

Databehandlersaftale

for

Databehandleren

NPS A/S

CVR 15200898

Landbrugsvej 6

5260 Odense S

Danmark



1 Indhold

2	Baggrund for databehandleraftalen.....	3
3	Den dataansvarliges forpligtelser og rettigheder.....	3
4	Databehandleren handler efter instruks.....	4
5	Fortrolighed.....	4
6	Behandlingssikkerhed.....	4
7	Anvendelse af underdatabehandlere.....	5
8	Overførsel af oplysninger til tredjelande eller internationale organisationer	5
9	Bistand til den dataansvarlige	6
10	Underretning om brud på persondatasikkerheden	7
11	Sletning og tilbagelevering af oplysninger	7
12	Tilsyn og revision	8
13	Varighed og ophør.....	8
	Bilag A Oplysninger om behandlingen	9
	Bilag B Betingelser for databehandlerens brug af underdatabehandlere.....	10
	Bilag C Instruks vedrørende behandling af personoplysninger	11

2 Baggrund for databehandleraftalen

1. Denne aftale fastsætter de rettigheder og forpligtelser, som finder anvendelse, når databehandleren foretager behandling af personoplysninger på vegne af den dataansvarlige.
2. Aftalen 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)*, som stiller specifikke krav til indholdet af en databehandleraftale.
3. Denne databehandleraftale har forrang i forhold til eventuelle tilsvarende bestemmelser i andre aftaler mellem parterne.
4. Til denne aftale hører vedlagte tre bilag. Bilagene fungerer som en integreret del af databehandleraftalen.
5. Databehandleraftalens Bilag A indeholder nærmere oplysninger om behandlingen, herunder om behandlingens formål og karakter, typen af personoplysninger, kategorierne af registrerede og varighed af behandlingen.
6. Databehandleraftalens Bilag B indeholder en liste over de eventuelle underdatabehandlere som anvendes.
7. Databehandleraftalens Bilag C indeholder nærmere information om, hvilken behandling databehandleren foretager på vegne af den dataansvarlige (behandlingens genstand), hvilke sikkerhedsforanstaltninger, som iagttages, samt hvordan der føres tilsyn med databehandleren og eventuelle underdatabehandlere.
8. Databehandleraftalen med tilhørende bilag opbevares af begge parter.
9. Denne databehandleraftale frigør ikke databehandleren for forpligtelser, som efter databeskyttelsesforordningen eller enhver anden lovgivning direkte er pålagt databehandleren.

3 Den dataansvarliges forpligtelser og rettigheder

1. Den dataansvarlige har overfor omverdenen (herunder den registrerede) som udgangspunkt ansvaret for, at behandlingen af personoplysninger sker indenfor rammerne af databeskyttelsesforordningen og databeskyttelsesloven.
2. Den dataansvarlige har derfor både rettighederne og forpligtelserne til at træffe beslutninger om, til hvilke formål og med hvilke hjælpemidler der må foretages behandling.

3. Den dataansvarlige er blandt andet ansvarlig for, at der foreligger hjemmel til den behandling, som databehandleren instrueres i at foretage.

4 Databehandleren handler efter instruks

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; i så fald underretter databehandleren den dataansvarlige om dette retlige krav inden behandling, medmindre den pågældende ret forbyder en sådan underretning af hensyn til vigtige samfundsmæssige interesser, jf. art 28, stk. 3, litra a.
2. Databehandleren underretter snarest muligt den dataansvarlige, hvis en instruks efter databehandlerens mening er i strid med databeskyttelsesforordningen eller databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret.

5 Fortrolighed

1. Databehandleren sikrer, at kun de personer, der er autoriseret hertil, har adgang til de personoplysninger, der behandles på vegne af den dataansvarlige. Adgangen til oplysningerne skal derfor straks lukkes ned, hvis autorisationen fratages eller udløber.
2. Databehandleren sikrer, at de personer, der er autoriseret til at behandle personoplysninger på vegne af den dataansvarlige, har forpligtet sig til fortrolighed eller er underlagt en passende lovbestemt tavshedspligt.

6 Behandlingssikkerhed

1. Databehandleren iværksætter alle foranstaltninger, som kræves i henhold til databeskyttelsesforordningens artikel 32, hvoraf det bl.a. fremgår, at der under hensyntagen til det aktuelle niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder skal gennemføres passende tekniske og organisatoriske foranstaltninger for at sikre et sikkerhedsniveau, der passer til disse risici.
2. Databehandleren skal i forbindelse med ovenstående – i alle tilfælde – som minimum iværksætte det sikkerhedsniveau og de foranstaltninger, som er specificeret nærmere i denne aftales Bilag C.
3. Såfremt den dataansvarlige efterfølgende stiller krav om yderligere sikkerhedsforanstaltninger hos databehandleren, vil dette blive etableret for den dataansvarliges regning og efter databehandlerens til enhver tid gældende salgs- og leveringsbetingelser, samt de til enhver tid gældende timesatser.

