

Del II

Databehandleraftale

Som en del af parternes Aftale, gælder følgende Databehandleraftale i henhold til artikel 28, stk. 3, i forordning 2016/679 (databeskyttelsesforordningen) mellem:

Visma DataLøn og ProLøn A/S
CVR 48117716
Tronholmen 3,
8960 Randers
Danmark

herefter "databehandleren"

og

Kunden

herefter "den dataansvarlige"

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

1. Indhold	
2. Præambel	3
3. Den dataansvarliges rettigheder og forpligtelser	4
4. Databehandleren handler efter instruks	4
5. Fortrolighed	4
6. Behandlingssikkerhed	4
7. Anvendelse af underdatabehandlere	5
8. Overførsel til tredjelande eller internationale organisationer	6
9. Bistand til den dataansvarlige	7
10. Underretning om brud på persondatasikkerheden	8
11. Sletning og returnering af oplysninger	9
12. Revision, herunder inspektion	9
13. Parternes aftale om andre forhold	9
14. Ikrafttræden og ophør	9
Bilag A Oplysninger om behandlingen	10
Bilag B Underdatabehandlere	12
Bilag C Instruks vedrørende behandling af personoplysninger	14
Bilag D Sletning af data i ProLøn og ProArkiv	18

2. Præambel

1. Disse Bestemmelser fastsætter databehandlerens rettigheder og forpligtelser, når denne foretager behandling af personoplysninger på vegne af den dataansvarlige.
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 den aftalte ydelse behandler databehandleren personoplysninger på vegne af den dataansvarlige 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 den dataansvarliges betingelser for databehandlerens brug af underdatabehandlere og en liste af underdatabehandlere, som den dataansvarlige har godkendt brugen af.
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.
9. Bestemmelserne med tilhørende bilag skal opbevares skriftligt, herunder elektronisk, af begge parter.
10. Disse Bestemmelser frigør ikke databehandleren fra forpligtelser, som databehandleren er pålagt efter databeskyttelsesforordningen eller enhver anden lovgivning.

3. Den dataansvarliges rettigheder og forpligtelser

1. Den dataansvarlige er ansvarlig for at sikre, at behandlingen af personoplysninger sker i overensstemmelse med databeskyttelsesforordningen (se forordningens artikel 24), databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes¹ nationale ret og disse Bestemmelser.
2. Den dataansvarlige har ret og pligt til at træffe beslutninger om, til hvilke(t) formål og med hvilke hjælpemidler, der må ske behandling af personoplysninger.
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.

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

5. Fortrolighed

1. Databehandleren må kun give adgang til personoplysninger, som behandles på den dataansvarliges vegne, til personer, som er underlagt databehandlerens instruktionsbeføjelser, som har forpligtet sig til fortrolighed eller er underlagt en passende lovbestemt tavshedspligt, og kun i det nødvendige omfang. Listen af personer, som har fået tildelt adgang, skal løbende gennemgås. På baggrund af denne gennemgang kan adgangen til personoplysninger lukkes, hvis adgangen ikke længere er nødvendig, og personoplysningerne skal herefter ikke længere være tilgængelige for disse personer.
2. Databehandleren skal efter anmodning fra den dataansvarlige kunne påvise, at de pågældende personer, som er underlagt databehandlerens instruktionsbeføjelser, er underlagt ovennævnte tavshedspligt.

6. Behandlingssikkerhed

1. Databeskyttelsesforordningens artikel 32 fastslår, at den dataansvarlige og databehandleren, under hensyntagen til det aktuelle tekniske niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang,

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

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:

- 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 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.
3. Derudover skal databehandleren bistå den dataansvarlige med vedkommendes overholdelse af den dataansvarliges forpligtelse efter forordningens artikel 32, ved bl.a. at stille den nødvendige information til rådighed for den dataansvarlige vedrørende de tekniske og organisatoriske sikkerhedsforanstaltninger, som databehandleren allerede har gennemført i henhold til forordningens artikel 32, og mod fakturering af anden information, der er nødvendig for den dataansvarliges overholdelse af sin forpligtelse efter forordningens artikel 32. Vilkår for den dataansvarliges kontrol med databehandleren er beskrevet i bilag C.

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.

