

Standardkontraktbestemmelser

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

mellem

IT Relation A/S
CVR 27001092
Dalgas Plads 7,1
7400 Herning
Danmark

herefter "Databehandleren"

og

Nasure A/S
CVR 35 47 25 25
Rødovrevej 253C
2610 Rødovre

Bemærk ny adresse pr. 1/10
Torsted alle 67
8700 Horsens
Danmark

herefter "Underdatabehandleren"

der hver især er en "part" og sammen udgør "parterne"

HAR AFTALT følgende standardkontraktbestemmelser (Bestemmelserne) med henblik på at overholde databeskyttelsesforordningen og sikre beskyttelse af privatlivets fred og fysiske personers grundlæggende rettigheder og frihedsrettigheder

1. Indhold	
2. Præambel.....	3
3. Databehandlerens forpligtelser	3
4. Behandling efter instruks.....	4
5. Fortrolighed	4
6. Behandlingssikkerhed	4
7. Underdatabehandlerens anvendelse af andre databehandlere	5
8. Overførsel til tredjelande eller internationale organisationer	6
9. Bistand til Databehandleren og den Dataansvarlige	7
10. Underretning om brud på persondatasikkerheden	8
11. Sletning og returnering af oplysninger	8
12. Revision, herunder inspektion	9
13. Parternes aftale om andre forhold.....	9
14. Ikrafttræden og ophør	9
15. Kontaktpersoner hos Databehandleren og Underdatabehandleren.....	10
Bilag A Oplysninger om behandlingen	11
Bilag B Underdatabehandlere	13
Bilag C Instruks vedrørende behandling af personoplysninger	15
C.7.1 Egenkontrol.....	16
C.7.2 Skriftligt tilsyn og fysisk inspektion	17
Bilag D Parternes regulering af andre forhold	18
D. 2 Konsekvenser af Databehandlerens ulovlige instruks	18
D.6 Sletning og returnering af oplysninger	19
D.7 Vederlag.....	Fejl! Bogmærke er ikke defineret.
D.8 Ansvar og misligholdelse	19

2. Præambel

1. Disse Bestemmelser fastsætter Databehandlerens rettigheder og forpligtelser, der finder anvendelse, når det overlades til Underdatabehandleren at foretager behandling af personoplysninger på vegne af Databehandleren.
2. Disse bestemmelser 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).
3. I forbindelse med leveringen af tjeneste omfattet af parternes aftale (Hovedaftale) om EDI Portalen ("tjenesten") behandler Underdatabehandleren personoplysninger på vegne af Databehandleren i overensstemmelse med disse Bestemmelser.
4. Bestemmelserne har forrang i forhold til eventuelle tilsvarende bestemmelser i andre aftaler mellem parterne.
5. Der hører fire bilag til disse Bestemmelser, og bilagene udgør en integreret del af Bestemmelserne.
6. Bilag A indeholder nærmere oplysninger om behandlingen af personoplysninger, herunder om behandlingens formål og karakter, typen af personoplysninger, kategorierne af registrerede og varighed af behandlingen.
7. Bilag B indeholder Databehandlerens betingelser for Underdatabehandlerens brug af andre underdatabehandlere og en liste af de andre underdatabehandlere, som Databehandleren har godkendt brugen af.
8. Bilag C indeholder Databehandlerens instruks for så vidt angår Underdatabehandlerens behandling af personoplysninger, en beskrivelse af de sikkerhedsforanstaltninger, som Underdatabehandleren som minimum skal gennemføre, og hvordan der føres tilsyn med Underdatabehandleren og eventuelle andre underdatabehandlere.
9. Bilag D indeholder bestemmelser vedrørende andre aktiviteter, som ikke er omfattet af Bestemmelserne.
10. Bestemmelserne med tilhørende bilag skal opbevares skriftligt, herunder elektronisk, af begge parter.
11. Disse Bestemmelser frigør ikke Underdatabehandleren fra forpligtelser, som Underdatabehandleren er pålagt efter databeskyttelsesforordningen eller enhver anden lovgivning.

3. Databehandlerens forpligtelser

1. Databehandleren er ansvarlig for, at alle instrukser afgivet til Underdatabehandleren, herunder tredjelandsoverførelser og anvendelse af yderligere underdatabehandlere, er i overensstemmelse med de instrukser, som den Dataansvarlige har afgivet til Databehandleren.

