Databehandleraftale udarbejdet efter Datatilsynets standardkontraktbestemmelser accepteret af Det Europæiske Databeskyttelsesråd

# Databehandleraftale

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

mellem

Kunde
-
- -
DK
CVR-nr.:
herefter den "Dataansvarlige"

og

nps.today ApS
Lyngbyvej 16
2100 København
DK
CVR-nr.: 36464917
herefter "Databehandleren"

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

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

Dette er version 5, sidst opdateret den 23.04.2025 08:37.

**Indholdsfortegnelse**



**Appendix**

## 1. Præambel

1.1 Disse bestemmelser fastsætter Databehandlerens rettigheder og forpligtelser, når denne foretager behandling af personoplysningerne på vegne af den Dataansvarlige.

1.2 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 ("GDPR").

1.3 I forbindelse med leveringen af Levering af nps.todays software og relaterede serviceydelser. behandler Databehandleren personoplysninger på vegne af den Dataansvarlige i overensstemmelse med disse Bestemmelser.

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

1.5 Der hører bilag til disse Bestemmelser, og bilagene udgør en integreret del af Bestemmelserne.

1.6 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.

1.7 Bilag B 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 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 indeholder bestemmelser vedrørende andre aktiviteter, som ikke er omfattet af Bestemmelserne.

1.10 Hvis standardkontraktbestemmelser som omhandlet i GDPR, artikel 46, stk. 1, litra c og d, udgør grundlag for overførsel af personoplysninger mellem den Dataansvarlige og Databehandleren til tredjelande som omhandlet i GDPR, kapitel V, er disse vedlagt i engelsk version som Bilag E og E1.

1.11 Bestemmelserne med tilhørende bilag skal opbevares skriftligt, herunder elektronisk, af begge Parter.

1.12 Disse Bestemmelser frigør ikke Databehandleren fra forpligtelser, som Databehandleren er pålagt efter GDPR 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 GDPR (se GDPR, artikel 24), databeskyttelsesbestemmelser i anden EU-ret eller EU/EØS-medlemsstaternes nationale ret og disse Bestemmelser.

2.2 Den Datansvarlige har ret og pligt til at træffe beslutning 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 EU-/EØS-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 disse Bestemmelser.

3.2 Databehandleren underretter omgående den Dataansvarlige, hvis en instruks efter vedkommendes mening er i strid med GDPR eller databeskyttelsesbestemmelser i anden EU-ret eller EU-/EØS-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, og 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.

## 5. Behandlingssikkerhed

5.1 GDPR, 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.

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:

5.1.1 Pseudonymisering og kryptering af personoplysninger

5.1.2 evne til at sikre vedvarende fortrolighed, integritet, tilgængelighed og robusthed af behandlingssystemer og -tjenester

5.1.3 evne til rettidigt at genoprette tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse

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

5.2 Efter GDPR, 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.

5.3 Derudover skal Databehandleren bistå den Dataansvarlige med vedkommendes overholdelse af den Dataansvarliges forpligtelse efter GDPR, 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 GDPR, artikel 32, og al anden information, der er nødvendig for den Dataansvarliges overholdelse af sin forpligtelse efter GDPR, 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 GDPR, 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 disse Bestemmelser uden forudgående generel 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 60 kalenderdages 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 EU-/EØS-medlemsstaternes nationale ret, pålægge underdatabehandleren de samme databeskyttelsesforpligtelser som dem, der fremgår af disse Bestemmelser, 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 disse Bestemmelser og GDPR.

Databehandleren er derfor ansvarlig for at kræve, at underdatabehandleren som minimum overholder Databehandlerens forpligtelser efter disse Bestemmelser og GDPR.

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 disse Bestemmelser er pålagt underdatabehandleren. Bestemmelser om kommercielle vilkår, som ikke påvirker det databeskyttelsesretlige indhold af underdatabehandleraftalen, skal ikke sendes til den Dataansvarlige.

6.6 Databehandleren skal i sin aftale med underdatabehandleren indføje den Dataansvarlige som begunstiget tredjemand, således at den Dataansvarlige i tilfælde af at Databehandleren faktisk eller retligt set er ophørt med at eksistere eller i tilfælde af Databehandlerens konkurs, har ret til at opsige underdatabehandleraftalen og instruere underdatabehandleren i at slette eller tilbagelevere personoplysningerne.

6.7 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 GDPR, herunder særligt GDPR, artikel 79 og 82, over for den Dataansvarlige og Databehandleren, herunder underdatabehandleren.