7. Anvendelse af underdatabehandlere

1. Databehandleren skal opfylde de betingelser, der er omhandlet i databeskyttelsesforordningens artikel 28, stk. 2, og stk. 4, for at gøre brug af en anden databehandler (en underdatabehandler).
2. Databehandleren må således ikke gøre brug af en underdatabehandler til opfyldelse af disse Bestemmelser uden forudgående generel skriftlig godkendelse fra den dataansvarlige.
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 1 måneds varsel til den 1. i en måned og derved give den dataansvarlige mulighed for at gøre indsigelse mod sådanne ændringer inden brugen af de(n) omhandlede underdatabehandler(e). Listen over underdatabehandlere, som den dataansvarlige allerede har godkendt, fremgår af bilag B.

4. Når databehandleren gør brug af en underdatabehandler i forbindelse med udførelse af specifikke behandlingsaktiviteter på vegne af den dataansvarlige, skal databehandleren, gennem en kontrakt eller andet retligt dokument i henhold til EU-retten eller medlemsstaternes nationale ret, pålægge underdatabehandleren de samme databeskyttelsesforpligtelser som dem, der fremgår af 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 databeskyttelsesforordningen.

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

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

8. Overførsel til tredjelande eller internationale organisationer

1. Enhver overførsel af personoplysninger til tredjelande eller internationale organisationer må kun foretages af databehandleren på baggrund af dokumenteret instruks herom fra den dataansvarlige og skal altid ske i overensstemmelse med databeskyttelsesforordningens kapitel V.
2. Hvis overførsel af personoplysninger til tredjelande eller internationale organisationer, som databehandleren ikke er blevet instrueret i at foretage af den dataansvarlige, kræves i henhold til EU-ret eller medlemsstaternes nationale ret, som databehandleren er underlagt, skal databehandleren underrette den dataansvarlige om dette retlige krav inden behandling, medmindre den pågældende ret forbyder en sådan underretning af hensyn til vigtige samfundsmæssige interesser.
3. Uden dokumenteret instruks fra den dataansvarlige kan databehandleren 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. 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.
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 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 III.

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

- a. oplysningspligten ved indsamling af personoplysninger hos den registrerede
 - b. oplysningspligten, hvis personoplysninger ikke er indsamlet hos den registrerede
 - c. 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 databehandlerens forpligtelse til at bistå den dataansvarlige i henhold til Bestemmelse 6.3., bistår databehandleren endvidere, under hensyntagen til behandlingens karakter og de oplysninger, der er tilgængelige for databehandleren, den dataansvarlige med:
- a. den dataansvarliges forpligtelse til uden 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 databehandleren skal bistå 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. Databehandleren underretter uden unødigt forsinkelse den dataansvarlige efter at være blevet opmærksom på, at der er sket et brud på persondatasikkerheden.
2. Databehandlerens underretning til den dataansvarlige skal om muligt ske senest 24 timer efter, at denne er blevet bekendt med bruddet, sådan at den dataansvarlige kan overholde sin forpligtelse til at anmelde bruddet på persondatasikkerheden til den kompetente tilsynsmyndighed, jf. databeskyttelsesforordningens artikel 33.
3. I overensstemmelse med Bestemmelse 9.2.a skal databehandleren bistå den dataansvarlige med at foretage anmeldelse af bruddet til den kompetente tilsynsmyndighed. Det betyder, at databehandleren skal bistå med at tilvejebringe nedenstående 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 databehandleren skal tilvejebringe i forbindelse med sin bistand til 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 databehandleren forpligtet til at slette alle personoplysninger, der er blevet behandlet på vegne af den dataansvarlige, efter aftale, medmindre EU-retten eller medlemsstaternes nationale ret foreskriver opbevaring af personoplysningerne.

Databehandleren 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. Databehandleren stiller alle oplysninger, der er nødvendige for at påvise overholdelsen af databeskyttelsesforordningens 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.
2. Procedurene for den dataansvarliges revisioner, herunder inspektioner, med databehandleren og underdatabehandlere er nærmere angivet i Bilag C.7. og C.8.
3. Databehandleren er forpligtet til at give tilsynsmyndigheder, som efter gældende lovgivningen har adgang til den dataansvarliges eller databehandlerens faciliteter, eller repræsentanter, der optræder på tilsynsmyndighedens vegne, adgang til databehandlerens fysiske faciliteter mod behørig legitimation.