4. Behandling efter instruks

1. Underdatabehandleren må kun behandle personoplysninger efter dokumenteret instruks fra Databehandleren, medmindre det kræves i henhold til EU-ret eller medlemsstaternes nationale ret, som Underdatabehandleren er underlagt. Denne instruks skal være specificeret i bilag A og C. Efterfølgende instruks kan også gives af Databehandleren, mens der sker behandling af personoplysninger, men instruksen skal altid være dokumenteret og opbevares skriftligt, herunder elektronisk, sammen med disse Bestemmelser.
2. Ved behandling af personoplysninger udenfor den fastsatte instruks skal Underdatabehandleren underrette Databehandleren om årsagen hertil. Underretningen skal ske, inden behandlingen foretages, og skal indeholde en henvisning til de retlige krav, der ligger til grund for behandlingen. Underretningen skal dog ikke ske, hvis underretningen vil være i strid med EU-retten eller den nationale ret.
3. Underdatabehandleren underretter omgående Databehandleren, hvis en instruks efter vedkommendes mening er i strid med denne forordning eller databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret.

5. Fortrolighed

1. Underdatabehandleren må kun give adgang til personoplysninger, som behandles på Databehandlerens vegne, til personer, som er underlagt Underdatabehandlerens 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.
2. Underdatabehandleren skal efter anmodning fra Databehandleren kunne påvise, at de pågældende personer, som er underlagt Underdatabehandlerens instruktionsbeføjelser, er underlagt ovennævnte tavshedspligt.

6. Behandlingssikkerhed

1. Databeskyttelsesforordningens artikel 32 fastslår, at Databehandleren og Underdatabehandleren, 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.

Databehandleren 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.
2. Efter forordningens artikel 32 skal Underdatabehandleren – uafhængigt af Databehandleren – også vurdere risiciene for fysiske personers rettigheder som behandlingen udgør og gennemføre foranstaltninger for at imødegå disse risici. Med henblik på denne vurdering skal Databehandleren stille den nødvendige information til rådighed for Underdatabehandleren som gør vedkommende i stand til at identificere og vurdere sådanne risici.
3. Derudover skal Underdatabehandleren bistå Databehandleren med vedkommendes overholdelse af Databehandlerens forpligtelse efter forordningens artikel 32, ved bl.a. at stille den nødvendige information til rådighed for Databehandleren vedrørende de tekniske og organisatoriske sikkerhedsforanstaltninger, som Underdatabehandleren allerede har gennemført i henhold til forordningens artikel 32, og al anden information, der er nødvendig for Databehandlerens overholdelse af sin forpligtelse efter forordningens artikel 32.

Hvis imødegåelse af de identificerede risici – efter Databehandlerens vurdering – kræver gennemførelse af yderligere foranstaltninger end de foranstaltninger, som Underdatabehandleren allerede har gennemført, skal Databehandlerne angive de yderligere foranstaltninger, der skal gennemføres, i bilag C.

7. Underdatabehandlerens anvendelse af andre databehandlere

1. Underdatabehandleren 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).
2. Underdatabehandleren må kun gøre brug af andre underdatabehandlere med Databehandlerens forudgående specifikke skriftlige godkendelse. Underdatabehandleren skal indgive anmodningen om en specifik godkendelse mindst 60 dage inden anvendelsen af den pågældende underdatabehandler. Listen over andre underdatabehandlere, som Databehandleren allerede har godkendt, fremgår af bilag B.
3. Underdatabehandleren må således ikke gøre brug af andre underdatabehandlere til opfyldelse af disse Bestemmelser uden forudgående specifik skriftlig godkendelse fra Databehandleren.
4. Når Underdatabehandleren gør brug af en anden underdatabehandler i forbindelse med udførelse af specifikke behandlingsaktiviteter på vegne Databehandleren, skal Underdatabehandleren, gennem en kontrakt eller andet retligt dokument i henhold til EU-retten eller medlemsstaternes nationale ret, pålægge den anden underdatabehandler de samme databeskyttelsesforpligtelser som dem, der fremgår af disse Bestemmelser, hvorved der navnlig stilles de fornødne garantier for, at den anden

underdatabehandler vil gennemføre de tekniske og organisatoriske foranstaltninger på en sådan måde, at behandlingen overholder kravene i disse Bestemmelser og databeskyttelsesforordningen.

Underdatabehandleren er derfor ansvarlig for at kræve, at den anden underdatabehandler som minimum overholder Underdatabehandlerens forpligtelser efter disse Bestemmelser og databeskyttelsesforordningen.