6.8 Ret til indsigelse ved nye underdatabehandlere.

Den Dataansvarlige kan gøre indsigelse mod Databehandlernes brug af en ny underdatabehandler ved at underrette Databehandleren skriftligt inden for tredive (30) hverdage efter modtagelsen af nps.today-meddelelsen ved en skriftlig meddelelse til privacy@npstoday.com.

I tilfælde af, at den Dataansvarlige gør indsigelse mod en ny underdatabehandler, vil Databehandleren bestræbe sig på at gøre en rimelig indsats for at stille en ændring i tjenesterne til rådighed for den Dataansvarlige eller anbefale en kommercielt rimelig ændring af Dataansvarliges konfiguration eller brug af tjenesterne, for at undgå behandling af personoplysninger hos den nye underdatabehandler, som den

Dataansvarlige har gjort indsigelse mod, til en ny/anden underdatabehandler uden at belaste den Dataansvarlige urimeligt.

Hvis Databehandleren ikke er i stand til at stille en sådan ændring til rådighed inden for et rimeligt tidsrum, som ikke må overstige halvfems (90) dage, kan den Dataansvarlige opsige de gældende aftaler med hensyn til de tjenester, som ikke kan leveres af Databehandleren uden brug af de indsigede mod ny underdatabehandler ved at give skriftlig meddelelse til Databehandler.

## 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 GDPR, 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 EU-/EØS-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 disse Bestemmelser:

7.3.1 overføre personoplysninger til en dataansvarlig eller databehandler i et tredjeland eller en international organisation

7.3.2 overlade behandling af personoplysninger til en underdatabehandler i et tredjeland

7.3.3 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 Disse Bestemmelser skal ikke forveksles med standardkontraktsbestemmelser som omhandlet i GDPR, artikel 46, stk. 2, litra c og d, og disse Bestemmelser kan ikke udgøre et grundlag for overførsel af personoplysninger som omhandlet i GDPR, kapitel V, medmindre sådanne standardkontraktbestemmelser er vedhæftet i Bilag E.

## 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 GDPR, kapitel III.

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

8.1.1 oplysningspligten ved indsamling af personoplysninger hos den registrerede

8.1.2 oplysningspligten, hvis personoplysninger ikke er indsamlet hos den registrerede

8.1.3 indsigtsretten

8.1.4 retten til berigtigelse

8.1.5 retten til sletning ("retten til at blive glemt")

8.1.6 retten til begrænsning af behandling

8.1.7 underretningspligten i forbindelse med berigtigelse eller sletning af personoplysninger eller begrænsning af behandling

8.1.8 retten til dataportabilitet

8.1.9 retten til indsigelse

8.1.10 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 bestemmelse 5.3, bistår Databehandleren endvidere, under hensyntagen til behandlingens karakter og de oplysninger, der er tilgængelige for Databehandleren, den Dataansvarlige med:

8.2.1 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 Datatilsynet, medmindre at det er usandsynligt, at bruddet på persondatasikkerheden indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder

8.2.2 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

8.2.3 den Dataansvarliges forpligtelse til forud for behandlingen at foretage en analyse af de påtænkte behandlingsaktiviteters konsekvenser for beskyttelse af personoplysninger (en konsekvensanalyse)

8.2.4 den Dataansvarliges forpligtelse til at høre Datatilsynet, som måtte have kompetence 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 Bestemmelse 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 straks og senest 12 timer efter det tidspunkt, hvor Databehandleren er blevet bekendt med bruddet på persondatasikkerheden, sådan at den Dataansvarlige kan overholde sin forpligtelse til at anmelde bruddet på persondatasikkerheden til den kompetente tilsynsmyndighed, jf. GDPR, artikel 33.

9.3 I overensstemmelse med bestemmelse 8.2.1 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 information, som ifølge artikel 33, stk. 3, skal fremgå af den Dataansvarliges anmeldelse af bruddet til den kompetente tilsynsmyndighed:

9.3.1 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

9.3.2 de sandsynlige konsekvenser af bruddet på persondatasikkerheden

9.3.3 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 D 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 Ved ophør af tjenesterne vedrørende behandling af personoplysninger, er Databehandleren forpligtet til at slette alle personoplysinger, der er blevet behandlet på vegne af den Dataansvarlige og bekræfte over for den Dataansvarlige, at oplysningerne er slettet, medmindre EU-retten eller EU-/EØS-medlemsstaternes nationale ret foreskriver opbevaring af personoplysningerne.