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 parternes indgåelse af aftale om levering af tjenesterne.
2. Begge parter kan kræve Bestemmelserne genforhandlet, hvis lovændringer eller uhensigtsmæssigheder 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.

Bilag A Oplysninger om behandlingen

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

Formålet med databehandlerens behandling af personoplysninger på vegne af den dataansvarlige er levering af et en standard IT-løsningen, der på baggrund af Kundens indberetninger til databehandleren foretager lønbehandling for Kunden, i henhold til Aftalen.

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

Behandlingen af personoplysninger drejer sig primært om varetagelse af it-systemer til håndtering af den dataansvarliges lønadministration.

Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige drejer sig om lønbehandling, herunder:

- beregne Medarbejdernes løn,
- foretage alle beregninger og indberetninger til og foranlediger pengeoverførsler til SKAT, ATP, ferie- og barselsfonde, pensionskasser m.v. på Kundens vegne,
- foretage indberetning af statistik til arbejdsgiverforening og Danmarks Statistik på Kundens vegne,
- sende lønsedler til Medarbejdernes digitale postkasse
- gemmer Kundens lønbilag i et elektronisk arkiv
- yde hjælp til opstart og oprettelse af Kunden og Medarbejderne, og
- levere support- og konsulenttydelser telefonisk og online fra Visma DataLøn og ProLøns lønkonsulenter, når Kunden har brug for hjælp.

Databehandleren foretager ingen udvikling eller tilpasning af ProLøn i forhold til Kundens specifikke behov eller ønsker.

Herudover faciliterer databehandleren drift, test, vedligehold, udvikling samt fejlrretning af systemer og applikationer.

Databehandleren får derudover en ikke-eksklusiv, royaltyfri, evig og uigenkaldelig ret til i overensstemmelse med gældende lovgivning uigenkaldeligt at anonymisere og herefter aggregere den dataansvarliges data og brug af Visma DataLøn og ProLøn A/S' produkter, og herefter anvende disse til at:

- Forbedre, optimere og udvikle databehandlerens eksisterende eller fremtidige moduler, produkter og funktioner, og
- Udarbejde statistikker vedrørende:
 - løndannelse og lønudvikling,,
 - virksomheds- og medarbejderforhold,
 - demografi,herunder til brug i fremtidige funktioner og produkter.

Ved anonymisering af personoplysninger, skal databehandleren sikre, at ingen fysiske personer kan identificeres ud fra oplysningerne eller i kombination med andre oplysninger, og at oplysningerne ikke kan føres tilbage til en identificerbar eller identificeret fysisk person. Anonymiseringen skal være uigenkaldelig.

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

Typer af persondata som er underlagt behandling i henhold til aftalen:

Almindelige personoplysninger:

- Kontaktoplysninger, som navn, adresse, mail, telefon
- CPR-nr.
- Stillingskategori, oplysninger om løn, arbejdstid, fravær, pension, skat, bankkonto
- ferieafregning
- pensionsafregning
- skatteafregning
- kontooplysninger
- Medarbejdersnummer

Særlige kategorier af personoplysninger

- medlemskab af fagforening, i de særlige situationer, hvor medarbejderens faglige kontingent bliver trukket over lønnen

For alle ovenstående gælder at ingen af følgende følsomme personoplysninger vil indgå i behandlingen:

- race eller etnisk, eller politisk, filosofisk eller religiøs overbevisning
- at en person er mistænkt, sigtet eller dømt for en forbrydelse
- helbredsoplysninger
- seksuel orientering
- genetiske eller biometriske data

A.4. Behandlingen omfatter følgende kategorier af registrerede

Kategorier af registrerede som indgår i behandlingen:

- Den dataansvarliges (Kundens) slutbrugere
- Den dataansvarliges (Kundens) medarbejdere
- Den dataansvarliges (Kundens) kontaktpersoner

A.5. Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige kan påbegyndes efter disse Bestemmelser i krafttræden. Behandlingen har følgende varighed

Denne aftale er gældende, så længe databehandleren behandler personoplysninger på vegne af den dataansvarlige i overensstemmelse med leveringsaftalen (Aftalen)

Bilag B Underdatabehandlere

B.1. Godkendte underdatabehandlere

Ved Bestemmelsernes ikrafttræden har den dataansvarlige godkendt brugen af følgende underdatabehandlere:

