks. udfyldelse af spørgeskemaer, self-audits mv., skal Databehandleren kompenseres herfor efter medgået tid i henhold til Databehandlerens sædvanlige timetakster, jf. også Bilag D - Bestemmelser vedrørende andre forhold.

C.8 Procedurer for revisioner, herunder inspektioner, med behandling af personoplysninger, som er overladt til underdatabehandlere

Databehandleren har implementeret procedurer for tilsyn med underdatabehandlere, hvor tilsyn varetages i henhold til den identificerede risiko samt indhentelse og gennemgang af tredjepartserklæringer – der tilsammen sikrer, at personoplysninger bliver opbevaret af underdatabehandleren på sikker og forsvarlig vis, hvor uvedkommende ikke kan få adgang.

Bilag D - Bestemmelser vedrørende andre forhold

Kompensation til Databehandleren

Databehandleren skal modtage kompensation for Databehandlerens assistance til den Dataansvarlige efter Databehandleraftalen og databeskyttelsesforordningen.

Kompensationen omfatter f.eks. assistance efter Databehandleraftalens punkt 9.1 og 9.2 (besvarelse af anmodninger fra registrerede, håndtering af brud på persondatasikkerheden, assistance med konsekvensanalyser, høring af Datatilsynet mv.) og sletning og tilbagelevering af personoplysninger i overensstemmelse med punkt 11.

Databehandleren er ikke berettiget til kompensation i det omfang Databehandlerens assistance til den Dataansvarlige er blevet gjort nødvendig som følge af Databehandlerens manglende overholdelse af Databehandleraftalen eller databeskyttelsesforordningen.

Databehandleren har ret til kompensation for ændringer i Databehandlerens behandlingsaktiviteter, herunder sikkerhedsforanstaltninger, som skyldes en ændring i instruksen fra den Dataansvarlige, med mindre sådanne ændringer er påkrævet i henhold til lovgivningen.

Kompensationen til Databehandleren skal honoreres i overensstemmelse med Databehandlerens øvrige honorar fra den Dataansvarlige.

Der er med Databehandleraftalen ikke taget stilling til den Dataansvarliges betaling for de ydelser, som Databehandleren skal levere i henhold til Parternes Rammeaftalen.

Erstatningsansvar
Spørgsmål om erstatningsansvar skal vurderes efter Parternes Rammeaftale.

Det understreges i den forbindelse, at den Dataansvarlige er erstatningsansvarlig over for Databehandleren for evt. ulovlige instrukser til Databehandleren.

Tvister, lovvalg og værneting
Spørgsmål om lovvalg og værneting skal vurderes efter Parternes Rammeaftale.

Databehandleraftalen er senest opdateret den 24. september 2024.

***