## 11. Revision, herunder inspektion

11.1 Databehandleren stiller alle oplysninger, der er nødvendige for at påvise overholdelsen af GDPR, artikel 28, og disse Bestemmelser, 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 lovgivning 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 Bestemmelserne eller forringer den registreredes grundlæggende rettigheder og frihedsrettigheder, som følger af GDPR.

## 13. Ikrafttræden og ophør

13.1 Bestemmelserne er bindende mellem Parterne.

13.2 Begge Parter kan kræve Bestemmelserne genforhandlet, hvis lovændringer eller uhensigtsmæssigheder i Bestemmelserne giver anledning hertil.

13.3 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.

13.4 Hvis levering af tjenesterne vedrørende behandling af personoplysninger ophører, og personoplysningerne er slettet eller returneret til den Dataansvarlige i overensstemmelse med Bestemmelse 10.1 og Bilag C.4, kan Bestemmelserne opsiges med skriftlig varsel af begge Parter.

13.5 Databehandleren er bundet af Bestemmelserne uden Parternes underskrift. Bestemmelserne indgås således uden fysiske/digitale underskrifter, idet Bestemmelserne er bindende i overensstemmelse med kravet i GDPR, artikel 28, stk. 3, 1. pkt.

## 14. Kontaktpersoner hos den Dataansvarlige og Databehandleren

14.1 Parterne kan kontakte hinanden via nedenstående kontaktpersoner.

14.2 Parterne er forpligtet til løbende at orientere hinanden om ændringer vedrørende kontaktpersoner.

Kontaktoplysninger for den Dataansvarlige:
Der henvises til hovedaftalen.

Kontaktoplysninger for Databehandleren:
Der henvises til hovedaftalen.

## Bilag A Oplysninger om behandlingen

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

1.1 Følgende formål ligger til grund for Databehandlerens behandling af personoplysninger på vegne af den Dataansvarlige:

Behandlingen af personoplysninger foretages herudover med henblik på opfyldelsen af følgende formål: Den Dataansvarlige ønsker at bruge nps.today software, som ejes o g drives af Databehandleren, hvor der i forbindelse med brugen af softwaren vil blive i ndsamlet og behandlet loyalitets information om den Dataansvarliges kunder, samarb ejdspartnere og medarbejdere.

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

2.1 Databehandleren stiller nps.today software tilrådighed til den Dataansvarlige og vil derved behandle og opbevare de personoplysninger, som den Dataansvarlige indtaster i softwaren.

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

3.1 e-mail, IP-adresse, navn, telefonnummer

og nps score, nps kommentarer, kunde ID og tidsstempel.

### 4. Behandlingen omfatter følgende kategorier af registrerede

4.1 1) Den Dataansvarliges relevante medarbejdere, som arbejder i nps softwaren. 2) De personer som den Dataansvarlige sender spørgeskemaundersøgelser ud til, f.eks. den Dataansvarliges kunder, samarbejdsparter osv. 3) Andre personer som har eller har haft en direkte eller indirekte kunde og/eller ansættelsesretlig relation til den Dataansvarlige.

### 5. Databehandlerens behandling af personoplysninger på vegne af den Dataansvarlige kan påbegyndes efter disse Bestemmelsers ikrafttræden. Behandlingen har følgende varighed

5.1 Personoplysningerne behandles indtil ophør af tjenesterne vedrørende behandling af

personoplysninger, hvorefter personoplysningerne slettes eller returneres i overensstemmelse med afsnit 10. Behandlingen foretages således så længe den eller de bagvedliggende kommercielle aftaler består.

## Bilag B Underdatabehandlere

### 1. Godkendte underdatabehandlere

1.1 Ved Bestemmelsernes ikrafttræden har den Dataansvarlige godkendt brugen af følgende underdatabehandlere:

- Microsoft Ireland Operations Limited (Data storage and processing) VAT: IE8256796U
- Flowmailer (NL) (afsendelse af email) VAT: NL854692538B01
- Link Mobility (EU) (afsendelse af SMS) VAT: 984 066 910

1.2 Ved Bestemmelsernes ikrafttræden har den Dataansvarlige godkendt brugen af ovennævnte underdatabehandlere for den beskrevne behandlingsaktivitet. Databehandleren må ikke – uden den Dataansvarliges 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.