5. Underdatabehandleraftale(r) og eventuelle senere ændringer hertil sendes – efter Databehandlerens anmodning herom – i kopi til Databehandleren, som herigennem har mulighed for at sikre sig, at tilsvarende databeskyttelsesforpligtelser som følger af disse Bestemmelser er pålagt den anden underdatabehandler. Bestemmelser om kommercielle vilkår, som ikke påvirker det databeskyttelsesretlige indhold af underdatabehandleraftalen, skal ikke sendes til Databehandleren.
6. Hvis den anden underdatabehandler ikke opfylder sine databeskyttelsesforpligtelser, forbliver Underdatabehandleren fuldt ansvarlig over for Databehandleren for opfyldelsen af den anden 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 og dennes andre underdatabehandlere.

8. Overførsel til tredjelande eller internationale organisationer

1. Enhver overførsel af personoplysninger til tredjelande eller internationale organisationer må kun foretages af Underdatabehandleren på baggrund af dokumenteret instruks herom fra Databehandleren og skal altid ske i overensstemmelse med databeskyttelsesforordningens kapitel V.
2. Hvis overførsel af personoplysninger til tredjelande eller internationale organisationer, som Underdatabehandleren ikke er blevet instrueret i at foretage af Databehandleren, kræves i henhold til EU-ret eller medlemsstaternes nationale ret, som Underdatabehandleren er underlagt, skal Underdatabehandleren underrette Databehandleren om dette retlige krav inden behandling, medmindre den pågældende ret forbyder en sådan underretning af hensyn til vigtige samfundsmæssige interesser.
3. Uden dokumenteret instruks fra Databehandleren kan Underdatabehandleren således ikke inden for rammerne af disse Bestemmelser:
 - 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
 - c. behandle personoplysningerne i et tredjeland
4. Databehandlerens 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.
5. Disse Bestemmelser skal ikke forveksles med standardkontraktbestemmelser som omhandlet i databeskyttelsesforordningens artikel 46, stk. 2, litra c og d, og disse Bestemmelser kan ikke udgøre

et grundlag for overførsel af personoplysninger som omhandlet i databeskyttelsesforordningens kapitel V.

9. Bistand til Databehandleren og den Dataansvarlige

1. Underdatabehandleren bistår, under hensyntagen til behandlingens karakter, så vidt muligt Databehandleren og 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 Underdatabehandleren så vidt muligt skal bistå Databehandleren og 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. indsigtretten
 - 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
 - j. retten til ikke at være genstand for en afgørelse, der alene er baseret på automatisk behandling, herunder profilering
2. I tillæg til Underdatabehandlerens forpligtelse til at bistå Databehandleren og den Dataansvarlige i henhold til Bestemmelse 6.3., bistår Underdatabehandleren endvidere, under hensyntagen til behandlingens karakter og de oplysninger, der er tilgængelige for Underdatabehandleren, Databehandleren og den Dataansvarlige med:
 - a. den Dataansvarliges forpligtelse til uden unødigt 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 unødigt 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)

- 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.
3. Parterne skal i bilag C angive de fornødne tekniske og organisatoriske foranstaltninger, hvormed Underdatabehandleren skal bistå Databehandleren og den Dataansvarlige samt i hvilket omfang og udstrækning. Det gælder for de forpligtelser, der følger af Bestemmelse 9.1. og 9.2.

10. Underretning om brud på persondatasikkerheden

1. Underdatabehandleren underretter uden unødigt forsinkelse Databehandleren efter at være blevet opmærksom på, at der er sket et brud på persondatasikkerheden.
2. Underdatabehandlerens underretning til Databehandleren 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.
3. I overensstemmelse med Bestemmelse 9.2.a skal Underdatabehandleren bistå Databehandleren og den Dataansvarlige med at foretage anmeldelse af bruddet til den kompetente tilsynsmyndighed. Det betyder, at Underdatabehandleren skal bistå med at tilvejebringe nedenstående information, 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
 - 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.
4. Parterne skal i bilag C angive den information, som Underdatabehandleren skal tilvejebringe i forbindelse med sin bistand til Databehandleren og den Dataansvarlige i dennes forpligtelse til at anmelde brud på persondatasikkerheden til den kompetente tilsynsmyndighed.

11. Sletning og returnering af oplysninger

1. Ved ophør af tjenesterne vedrørende behandling af personoplysninger, er Underdatabehandleren forpligtet til at slette alle personoplysninger, der er blevet behandlet på vegne af Databehandleren og bekræfte over for Databehandleren, at oplysningerne er slettet eller tilbageleveret alle personoplysninger og slette eksisterende kopier, medmindre EU-retten eller medlemsstaternes nationale ret foreskriver opbevaring af personoplysningerne.