7 Anvendelse af underdatabehandlere

1. Databehandleren skal opfylde de betingelser, der er omhandlet i databeskyttelsesforordningens artikel 28, stk. 2 og 4, for at gøre brug af en anden databehandler (underdatabehandler).
2. Databehandleren må således ikke gøre brug af en anden databehandler (underdatabehandler) til opfyldelse af databehandleraftalen uden forudgående underretning til den dataansvarlige.
3. Underdatabehandlere er anført i denne aftales Bilag B.
4. Databehandleren er ansvarlig for – igennem indgåelsen af en underdatabehandleraftale – at pålægge en eventuel underdatabehandler mindst de forpligtelser, som databehandleren selv er underlagt efter databeskyttelsesreglerne og denne databehandleraftale med tilhørende bilag.
5. Hvis underdatabehandleren ikke opfylder sine databeskyttelsesforpligtelser, forbliver databehandleren fuldt ansvarlig over for den dataansvarlige for opfyldelsen af underdatabehandlerens forpligtelser.

8 Overførsel af oplysninger til tredjelande eller internationale organisationer

1. Databehandleren må kun behandle personoplysninger efter dokumenteret instruks fra den dataansvarlige, herunder for så vidt angår overførsel (overladelse, videregivelse samt intern anvendelse) af personoplysninger til tredjelande eller internationale organisationer, medmindre det kræves i henhold til EU-ret eller medlemsstaternes nationale ret, som databehandleren er underlagt; i så fald underretter databehandleren den dataansvarlige om dette retlige krav inden behandling, medmindre den pågældende ret forbyder en sådan underretning af hensyn til vigtige samfundsmæssige interesser, jf. art 28, stk. 3, litra a.
2. Uden den dataansvarliges instruks eller godkendelse kan databehandleren – indenfor rammerne af databehandleraftalen - derfor bl.a. ikke
 - a. videregive personoplysningerne til en dataansvarlig i et tredjeland eller i en international organisation,
 - b. overlade behandlingen af personoplysninger til en underdatabehandler i et tredjeland,
 - c. lade oplysningerne behandle i en anden af databehandlerens afdelinger, som er placeret i et tredjeland.

9 Bistand til den dataansvarlige

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 3.

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. den registreredes indsigtsret
 - d. retten til berigtigelse
 - e. retten til sletning («retten til at blive glemt»)
 - f. retten til begrænsning af behandling
 - g. underretningspligt i forbindelse med berigtigelse eller sletning af personoplysninger eller begrænsning af behandling
 - h. retten til dataportabilitet
 - i. retten til indsigelse
 - j. retten til at gøre indsigelse mod resultatet af automatiske individuelle afgørelser, herunder profilering
2. Databehandleren bistår den dataansvarlige med at sikre overholdelse af den dataansvarliges forpligtelser i medfør af databeskyttelsesforordningens artikel 32-36 under hensyntagen til behandlingens karakter og de oplysninger, der er tilgængelige for databehandleren, jf. art 28, stk. 3, litra f.

Dette indebærer, at databehandleren under hensyntagen til behandlingens karakter skal bistå den dataansvarlige i forbindelse med, at den dataansvarlige skal sikre overholdelsen af:

- a. forpligtelsen til at gennemføre passende tekniske og organisatoriske foranstaltninger for at sikre et sikkerhedsniveau, der passer til de risici, der er forbundet med behandlingen
- b. forpligtelsen til at anmelde brud på persondatasikkerheden til tilsynsmyndigheden (Datatilsynet) uden unødigt forsinkelse og om muligt senest 72 timer, efter at den dataansvarlige er blevet bekendt med bruddet, medmindre at det er usandsynligt, at bruddet på persondatasikkerheden indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder.
- c. forpligtelsen til – uden unødigt forsinkelse – at underrette den/de registrerede om brud på persondatasikkerheden, når et sådant brud sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder og frihedsrettigheder

- d. forpligtelsen til at gennemføre en konsekvensanalyse vedrørende databeskyttelse, hvis en type behandling sandsynligvis vil indebære en høj risiko for fysiske persons rettigheder og frihedsrettigheder
 - e. forpligtelsen til at høre tilsynsmyndigheden (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. Vederlæggelse i forbindelse med databehandlerens bistand til den dataansvarlige i denne forbindelse vil blive udført for den dataansvarliges regning og efter databehandlerens til enhver tid gældende salgs- og leveringsbetingelser, samt de til enhver tid gældende tidsfrister.