## Bilag C Instruks vedrørende behandling af personoplysninger

### 1. Behandlingens genstand/instruks

1.1 Den Dataansvarlige ønsker at bruge nps.today software, som ejes og drives af Databehandleren, hvor der i forbindelse med brugen af softwaren vil blive indsamlet og behandlet loyalitets information om den Dataansvarliges kunder, samarbejdspartnere og medarbejdere, som udfyldes ad respondenten af surveyet.

### 2. Behandlingssikkerhed

2.1 Sikkerhedsniveauet skal afspejle:

Databehandleren skal etablere et passende sikkerhedsniveau under hensyntagen til behandlingens karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder.

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.

Databehandleren skal dog - under alle omstændigheder og som minimum - gennemføre følgende foranstaltninger, som er aftalt med den Dataansvarlige:

**Organisatorisk sikkerhed**
Databehandleren gennemfører følgende foranstaltninger organisatoriske sikkerhedsforanstaltninger:

a) Alle medarbejdere er underlagt fortrolighedsforpligtelse, der gælder for alle behandlede personoplysninger.
b) Medarbejdernes adgang til personoplysninger i systemer og på eventuelle fysiske medier eller faciliteter er begrænset, sådan at det kun er de relevante medarbejdere, der har adgang til de relevante personoplysninger.
c) Medarbejderes behandling af personoplysninger logges helt eller delvis og kan kontrolleres efter behov.
d) Databehandleren har en it-sikkerhedspolitik.
e) Databehandleren har en dokumenteret procesbeskrivelse for brud på persondatasikkerheden, der minimum tages op til revidering årligt.
f) Databehandleren har en fast proces, der sikrer, at der ved reparation, service og kassation af hardware sørges for sletning eller fortsat fortrolighed vedrørende personoplysninger på det berørte hardware.
g) Databehandleren har mulighed for at reagere ansættelsesretligt på medarbejderes brud på Databehandlerens datasikkerhed eller brud på instruks om behandling af personoplysninger.
h) Databehandlerens medarbejdere dokumenterer og rapporterer regelmæssigt brud på persondatasikkerheden eller risici herfor.

**Teknisk sikkerhed: Adgang til og beskyttelse af systemer**
Databehandleren gennemfører følgende tekniske sikkerhedsforanstaltninger vedrørende adgang til og beskyttelse af systemer:

a) Der anvendes politik for sammensætningen af adgangskoder, herunder minimumskrav.
b) Databehandlerens kræver, at medarbejdere anvender individuelle adgangskoder (passwords).
c) Der foretages logning og kontrol af uautoriserede eller gentagne mislykkede forsøg på log-in på Databehandlerens systemer.
d) Databehandlerens benytter antivirus-programmer, som opdateres jævnligt.
e) Databehandlerens systemer har logisk adgangskontrol ved brugernavn og adgangskode eller anden autorisation.
f) Databehandlerens PC'er har automatisk adgangsbeskyttelse ved inaktivitet, dvs. låst pauseskærm.
g) Der er procedure(r) for tildeling af autorisationer til it-systemer ved en medarbejders ansættelse.
h) Der er procedure(r) for tilbagekaldelse af tilladelser, når en medarbejder stopper hos Databehandleren eller skifter afdeling.

**Teknisk sikkerhed: Adgang til personoplysninger (data)**
Databehandleren gennemfører følgende tekniske sikkerhedsforanstaltninger vedrørende adgang til personoplysninger:

a) Databehandleren foretager logning og kontrol af uautoriserede eller gentagne mislykkede forsøg på adgang til data.
b) Databehandleren foretager logning og kontrol af uautoriserede eller gentagne mislykkede forsøg på sletning af data.
c) Databehandleren foretager regelmæssig gennemgang og kontrol af brugerautorisationer til specifikke systemer.
d) Databehandleren foretager regelmæssigt gennemgang af systemkontrol.
e) Databehandleren har procedure(r) for at genskabe/reetablere data fra backup.
f) Databehandleren har sporbarhed af adgang til, ændring af og sletning af data foretaget af individuelle brugere.
g) Databehandleren tildeler enkelte eller grupper af brugere autorisationer til at tilgå, ændre og slette behandlede personoplysninger.

Data er opbevaret i Microsoft Azure Data Center i EU, konkret Amsterdam, Holland og data backup i Dublin, Irland.
(Læs mere her: Microsoft Azure Security and Rights Center: https://azure.microsoft.com/en-us/support/trust-center/).