2. Underdatabehandleren forpligter sig til alene at behandle personoplysningerne til de(t) formål, i den periode og under de betingelser, som disse regler foreskriver.

12. Revision, herunder inspektion

1. Underdatabehandleren stiller alle oplysninger, der er nødvendige for at påvise overholdelsen af databeskyttelsesforordningens artikel 28 og disse Bestemmelser, til rådighed for Databehandleren og/eller den Dataansvarlige og giver mulighed for og bidrager til revisioner, herunder inspektioner, der foretages af Databehandleren og/eller den Dataansvarlige eller en anden revisor, som er bemyndiget af Databehandleren og/eller den Dataansvarlige.
2. Procedurene for Databehandlerens og/eller den Dataansvarliges revisioner, herunder inspektioner, med Underdatabehandleren og dennes underdatabehandlere er nærmere angivet i Bilag C.7. og C.8.
3. Underdatabehandleren er forpligtet til at give tilsynsmyndigheder, som efter gældende lovgivningen har adgang til den Dataansvarliges, Databehandlerens eller Underdatabehandlerens faciliteter, eller repræsentanter, der optræder på tilsynsmyndighedens vegne, adgang til Underdatabehandlerens fysiske faciliteter mod behørig legitimation.

13. Parternes aftale om andre forhold

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 Bestemmelserne eller forringer den registreredes grundlæggende rettigheder og frihedsrettigheder, som følger af databeskyttelsesforordningen.

14. Ikrafttræden og ophør

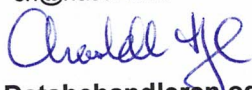
1. Bestemmelserne træder i kraft på datoen for begge parters underskrift heraf.
2. Begge parter kan kræve Bestemmelserne genforhandlet, hvis lovændringer eller u hensigtsmæssigheder i Bestemmelserne giver anledning hertil.
3. Bestemmelserne er gældende, så længe tjenesten vedrørende behandling af personoplysninger varer. I denne periode kan Bestemmelserne ikke opsiges, medmindre andre bestemmelser, der regulerer levering af tjenesten vedrørende behandling af personoplysninger, aftales mellem parterne.
4. Hvis levering af tjenesterne vedrørende behandling af personoplysninger ophører, og personoplysningerne er slettet eller returneret til den Dataansvarlige i overensstemmelse med Bestemmelse 11.1 og Bilag C.4, kan Bestemmelserne opsiges med skriftligt varsel af begge parter.

5. Underskrift

På vegne af den Databehandleren

Navn	Frank Bech Jensen
Stilling	Head of Compliance and Security
Telefonnummer	+45 40906035
E-mail	frbec@itrelation.dk
Underskrift	

På vegne af Underdatabehandleren

Navn	Charlotte Huge
Stilling	CEO
Telefonnummer	28 89 87 89
E-mail	ch@nasure.dk
Underskrift	

15. Kontaktpersoner hos Databehandleren og Underdatabehandleren

1. Parterne kan kontakte hinanden via nedenstående kontaktpersoner.
2. Parterne er forpligtet til løbende at orientere hinanden om ændringer vedrørende kontaktpersoner.

Navn	Anne-Sofie Bejtrup Borregaard-Otzen
Stilling	Systemkonsulent
Telefonnummer	+4570492750
E-mail	anbor@itrelation.dk

Navn	Christina Lindal Hansen
Stilling	Support
Telefonnummer	6996 0591
E-mail	mail@nasure.dk

Bilag A Oplysninger om behandlingen

A.1. Formålet med Underdatabehandlerens behandling af personoplysninger på vegne af Databehandleren

Databehandleren har indgået en aftale med den Dataansvarlige vedrørende levering af EDI Portalen, hvilket omfatter f.eks. vedligehold, support og løsning af konkrete opgaver fra den Dataansvarlige. Når Databehandleren leverer it-systemet, vil dette medføre behandling af personoplysninger på vegne af den Dataansvarlige.

Denne aftale (Underdatabehandleraftalen) fastsætter de rettigheder og forpligtelser, der finder anvendelse, når det overlades til Underdatabehandleren at foretage behandling af personoplysninger på vegne af Databehandleren.

Underdatabehandleraftalen er udformet med henblik på parternes efterlevelse af art. 28 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), som stiller specifikke krav til indholdet af en databehandleraftale.