Navn	Land	Juridisk overdragelsesmekanisme, hvis underdatabehandleren har adgang til personoplysninger fra lande uden for EU/EØS	Bistår Databehandleren med
Google LLC 1600 Amphitheatre Parkway Mountain View, CA 94043 USA	Irland	Ikke relevant	Sagsstyring intern, mails og informationsdeling
Mastercard Payment Services Denmark A/S Arne Jacobsens Allé 13 2300 København S CVR: 40695869	Danmark	Ikke relevant	Overførsels- og informationservice Datalagring af lønberegninger, gamle lønberegninger
PostNord Strålfors A/S Hedegaardsvej 88 2300 København S CVR-nr. 10068657	Danmark	Ikke relevant	Konvertering og levering til e-Boks
Visma IT AS Karenslyst Alle 56 0277 Oslo Org no: 97920737	Norge	Ikke relevant	Netværk
Proinfo Tronholmen 3, 8960 Randers CVR nr. 26056446	Danmark	Ikke relevant	Infrastruktur
Proinfo - IT drift Tronholmen 3, 8960 Randers CVR nr. 36392762	Danmark	Ikke relevant	Infrastruktur og udviklingservice, herunder hosting og drift af lønmotor
Netcompany A/S Grønningen 17 1, 1270 København K CVR nr. 14814833	Danmark	Ikke relevant	Konvertering og udsendelse af digital post Digital postkasse (Mit.dk) Print og udsendelse af breve

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.

B.2. Varsel for godkendelse af underdatabehandlere

Databehandleren skal skriftligt underrette den dataansvarlige om eventuelle planlagte ændringer vedrørende tilføjelse eller erstatning af underdatabehandlere og derved give den dataansvarlige mulighed for at gøre indsigelse mod sådanne ændringer.

En sådan underretning skal ske med 1 måneds varsel til den 1. i en måned.

Såfremt den dataansvarlige har indsigelser mod ændringerne, skal den dataansvarlige give meddelelse herom til databehandleren. Den dataansvarlige kan alene gøre indsigelse, såfremt den dataansvarlige har rimelige, konkrete årsager hertil.

Indsigelse mod tilføjelse eller erstatning af underdatabehandlere har ikke opsættende virkning for gennemførelsen heraf. Hvis den dataansvarlige har indsigelser, er såvel den dataansvarlige og databehandleren berettiget til skriftligt at opsiges Aftalen med virkning fra tidspunktet for ibrugtagning af nye underdatabehandlere, således at ændringen ikke vil træde i kraft overfor den dataansvarlige.

Bilag C Instruks vedrørende behandling af personoplysninger

C.1. Behandlingens genstand/instruks

Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige sker ved, at databehandleren udfører behandlingsaktiviteterne som er beskrevet i bilag A

C.2. Behandlingssikkerhed

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, implementerings-omkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder skal implementeres et højt sikkerhedsniveau.

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

Politikker, procedurer, processer, organisatoriske beslutningsprocesser og aktiviteter inden for følgende informationssikkerhedskontrolområder er implementeret:

- Informationssikkerhedspolitikker
 - Overordnede retningslinjer og krav til informationssikkerhed
- Organisering af informationssikkerhed herunder udpeget
 - udpeget Information Security Manager og Data Protection Manager,
 - implementeret Information Security Board.
- Medarbejdersikkerhed herunder
 - baggrundstjek,
 - gennemgang af straffeattest,
 - fortrolighedserklæringer,
 - awarenessstræning
- Adgangsstyring herunder
 - begrænsning af adgang til data ud fra arbejdsbetinget behov således at forpligtelser i henhold til Hovedaftalen kan opfyldes
- Kryptografi herunder
 - kryptering eller anonymisering af data
- Fysisk sikring og miljøsikring herunder
 - beskyttelse af fysiske adgangsveje til databehandlerens lokationer
- Driftssikkerhed herunder
 - implementerede processer til håndtering af udviklings- og ændringsstyring,
 - backup,
 - logning,
 - overvågning af og beskyttelse mod tekniske sårbarheder.
- Kommunikationssikkerhed herunder
 - beskyttelse og opdeling af netværk
 - etablerede sikre kommunikationsformer.
- Anskaffelse, udvikling og vedligeholdelse af systemer herunder