Microsoft opfylder de strengeste sikkerhedskrav og har de højeste standarder for certificering: https://www.microsoft.com/en-us/TrustCenter/Compliance/default.aspx

Adgangen til data sker via hjemmesiden, som er hostet i Azure, og dermed beskyttet i overensstemmelse med alle retningslinjer og standardiserede teknologier fra Microsoft. Adgangskoder er krypteret med den stærke krypteringsalgoritme (SHA-256)

og TLS (https) bruges til alle webopkald.

**Teknisk sikkerhed: Kryptering**
Databehandleren gennemfører følgende tekniske sikkerhedsforanstaltninger vedrørende kryptering:

a) Der anvendes kryptering af netværk.
b) Databehandlerens hjemmesider anvender HTTPS (Hyper Text Transfer Protocol Secure).
c) Personoplysninger krypteres i relevante systemer og/eller på opbevaringsmedier.
d) Databehandlerens computere har krypterede harddiske.

**Teknisk sikkerhed: Tilgængelighed og robusthed**
Databehandleren gennemfører følgende tekniske sikkerhedsforanstaltninger vedrørende tilgængelighed og robusthed:

a) Tilgængelighed og robusthed i Databehandlerens systemer og servere er sikret af tredjemand, som Databehandleren har en aftale med.
b) Temperatur og luftfugtighed overvåges i serverrum.
c) Serverrum har røgalarm og brandslukkere.
d) Serverrum har airconditionssystem.
e) Kun autoriserede medarbejdere har adgang til Databehandlerens eventuelle egne servere.
f) Der foretages regelmæssig backup (enten egen eller hos leverandør).
g) Der er regler og retningslinjer for genskabelse af data fra backup.
h) Der er regler og retningslinjer for backup af data.
i) Der anvendes uafbrudt strømforsyning (UPS).
j) Databehandlerens har procedurebeskrivelse(r) for brud på persondatasikkerheden, der minimum tages op til revidering årligt.
k) Aktiv alarmering ved forsøg på uautoriseret adgang til serverrum og/eller behandlingssystemer og data.

## 3. Bistand til den dataansvarlige

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

3.1.1 Hvis den Dataansvarlige modtager en anmodning om udøvelsen af personers rettigheder efter gældende databeskyttelseslovgivning, og korrekt besvarelse af anmodningen kræver bistand fra Databehandleren, skal Databehandleren bistå den Dataansvarlige med nødvendige og relevante oplysninger og dokumentation samt passende tekniske og organisatoriske sikkerhedsforanstaltninger.

3.1.2 Hvis den Dataansvarlige vil have hjælp til at besvare en anmodning fra en registreret person, skal den Dataansvarlige sende skriftlig anmodning herom til Databehandleren, og Databehandleren skal som svar herpå levere den nødvendige hjælp eller dokumentation hurtigst muligt og senest 7 kalenderdage efter modtagelse af anmodning herom.

3.1.3 Hvis Databehandleren modtager en anmodning om udøvelsen af personers rettigheder efter gældende databeskyttelseslovgivning fra andre end den Dataansvarlige, og anmodningen vedrører personoplysninger behandlet på vegne af den Dataansvarlige, skal Databehandleren uden unødvendig forsinkelse videresende anmodningen til den Dataansvarlige.

## 4. Opbevaringsperiode/sletterutine

4.1 Efter 3 års inaktivitet hos en undersøgelsesdeltager vil personoplysninger automatisk blive anonymiseret (medmindre andet er aftalt). De anonymiserede data vil blive opbevaret til statistiske formål.

Efter anmodning eller ved ophør af leveringen af tekniske databehandlingstjenester (f.eks. tekniske undersøgelsesdata) vil data blive anonymiseret senest 30 dage efter opsigelsesmeddelelsen. På grund af systemtjenester, såsom sikkerhedskopieringsenheder, kan data forblive i systemerne i yderligere 30 dage. Opsummeret kan de data, der skal anonymiseres, forblive i systemerne uændrede i op til 60 dage, før de er afsluttede. Eventuelle personoplysninger, der behandles, f.eks. undersøgelseskommentarer eller svar på opfølgende spørgsmål (alle fritekstfelter) vil blive slettet inden for de 60 dage, i overensstemmelse med afsnit 11.1.

## 5. Lokalitet for behandling

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

Hos Databehandleren egne hovedkontorer og på hovedkontorerne for godkendte underdatabehandlere, som angivet i bilag B.