Underdatabehandlerens behandling af personoplysninger for Databehandleren sker med henblik på opfyldelse af parternes aftale eller aftaler om levering af it-ydelser fra Underdatabehandleren til Databehandleren, og som Databehandleren anvender i sine leverancer ud mod kunder. Underdatabehandleren optræder dermed som en anden databehandler (underdatabehandler) i overensstemmelse med Databeskyttelsesforordningen art. 28(4).

Formålet med Underdatabehandlerens behandling af personoplysninger på vegne af Databehandleren er at udveksle sundhedsdata på en sikker måde gennem EDI portalen. Når Underdatabehandleren leverer EDI Portalen, vil dette medføre behandling af personoplysninger på vegne af Databehandleren og den Dataansvarlige. Underdatabehandleraftalen har dermed til formål at pålægge Underdatabehandleren de samme databeskyttelsesforpligtelser, som Databehandleren er pålagt i sin aftale med den Dataansvarlige.

A.2. Underdatabehandlerens behandling af personoplysninger på vegne af Databehandleren drejer sig primært om (karakteren af behandlingen)

Databehandlerens behandling af personoplysninger på vegne af den Dataansvarlige drejer sig primært om, at Databehandleren yder vedligeholdelse og support af EDI Systemet til den Dataansvarlige.

Underdatabehandlerens behandling af personoplysninger på vegne af Databehandleren og den Dataansvarlige drejer sig primært om karakteren af behandling af Underdatabehandleren på vegne af Databehandlerens: EDI Portal

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

Behandlingen omfatter følgende typer af personoplysninger om de registrerede:

Almindelige personoplysninger, jf. Databeskyttelsesforordningen artikel 6:

Cpr-nr.

Navn

Adresse

Helbredsoplysninger

Følsomme personoplysninger, jf. Databeskyttelsesforordningens artikel 9:

- Helbredsforhold, herunder misbrug af medicin, narkotika, alkohol m.v.
- Biometriske data med det formål entydigt at identificere en fysisk person

CPR-numre, jf. Databeskyttelseslovens § 6, jf. Databeskyttelsesforordningens artikel 87

A.4. Behandlingen omfatter følgende kategorier af registrerede

Behandlingen omfatter følgende kategorier af registrerede:

- Ansatte
- Borgere mellem 0 og 18 år, der modtager kommunalt tandplejetilbud og deres forældre
- Borgere over 18 år, der modtager kommunalt omsorgstandpleje
- Borgere over 18 år, der modtager kommunalt specialtandpleje
- Borgere over 18 år, der modtager kommunalt forsorgstandpleje i Horsens statsfængsel

A.5. Underdatabehandlerens behandling af personoplysninger på vegne af Databehandleren kan påbegyndes efter disse Bestemmelser i krafttræden. Behandlingen har følgende varighed

Underdatabehandlerens behandling af personoplysninger på vegne af Databehandleren påbegyndes efter parternes Hovedaftale træder i kræft og indtil denne ophører.

Bilag B Underdatabehandlere

B.1. Godkendte underdatabehandlere

Ved Bestemmelsernes ikrafttræden har Databehandleren godkendt brugen af følgende andre underdatabehandlere:

NAVN	ADRESSE	LAND HVOR PERSON-OPLYSNINGER OPVE-CARES	BESKRIVELSE AF BE-HANDLING
MedCom	Forskerparken 10 5230 Odense M	EU	Cpr-opslag - SDN FMK -SDN
A-Data A/S	Rødovrevej 253C 2610 Rødovre	EU	Support og udvik- lingsassistance. Ho- sting af data
Link Mobility A/S	Ørestads Boulevard 108, 4 2300 Køben- havn S	EU	Sms-advisering
Region Syddanmark	Regionshuset Dam- haven 12 7100 Vejle	EU	Opbevaring af hen- visninger i Henvis- ningshotellet og vi- deredistribution til legale modtagere

Ved Bestemmelsernes ikrafttræden har Databehandleren godkendt brugen af ovennævnte andre underdatabehandlere for den beskrevne behandlingsaktivitet. Underdatabehandleren må ikke – uden Databehandlerens skriftlige godkendelse – gøre brug af en underdatabehandler til en anden behandlingsaktivitet end den beskrevne og aftalte eller gøre brug af en anden underdatabehandler til denne behandlingsaktivitet.

B.2. Varsel for godkendelse af underdatabehandlere

Underdatabehandlerens underretning om eventuelle planlagte ændringer vedrørende tilføjelse eller erstatning af andre underdatabehandlere skal være Databehandleren i hænde minimum 60 dage, før anvendelsen eller ændringen skal træde i kraft, så vidt dette umiddelbart er muligt.