10 Underretning om brud på persondatasikkerheden

1. Databehandleren underretter uden unødigt forsinkelse den dataansvarlige efter at være blevet opmærksom på, at der er sket brud på persondatasikkerheden hos databehandleren eller en eventuel underdatabehandler.

Databehandlerens underretning til den dataansvarlige skal om muligt ske senest 48 timer efter at denne er blevet bekendt med bruddet, sådan at den dataansvarlige har mulighed for at efterleve sin eventuelle forpligtelse til at anmelde bruddet til tilsynsmyndigheden indenfor 72 timer.

2. I overensstemmelse med denne aftales afsnit 10.2., litra b, skal databehandleren - under hensyntagen til behandlingens karakter og de oplysninger, der er tilgængelige for denne - bistå den dataansvarlige med at foretage anmeldelse af bruddet til tilsynsmyndigheden. Det kan betyde, at databehandleren bl.a. skal hjælpe med at tilvejebringe nedenstående oplysninger, som efter databeskyttelsesforordningens artikel 33, stk. 3, skal fremgå af den dataansvarliges anmeldelse til tilsynsmyndigheden:
 - 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. Sandsynlige konsekvenser af bruddet på persondatasikkerheden
 - c. Foranstaltninger, som er truffet eller foreslås truffet for at håndtere bruddet på persondatasikkerheden, herunder hvis det er relevant, foranstaltninger for at begrænse dets mulige skadevirkninger

11 Sletning og tilbagelevering af oplysninger

1. Ved ophør af tjenesterne vedrørende behandling forpligtes databehandleren til, efter den dataansvarliges valg, at slette eller tilbagelevere alle personoplysninger til den

dataansvarlige, samt at slette eksisterende kopier, medmindre EU-retten eller national ret foreskriver opbevaring af personoplysningerne.

12 Tilsyn og revision

1. Databehandleren stiller alle oplysninger, der er nødvendige for at påvise databehandlerens overholdelse af databeskyttelsesforordningens artikel 28 og denne aftale, 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. Enhver assistance af databehandleren i denne forbindelse skal honoreres af den dataansvarlige efter databehandlerens til enhver tid gældende timesatser og forretningsbetingelser, og efter løbende regning.
2. Databehandleren er forpligtet til at give myndigheder, der efter den til enhver tid gældende lovgivning har adgang til den dataansvarliges og databehandlerens faciliteter, eller repræsentanter, der optræder på myndighedens vegne, adgang til databehandlerens fysiske faciliteter mod behørig legitimation.

13 Varighed og ophør

1. Denne databehandleraftale er gældende så længe databehandler behandler personoplysninger på vegne af den dataansvarlige i henhold til aftalen. Databehandleraftalen ophører automatisk ved opsigelse af aftalen.
2. Ved denne aftales ophør sletter, returnerer eller opbevarer databehandler, de på vegne af den dataansvarlige behandlede personoplysninger efter aftale med den dataansvarlige.
3. Databehandleren kan tilbageholde personoplysninger efter opsigelse af aftalen, i det omfang det er påkrævet ved lov, som er underlagt samme tekniske og organisatoriske sikkerhedsforanstaltninger, som fremgår af denne databehandleraftale.
4. Enhver assistance af databehandleren i denne forbindelse skal honoreres af den dataansvarlige efter databehandlerens til enhver tid gældende timesatser og forretningsbetingelser, og efter løbende regning.

Bilag A Oplysninger om behandlingen

A.1 Formålet med databehandlerens behandling af personoplysninger på vegne af den dataansvarlige er:

Databehandleren stiller systemer til rådighed for den dataansvarlige. Systemer understøtter slutbrugerens anvendelse af selvbetjeningsautomater og andre selvbetjente betalingsløsninger.

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

Systemerne som databehandleren stiller til rådighed for den dataansvarlige er målrettet administration af købsdata. Funktionaliteten i disse løsninger omfatter databaseløsninger til opbevaring af data, klientprogrammer til overvågning af data, fysiske terminaler til interaktion med slutbrugeren, samt kommunikationsløsninger mellem terminaler og serverløsninger.

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

Persondata som behandles af databehandleren er data omkring køb og købsvaner. Disse er som oftest pseudonymiserede data, hvor data kun kan henføres den registrerede ved brug af anden data fra et eksternt system, som ikke opbevares af databehandleren. I nogle tilfælde vil data omfatte nummerplader og data som muliggør betaling ved brug af konto-/medlemskort (fx navn, adresse).