## 6. Instruks vedrørende overførsel af personoplysninger til tredjelande

6.1 Personoplysningerne behandles kun af Databehandleren på de lokationer, som er beskrevet i Bestemmelse C.5. Databehandleren overfører ikke personoplysninger til tredjelande eller internationale organisationer.

6.2 Hvis den Dataansvarlige ikke i disse Bestemmelser eller efterfølgende giver en dokumenteret instruks vedrørende overførsel af personoplysninger til et tredjeland, er

Databehandleren ikke berettiget til inden for rammerne af disse Bestemmelser at foretage sådanne overførsler.

6.3 Overførsel af personoplysninger må i alle tilfælde kun ske som foreskrevet i Bestemmelserne, på den Dataansvarliges instruks, og i det omfang det er tilladt i medfør af databeskyttelseslovgivningen.

6.4 Når Databehandleren, i overensstemmelse med disse bestemmelser, overfører personoplysninger omfattet af aftalen videre til underdatabehandlere eller selvstændigt dataansvarlige i tredjelande, skal Databehandleren selv sørge for at sikre, at overførslen overholder kapitel 5 i Forordning 2016/679.

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

7.1 Databehandleren skal på skriftlig anmodning dokumentere overfor den Dataansvarlige, at Databehandleren

7.1.1 overholder sine forpligtelser efter denne Databehandleraftale og Instruksen, og

7.1.2 overholder bestemmelserne i GDPR, for så vidt angår personoplysningerne, som behandles på den Dataansvarliges vegne.

7.2 Databehandlerens dokumentation i henhold til afsnit C.7.1 skal sendes til den Dataansvarlige inden for rimelig tid efter modtagelsen af anmodningen herom.

7.3 Databehandleren skal som dokumentation for løbende overholdelse af Bestemmelserne stille egenkontrolrapporter til rådighed for den Dataansvarlige. Disse egenkontrolrapporter skal som minimum udarbejdes én gang årligt og skal følge principperne og kontrolmålene i revisionsstandarden ISAE 3000 som udarbejdet af FSR-danske revisorer og Datatilsynet (og/eller alternativt andre internationalt anerkendte standarder såsom ISO/IEC 27701:2019). Egenkontrolrapporterne kan efter den Dataansvarliges valg ske ved den Dataansvarliges informationsindsamling og skal underskrives af Databehandlerens ledelse. Databehandleren er ikke forpligtet til selv at iværksætte og gennemføre ekstern revision (audit) af Databehandlerens overholdelse af Bestemmelserne.

7.4 Uanset afsnit C.7.3 skal Databehandleren derudover give mulighed for og bidrage til revisioner og inspektioner hver 12. måned, der foretages af revisorer udpeget af den Dataansvarlige, de offentlige myndigheder i Danmark eller af anden kompetent jurisdiktion, i det omfang det er nødvendigt for at kontrollere, at Databehandleren overholder Bestemmelserne og gældende databeskyttelseslovgivning. Den pågældende revisor skal være underlagt fortrolighed i henhold til lov eller aftale. Den Dataansvarlige skal skriftligt varsle revisioner som beskrevet med 10 kalenderdage.

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

8.1 Databehandleren skal minimum hver 12. måned for egen regning føre tilsyn med anvendte underdatabehandlere og fremsende dokumentation herfor til den Dataansvarlige.

8.2 Der er enighed mellem Parterne om, at ISAE 3000-standarden kan anvendes til dette formål.

## Bilag D Parternes regulering af andre forhold

### 1. Vederlag og omkostninger

1.1 Databehandlerens overholdelse af disse standardkontraktsbestemmelser skal kun betales særskilt, hvis det specifikt er aftalt.

Parterne er enige om, at Databehandleren er berettiget til at fakturere den Dataansvarlige efter medgået tid til udførelse af arbejde vedrørende:
- Databehandlerens bistand til udarbejdelse af konsekvensanalyser for de dataansvarlige og
- Databehandlerens bistand til den Dataansvarliges overholdelse af de registreredes rettigheder.

Databehandleren er berettiget til at fakturere den Dataansvarlige efter medgået tid, for udførelse af arbejde, som er nødvendig ved eventuelle ændringer i Instruksen, hvis disse ændringer er foretaget af den Dataansvarlige og ikke er et direkte resultat af ændringer i gældende lov.

Hvis der er ændringer i den gældende lovgivning, herunder fortolkningerne heraf og udstedte retningslinjer fra de relevante og gældende databeskyttelsesmyndigheder, skal alle meromkostninger bæres af hver part.