Såfremt Databehandleren har indsigelser mod ændringerne, skal Databehandleren give Underdatabehandleren meddelelse herom inden ændringens varslede virkningstidspunkt. Databehandleren kan alene gøre indsigelse, hvis Databehandleren har rimelige, konkrete årsager hertil.

Ved Databehandlerens indsigelse accepterer Databehandleren samtidig, at Underdatabehandleren kan være forhindret i at levere hele eller dele af de aftalte tjenester. Sådan manglende opfyldelse kan ikke tilskrives

Underdatabehandlerens misligholdelse. Underdatabehandleren opretholder sit krav på betaling for sådanne ydelser, uanset de ikke kan leveres til Databehandleren.

Hvor det er særligt aftalt, at Underdatabehandleren ikke må gøre brug af underdatabehandlere uden Databehandlerens forudgående tilladelse, accepterer Databehandleren, at dette kan medføre, at Underdatabehandleren kan blive afskåret fra at opfylde tjenesterne. Hvis Databehandleren har afslået, at der foretages ændringer vedrørende tilføjelse eller erstatning af underdatabehandlere, vil manglende levering af tjenester derfor ikke anses for en misligholdelse af en aftale, som kan tilskrives Underdatabehandleren i de tilfælde, hvor den manglende opfyldelse kan henføres til en anden underdatabehandlers forhold.

Bilag C Instruks vedrørende behandling af personoplysninger

C.1. Behandlingens genstand/instruks

Underdatabehandlerens behandling af personoplysninger på vegne af Databehandleren sker ved, at Underdatabehandleren udfører følgende:

Nasure fungerer som kommunikationsplatform og flytter i den forbindelse EDI-Fact /andre standardiserede dokumenter mellem aktører i sundhedsvæsenet identificeret ved EAN numre allokeret af Sundhedsdatastyrelsen.

C.2. Behandlingssikkerhed

Sikkerhedsniveauet skal afspejle:

Databehandleren iværksætter og gennemfører passende tekniske og organisatoriske foranstaltninger for at sikre et sikkerhedsniveau, der passer til de risici, der er forbundet med de behandlingsaktiviteter, databehandleren foretager for den dataansvarlige.

De tekniske og organisatoriske foranstaltninger fastsættes under hensyntagen til det aktuelle tekniske niveau, implementeringsomkostningerne, den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder.

Ved vurderingen af, hvilket sikkerhedsniveau der er passende, tages der navnlig hensyn til de risici, som behandling udgør, navnlig ved hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet.

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.

Det implementerede sikkerhedsniveau

Databehandleren har valgt at basere sit sikkerhedsniveau omkring EDI-portalen på ISO27001:2013 framework, og har implementeret alle kontroller defineret i Appendix A.

Databehandleren verificerer sin implementering af ISO27001:2013, gennem ekstern auditering og dertil følgende certificering.

Databehandleren sikrer løbende vedligeholdelse og recertificering, og forpligter sig til løbende, at dokumentere et gyldigt certifikat på databehandlerens hjemmeside.

C.3 Bistand til Databehandleren og den Dataansvarlige

Underdatabehandleren skal så vidt muligt – inden for det nedenstående omfang og udstrækning – bistå Databehandleren og/eller den Dataansvarlige i overensstemmelse med Bestemmelse 9.1 og 9.2 ved at gennemføre følgende tekniske og organisatoriske foranstaltninger:

- Bistand i forbindelse med de registreredes udøvelse af rettigheder.
- Bistand i forbindelse med den Dataansvarliges anmeldelse af brud på persondatasikkerheden.

- Bistand i forbindelse med den Dataansvarliges udøvelse af konsekvensanalyser.
- Bistand i forbindelse med den Dataansvarliges forpligtelse til at høre den kompetente tilsynsmyndighed, Datatilsynet.

Der betales almindelig timebetaling for denne service.

C.4 Opbevaringsperiode/sletterutine

Der foretages fysisk sletning efter 6 måneder inkl. retentionsperiode på 3 måneder.

C.5 Lokaltet for behandling

Behandling af de af Bestemmelserne omfattede personoplysninger kan ikke uden Databehandlerens forudgående skriftlige godkendelse ske på andre lokaliteter end et af Underdatabehandlerens kontorer.

Underdatabehandleren er forpligtet til at oplyse med præcise adresseangivelser, hvor Databehandlerens personoplysninger opbevares.