Systemerne som databehandleren stiller til rådighed for den dataansvarlige indeholder ikke persondata omkring race, etnicitet, politisk, filosofisk eller religiøs overbevisning, at en person er mistænkt, sigtet eller dømt for en forbrydelse, helbredsoplysninger, seksuel orientering, medlemskab af fagforening eller genetiske eller biometriske data. Endvidere indeholder oplysningerne ikke data om personnumre.

De registrerede data hører til i kategorien af data om den dataansvarliges slutbrugere.

A.4 Behandlingen omfatter følgende kategorier af registrerede:

De registrerede er personer, som har en kunderelation med den dataansvarlige.

A.5 Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige kan påbegyndes efter denne aftales ikrafttræden. Behandlingen har følgende varighed:

Behandlingen er ikke tidsbegrænset og de registreredes data gemmes så længe at disse er relevante for købsrelationen mellem den registrerede og den dataansvarlige.

Bilag B Betingelser for databehandlerens brug af underdatabehandlere

B.1 Betingelser for databehandlerens brug af eventuelle underdatabehandlere

Som databehandler gøres der brug af underdatabehandlere, idet databehandlerens systemer bliver hostet i et eksternt datacenter for at opnå den størst mulige stabilitet og sikkerhed for data. Databehandleren har den dataansvarliges generelle godkendelse til at gøre brug af underdatabehandlere såsom DIBS, Nets og eksternt datacenter til hosting af data.

B.2 Anvendte underdatabehandlere

Den dataansvarlige er ved databehandleraftalens ikrafttræden orienteret om anvendelsen af følgende underdatabehandlere:

Navn	Sted/land	Region	Bistår med
VIVA-IT	Denmark	EU	Infrastruktur
Nianet	Denmark	EU	Datalagring ERP
Global Connect	Denmark	EU	Datalagring servere
DIBS	Denmark	EU	Datalagring og transaktionsbehandling
Nets	Denmark	EU	Datalagring og transaktionsbehandling
Logos Design A/S	Denmark	EU	Transaktionsbehandling

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 stiller systemer til rådighed for den dataansvarlige. Systemer understøtter slutbrugerens anvendelse af selvbetjeningsautomater og andre selvbetjente betalingsløsninger

C.2 Behandlingsikkerhed

Databehandleren har indgået et samarbejde med underdatabehandlere for at underbygge en sikker og robust databehandling. Data vil fysisk være placeret i eksterne datacentre eller i databehandlerens egne serverum. Databehandleren modtager løbende erklæringer fra underdatabehandlere, som sikrer at underleverandøren opfylder databehandlerens politikker på de nævnte områder. Databehandlerens politikker omkring datasikkerhed omhandler:

Fysisk sikring af data

Adgangskontrol

Der kræves personligt adgangskort og/eller kode for at kunne få adgang til faciliteterne, hvor data er placeret.

Strøm, køl og brandsikring

De nødvendige resurser til at opretholde driften vil være til stede hos underleverandør eller i databehandlerens egne serverum, herunder UPS-systemer, temperaturovervågning og køleanlæg.

Systemsikkerhed

Overvågning

Databehandlerens underleverandør og databehandleren selv har implementeret interne procedurer, som sikrer, at der bliver taget hånd om alerts og alarmer med henblik på at reagere på relevante hændelser og handle derefter.

Firewall – DDoS-angreb

Adgangen til data sikres med firewall som kontrollerer, hvilke IP-adresser der kommunikerer på hvilke porte, og med adressekonvertering. Yderligere serverfunktionalitet som forebygger DDoS-angreb ved løbende at monitorere og sammenligne systemernes indgående trafik.

Backup & Restore

Databehandlerens underleverandører, i form af de eksterne datacentre, og databehandleren selv sikrer løbende, at backup og restore er muligt.

Datasikkerhed

Logning af transaktioner

Der foretages logning af brugertransaktioner, undtagelser og sikkerhedshændelser, og loggen opbevares på ubestemt tid.

Kryptering og pseudonymisering

Trafikken mellem serverne og diverse enheder i databehandlerens systemer sker via krypterede dataforbindelser.

Adgang til data i systemet

Adgang til server sker via VPN-forbindelser. For databehandlerens udviklere kræves der personlig brugernavn og passwords for adgang til produktionsserver.

Intervenering

Adgang til at rette og slette data på opfordring af den registrerede implementeres via administrationsprogrammer.

Personalesikkerhed

Databehandleren har sikret at medarbejdere og underleverandører har forstået deres ansvar og er kompetente til at varetage deres roller.