Bilag 1

Databehandleraftale

1. Indledning

Som en del af parternes Aftale, gælder følgende Databehandleraftale mellem Underdatabehandleren, Visma Dataløn A/S og Databehandleren, Lønpartner, med mindre andet er udtrykkeligt specificeret i andre aftaler mellem parterne.

Formålet med Databehandleraftalen er at regulere, hvordan og til hvilket formål Underdatabehandleren skal behandle Personoplysninger på vegne af Databehandleren samt at sikre, at den Dataansvarliges Personoplysninger behandles i henhold til Databehandlerens retningslinjer og instrukser samt gældende databeskyttelseslovgivning.

Kategorier af Registrerede og Personoplysninger, der behandles, fremgår af underbilag A.

2. Definitioner

Kundevirksomheden er dataansvarlig (herefter kaldet den Dataansvarlige), Lønpartner er databehandler (herefter kaldet Databehandler), og Visma DataLøn er underdatabehandler (herefter kaldet Underdatabehandler).

Personoplysninger, Særlige kategorier af Personoplysninger (Følsomme persondata), Behandling af personoplysninger, den Registrerede, den Dataansvarlige, Databehandler og Underdatabehandler skal have den betydning, som følger af gældende lovgivning om behandling af personoplysninger, herunder Databeskyttelsesforordningen (GDPR).

3. Den Dataansvarliges forpligtelser

Den Dataansvarlige har ansvaret for, at Behandlin-gen af Personoplysninger lever op til kravene i Data-beskyttelsesforordningen og Databeskyttelsesloven.

Den Dataansvarlige er ved brug af de tjenester, som Databehandler stiller til rådighed i henhold til aftalen, forpligtet til at behandle Personoplysninger i overens-stemmelse med bestemmelserne i gældende lovgiv-ning om behandling af personoplysninger.

Den Dataansvarlige er blandt andet ansvarlig for, at der foreligger hjemmel til den behandling, som Databehandleren instrueres i at foretage.

4. Databehandlerens forpligtelser

Databehandler er ved brug af de tjenester, som Underdatabehandler stiller til rådighed i henhold til Aftalen, forpligtet til at behandle Personoplysninger i overensstemmelse med bestemmelserne i gældende lovgivning om behandling af personoplysninger.

Databehandler er endvidere ansvarlig for, at den Dataansvarliges Personoplysninger behandles i henhold til retningslinjer og instrukser fra den Dataansvarlige.

5. Underdatabehandlerens forpligtelser

Underdatabehandleren behandler udelukkende Personoplysninger på vegne af og på baggrund af instrukser fra Databehandleren.

Databehandling skal ske på følgende måde:

- Alene i overensstemmelse med gældende lovgivning,
- For at opfylde alle forpligtelser i henhold til Aftalen,
- Som nærmere angivet gennem Databehandlerens almindelige brug af Underdatabehandlerens tjenester,
- Som angivet i denne Databehandleraftale.

Underdatabehandler underretter omgående Databehandleren, hvis en instruks efter Underdatabehandlerens mening er i strid med Databeskyttelsesforordningen eller databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret.

Underdatabehandler skal sikre, at Personoplysningerne er underlagt fortrolighed, integritet og tilgængelighed i henhold til gældende lovgivning om behandling af personoplysninger.

Underdatabehandler og dennes medarbejdere skal sikre fortrolighed vedrørende de behandlede Personoplysninger. Denne bestemmelse gælder også efter Aftalens ophør.

Underdatabehandler sikrer, at de personer, der er autoriseret til at behandle Personoplysninger på vegne af Databehandleren, har forpligtet sig til fortrolighed eller er underlagt en passende lovbestemt tavshedspligt.

Underdatabehandler skal bistå Databehandler med passende tekniske og organisatoriske foranstaltninger, så vidt dette er muligt, for opfyldelse af Databehandlerens forpligtelser til at bistå ved besvarelse af anmodninger fra Registrerede og om generel udøvelse af Registreredes rettigheder i henhold til Databeskyttelsesforordningens Kapitel 3 og Artikel 32 til 36.