Adresseangivelser:

Global Connect
Ejby Industrivej 1
2600 Glostrup

Underdatabehandleren skal ajourføre oplysningerne overfor Databehandlerens ved enhver ændring.

C.6 Instruks vedrørende overførsel af personoplysninger til tredjelande

Underdatabehandleren må ikke overføre personoplysninger til tredjelande.

C.7 Procedurer for Databehandlerens og/eller den dataansvarliges revisioner, herunder inspektioner, med behandlingen af personoplysninger, som er overladt til Underdatabehandleren

Databehandleren og den Dataansvarlige har efter databeskyttelsesforordningens art. 24 og 28 ret og pligt til at gennemføre tilsyn med Underdatabehandlerens behandling af personoplysninger på Databehandlerens og den Dataansvarliges vegne. Databehandlerens og/eller den Dataansvarliges gennemførelse af tilsyn med Underdatabehandleren kan ske ved, at Databehandleren og/eller den Dataansvarlige udfører en af følgende handlinger:

- Egenkontrol på baggrund af dokumenter, som Underdatabehandleren gør tilgængelig for Databehandleren og/eller den Dataansvarlige,
- Skriftligt tilsyn eller
- Fysiske inspektioner.

C.7.1 Egenkontrol

Databehandleren og/eller den Dataansvarlige skal på opfordring gives adgang til en række dokumenter til brug for gennemførelse af egenkontrol, herunder:

- Dokumentation for efterlevelse af ISO27001:2013 i form af løbende opretholdelse af certificering.
- Beskrivelse af fysisk og organisatorisk sikkerhed hos Underdatabehandleren.

- Risikovurdering – af delt infrastruktur (firewall, backup etc.).
- IT Sikkerhedspolitik.
- Beredskabsplaner hos Underdatabehandleren.

C.7.2 Skriftligt tilsyn og fysisk inspektion

Databehandleren og/eller den Dataansvarlige kan vælge at gennemføre et tilsyn enten som skriftligt tilsyn eller ved fysisk inspektion. Tilsynet kan udføres af Databehandleren og/eller af den Dataansvarlige selv og/eller i samarbejde med tredjepart.

Den udførende person skal være generelt egnet til at udføre inspektioner og revisioner, og Databehandlerens og/eller den Dataansvarliges valg af person/repræsentant/revisor skal forelægges Underdatabehandleren til godkendelse.

Revision og inspektion kan finde sted efter forudgående varsel på minimum 2 uger og skal udføres så det sker til mindst mulig gene for Underdatabehandlerens øvrige virksomhed.

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

Underdatabehandleren udfører, på baggrund af Underdatabehandlerens risikovurdering og under hensyntagen til de konkrete behandlingsaktiviteter, revisioner, herunder inspektioner, med andre underdatabehandleres behandling af personoplysninger i overensstemmelse med proceduren beskrevet ovenfor i punkt C.7.

Databehandleren og/eller den Dataansvarlige kan på Databehandlerens og/eller den Dataansvarliges anmodning få yderligere oplysninger om, hvilke kontrolforanstaltninger der iværksat og gennemført over for de enkelte yderligere underdatabehandlere.

Bilag D Parternes regulering af andre forhold

D.1 Generelt

I relation til Underdatabehandlerens behandling af personoplysninger på vegne af Databehandleren, har parterne aftalt den nedenfor indgivne særregulering.

I tilfælde af uoverensstemmelse mellem Bestemmelserne og de i dette bilag D fastsatte vilkår, skal bilag D have forrang.

D. 2 Konsekvenser af Databehandlerens ulovlige instruks

Databehandleren er bekendt med, at Underdatabehandleren er afhængig af Databehandlerens anvisninger om, i hvilket omfang Underdatabehandleren er berettiget til at anvende og behandle personoplysningerne på Databehandlerens vegne. Underdatabehandleren hæfter derfor ikke for krav, som udspringer af Underdatabehandlerens handlinger eller undladelser, i det omfang disse handlinger eller undladelser er en direkte databehandlingsaktivitet udøvet i overensstemmelse med Databehandlerens instrukser.

D.3 Implementering af andre sikkerhedsforanstaltninger

Underdatabehandleren er berettiget til at implementere og opretholde alternative sikkerhedsforanstaltninger i forhold til det i aftalen vedrørende levering af tjenesterne og bilag C.2 anførte, dog under forudsætning af at sådanne alternative sikkerhedsforanstaltninger som minimum giver samme sikkerhed som de foreskrevne sikkerhedsforanstaltninger.