- proces for sikker udvikling
- Leverandørforhold herunder
 - process til sikring af at leverandører lever op til samme forpligtelser som fastsat i denne Databehandleraftale,
 - proces for løbende opfølgning.
- Styring af informationssikkerhedsbrud og brud på persondatasikkerheden herunder
 - "Incident response" process,
 - process for underretning af den dataansvarlige.
- Informationsikkerhedsaspekter ved nød-, beredskabs- og reetableringsstyring herunder
 - implementeret Business Continuity Management process
- Overensstemmelse (compliance) herunder
 - proces for identifikation af lovgivningsmæssige eller kontraktuelle krav.

Hvis den dataansvarlige anmoder om oplysninger om sikkerhedsforanstaltninger, dokumentation eller andre former for oplysninger omkring hvordan databehandleren behandler Personoplysninger, og sådanne overskrider de standardoplysninger, beskrevet i Bestemmelse C.7, som databehandler har stillet til rådighed for opfyldelse af gældende lovgivning om behandling af personoplysninger som databehandler, og dette medfører ekstra arbejde for databehandler, er databehandler berettiget til at opkræve den dataansvarlige betaling for sådanne ekstra arbejde.

C.3 Bistand til den dataansvarlige

Databehandleren skal så vidt muligt bistå den dataansvarlige i overensstemmelse med Bestemmelse 9.1 og 9.2 herunder bistå den dataansvarlige med følgende oplysninger i tilfælde af brud på informationssikkerheden:

- Beskrivelse af hændelsesforløb
- Identifikation af de registrerede som er berørt af hændelsen
- Typer af persondata som omfattet af hændelsen

C.4 Opbevaringsperiode

Ved ophør af tjenesten vedrørende behandling af personoplysninger, skal databehandleren enten slette eller tilbagelevere personoplysningerne i overensstemmelse med bestemmelse 11.1, medmindre den dataansvarlige – efter accepten af disse bestemmelser – har ændret den dataansvarlige oprindelige valg. Sådanne ændringer skal være dokumenteret og opbevares skriftligt, herunder elektronisk, i tilknytning til bestemmelserne.

C.5 Lokaltid for behandling

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

Visma DataLøn og ProLøn A/S
Tronholmen 3
DK-8960 Randers

samt på lokationer for anvendte underdatabehandlere som angivet i Bilag B.

I tilfælde af distancearbejde kan behandling af persondata kun finde sted ved opkobling via VPN (Virtual Private Network).

C.6 Instruks vedrørende overførsel af personoplysninger til tredjelande

Den dataansvarlige giver instruks til, at personoplysninger behandles af de underdatabehandlere, der er nævnt i bilag B, samt på de pågældende lokationer heri.

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.

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

Databehandleren indhenter årligt en revisionserklæring fra underdatabehandler som er leverandør af databehandlerens mainframe (lønproduktionsmiljø BS2000 og hostingmiljø (fronted og CRM)). Erklæringen er udarbejdet af uafhængig tredjepart vedrørende databehandlerens og underdatabehandlerens overholdelse af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser.

Der er enighed mellem parterne om, at følgende typer af revisionserklæring kan anvendes i overensstemmelse med disse Bestemmelser:

ISAE 3402-erklæring

ISAE 3402 erklæring på lønproduktionsmiljø (BS2000) og hostingmiljø (frontend, CRM) kan fremsendes til den dataansvarlige til orientering. Derudover henvises der til Q&A, som findes på www.Proloen.dk.

Baseret på resultaterne af erklæringen, er den dataansvarlige berettiget til at anmode om gennemførelse af yderligere foranstaltninger med henblik på at sikre overholdelsen af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser. Parterne skal blive enige om eventuelle yderligere foranstaltninger. Databehandleren er berettiget til at opsige Aftalen mellem Parterne, hvis en aftale ikke kan opnås. Den dataansvarlige afholder alle udgifter i forbindelse med yderligere kontrol, herunder betaling for databehandlerens tidsforbrug.

For at anmode om at foretage en kontrol skal den dataansvarlige fremsende en detaljeret kontroloversigt mindst fire uger forud for den foreslåede kontroldato til databehandler med beskrivelse af det foreslåede omfang, varighed og starttidspunkt for kontrollen.

Den dataansvarlige eller en repræsentant for den dataansvarlige har herudover adgang til at foretage inspektioner, herunder fysiske inspektioner, med lokaliteterne hvorfra databehandleren foretager behandling af personoplysninger, herunder fysiske lokaliteter og systemer, der benyttes til eller i forbindelse med behandlingen. Sådanne inspektioner kan kun gennemføres, efter aftale mellem parterne.

Hvis behandling sker i et "multitenant" miljø eller lignende, giver den dataansvarlige databehandler ret til at bestemme, af sikkerhedsmæssige årsager, at kontrollerne skal foretages af en neutral tredjepartskontrollant efter databehandlerens valg.

Den dataansvarlige afholder alle omkostninger forbundet med sådanne inspektioner. I alle tilfælde skal kontroller foretages inden for normal arbejdstid på det pågældende sted, i medfør af databehandlerens politikker og må ikke på urimelig måde gribe forstyrrende ind i databehandlerens forretningsdrift.

Et eventuelt særskilt vederlag til databehandleren i henhold til det ovenstående beregnes på grundlag af det tidsforbrug, databehandleren anvender på fremskaffelsen af informationen, samt databehandlerens almindeligt gældende timesatser, og databehandleren har derudover krav på, at den dataansvarlige dækker eventuelle eksterne omkostninger afholdt af databehandleren til fremskaffelse af informationen, herunder omkostninger afholdt til eventuelt fornøden bistand fra underdatabehandlere.

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

Databehandleren indhenter på baggrund af en risikovurdering årligt dokumentation for relevante underdatabehandleres overholdelse af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser. Der er enighed mellem parterne om at proces for, gennemførelse og tilstrækkelighed heraf dokumenteres via den dataansvarliges revision af databehandleren jf C.7.

Hvis ydeligere information vedrørende underdatabehandleres overholdes af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser skal leveres til den dataansvarlige, vil databehandleren, for den dataansvarliges regning, indhente den, efter aftale, fornødne og tilgængelige dokumentation hos underdatabehandlere.

Bilag D Sletning af data i ProLøn og ProArkiv

I Mit ProLøn og ProArkiv slettes data efter følgende regler:

D.1 Efter aftalens ophør

Al data om kundeforholdet samt data om alle medarbejdere slettes løbende år +4 måneder efter aftalens ophør via driften.

D.2 Mit ProLøn

D.2.1 Medarbejderdata

Data på fratrådte/inaktive medarbejdere slettes automatisk i december løbende år +1 år. Hvis der udbetales løn på en fratrådt medarbejder forlænges perioden.

Al data på fratrådte medarbejdere kan også slettes på den dataansvarliges anmodning til ProLøn.

D.2.2 Brugeradgange

Kunderne administrerer selv brugeradgange. Hvis en rettighed fratages eller en bruger slettes, vil ændringen virke med det samme.

D.2.3 Logdata

Oplysninger om log-in i Mit ProLøn samt transaktionslogs gemmes i 4 måneder.

D.2.4 Beskeder

Beskeder bliver slettet efter samme regler som "Efter aftalens ophør".

D.2.5 Dokumenter

Dokumenter bliver slettet efter samme regler som "Efter aftalens ophør".

Det er dog muligt for den dataansvarlige at slette dokumenter selv.

D.2.6 Indlæs fil fra:

Indberet Løn

Indlæste filer og registreringer i Mit ProLøn gemmes ikke. De vil kun være tilgængelige, så længe de bliver brugt i lønbehandlingen.

Medarbejder

Indlæste filer og registreringer i Mit ProLøn gemmes ikke. De vil kun være tilgængelige, så længe de bliver brugt i lønbehandlingen.

Fraværstatistik

Indlæste filer og registreringer i Mit ProLøn gemmes ikke. De vil kun være tilgængelige, så længe de bliver brugt i lønbehandlingen.

D.3 ProArkiv:

D.3.1 Dokumenter

Dokumenter slettes automatisk i januar hvert år. Dokumenter, som er ældre end indeværende år + 5 år, vil blive slettet.

Indberettet løn

Data på fratrådte medarbejdere slettes automatisk i december efter løbende år +1 år.

Hvis der udbetales løn på en fratrådt medarbejder forlænges perioden.