D. 4 Bestemmelser om begunstiget tredjemand ift. underdatabehandlere

Parterne har aftalt at Bestemmelsernes punkt 7.6 (som udfærdigede nedenfor) ikke skal finde anvendelse mellem partner.

Følgende tekst udgør derfor af Bestemmelserne: *"Underdatabehandleren skal i sin aftale med den anden underdatabehandler indføre Databehandleren som begunstiget tredjemand i tilfælde af Underdatabehandlerens konkurs, således at Databehandleren kan indtræde i Underdatabehandlerens rettigheder og gøre dem gældende over for den anden underdatabehandler, som f.eks. gør Databehandleren i stand til at instruere den anden underdatabehandler i at slette eller tilbagelevere personoplysningerne."*

D.5 Underretning om brud på persondatasikkerheden

Det er mellem parterne aftalt at Bestemmelsernes pkt. 10.2. udformes som følge:

Underdatabehandlerens underretning til Databehandleren skal ske hurtigst muligt 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.

Hvis det ikke er muligt for Underdatabehandleren at give oplysningerne samlet, kan oplysningerne meddeles trinvist uden unødigt yderligere forsinkelse.

Underdatabehandleren kan oprette en formular til brug for underretning af Databehandleren, som sendes til Databehandlerens kontaktperson. Underdatabehandlerens beredskabsteam fastsætter under hensyn til et konkret brud på persondatasikkerheden, herunder også det antal berørte kunder, hvordan kommunikationen gives til Databehandleren.

D.6 Sletning og returnering af oplysninger

Det er mellem parterne aftalt at Databehandleren instruerer om Underdatabehandlerens sletning og returnering af personoplysninger i forbindelse med Bestemmelsernes ophør.

Databehandleren skal mindst 30 dage efter at behandlingen af personoplysninger er ophørt meddele Underdatabehandleren hvorvidt alle personoplysninger skal slettes eller tilbageleveres til Databehandleren. I det tilfælde hvor personoplysninger skal tilbageleveres til Databehandleren, skal Underdatabehandleren ligeledes slette eventuelle kopier. Underdatabehandleren skal sikre, at eventuelle andre underdatabehandlere ligeledes efterlever meddelelsen fra Databehandleren.

Såfremt Underdatabehandleren ikke har modtaget meddelelse fra Databehandleren inden 30 dage efter behandlingen af personoplysninger er ophørt, fremsender Underdatabehandleren en rykker til Databehandleren. Hvis Databehandleren herefter meddele Underdatabehandleren hvorvidt alle personoplysninger skal slettes eller tilbageleveres til Databehandleren, er Underdatabehandleren uden yderligere varsel berettiget til at slette personoplysninger.

D.7 Ansvar og misligholdelse

En eventuel misligholdelse af Bestemmelserne reguleres og behandles i overensstemmelse med parternes Hovedaftale.

Databehandleren og Underdatabehandleren er erstatningsansvarlige i overensstemmelse med parternes Hovedaftale med de yderligere begrænsninger der er angivet nedenfor.

Ingen af parterne er ansvarlige over for hinanden for indirekte tab og følgeskader, herunder men ikke begrænset til drifts- og avancetab, mistet besparelse, og tab af goodwill., tab af data og omkostningerne til disses reetablering eller anden lignende følgeskade.

For kompensation og andre beløb der skal betales til de registrerede som følge af overtrædelse af databeskyttelsesforordningens regler, finder databeskyttelsesforordningens artikel 82 anvendelse, og parterne er således inter partes hver især ansvarlig for betaling af sådanne beløb svarende til deres respektive del af erstatningsansvaret, under hensyntagen til vilkårene i Bestemmelserne. Uanset databeskyttelsesforordningens art 82, stk. 5 kan en part, der har udredt erstatningsbeløb til en skadelidte, der ikke svarer til fuld erstatning, gøre regres efter princippet i art. 82, stk. 5.

I forhold til anden godtgørelse for ikke-økonomiske tab til de registrerede skal princippet i art. 82 ligeledes finde anvendelse, for så vidt angår den interne endelige ansvarsfordeling mellem Underdatabehandleren og Databehandleren.

Parterne kan ikke gøre regres eller erstatningskrav gældende overfor den anden part for bøder eller anden straf, der er pålagt i medfør af databeskyttelsesloven § 41 samt for bødeforelæg accepteret efter databeskyttelsesloven § 42.

Ovenstående ansvarsbegrænsning gælder ikke for krav baseret på grov uagtsomhed eller forsætlig misligholdelse.