Underdatabehandler giver, uden unødig forsinkelse, meddelelse til Databehandler om hændelser, som Databehandler i henhold til lovgivningen er forpligtet til at meddele til den Dataansvarlige, Datatilsynet eller Registrerede.

Desuden giver Underdatabehandler, i det omfang det er hensigtsmæssigt og lovligt, Databehandler meddelelse om:

- Anmodninger om videregivelse af Personoplysninger modtaget fra en Registreret.
- Anmodninger om videregivelse af Personoplysninger fra offentlige myndigheder, såsom politiet.

Underdatabehandleren besvarer ikke direkte henvendelser fra Registrerede, medmindre der via Databehandler foreligger samtykke fra den Dataansvarlige. Underdatabehandleren videregiver ikke Personoplysninger til offentlige myndigheder, såsom politiet, medmindre der foreligger lovligt grundlag.

Underdatabehandleren har ikke ejerskab til, eller kontrol med, hvorvidt og hvordan Databehandler vælger at benytte sig af eventuel tredjeparts integrationer via Underdatabehandler API, via direkte databasekobling eller lignende. Ansvaret for sådanne integrationer med tredjepart påhviler udelukkende Databehandler.

6. Sikkerhed

Underdatabehandler skal indføre systematiske, organisatoriske og tekniske foranstaltninger til sikring af et passende sikkerhedsniveau under hensyntagen til teknologien og omkostningerne til indførelse i forhold til de risici, som behandlingen indebærer, samt arten af de Personoplysninger der skal beskyttes.

Underdatabehandler er forpligtet til at sikre et højt sikkerhedsniveau i sine produkter og tjenester. Underdatabehandler yder dette sikkerhedsniveau gennem organisatoriske, tekniske og fysiske sikkerhedsforanstaltninger i henhold til kravene til informationssikkerhedsforanstaltninger, som fremgår af Databeskyttelsesforordningens Artikel 32.

Desuden har de interne rammer for beskyttelse af Personoplysninger, som er udarbejdet af Visma-koncernen, til formål at sikre fortroligheden, integriteten, sikkerheden og tilgængeligheden af Personoplysninger. Følgende foranstaltninger har særlig betydning i denne forbindelse:

- Klassificering af Personoplysninger for at sikre iværksættelse af sikkerhedsforanstaltninger svarende til risikovurderinger.
- Vurdering af brug af kryptering og anonymisering som risikobegrænsende foranstaltninger.
- Begrænsning af tilgang til Personoplysninger til dem, som har brug for adgang til opfyldelse af forpligtelser i henhold til Aftalen.
- Kontrolsystemer, der registrerer, genopretter, forebygger og rapporterer brud i forbindelse med behandling af Personoplysninger.
- Sikkerhedsprocedurer som angivet i underbilag C.

Hvis Databehandler anmoder om oplysninger om sikkerhedsforanstaltninger, dokumentation eller andre former for oplysninger omkring, hvordan Underdatabehandler behandler Personoplysninger, og sådanne overskrider de standardoplysninger, som Underdatabehandler har stillet til rådighed for opfyldelse af gældende lovgivning om behandling af Personoplysninger som Underdatabehandler, og dette medfører ekstra arbejde for Underdatabehandler, er Underdatabehandler berettiget til at opkræve Databehandler betaling for sådanne ekstra arbejder.

Underdatabehandler underretter uden unødig forsinkelse Databehandler efter at være blevet opmærksom på, at der er sket brud på persondatasikkerheden hos Underdatabehandler eller en eventuel under-underdatabehandler.

7. Kontrol

Databehandler kan foretage kontrol for at påse, at Underdatabehandler overholder denne Databehandleraftale, op til 1 gang om året.

Hvis det er et lovkrav gældende for den Dataansvarlige eller Databehandler, kan Databehandler anmode om hyppigere kontrol.

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

Hvis tredjeparter skal foretage kontrollen, skal det som hovedregel aftales mellem parterne. Hvis behandling sker i et "multitenant" miljø eller lignende, giver Databehandler Underdatabehandler ret til at bestemme, af sikkerhedsmæssige årsager, at kontrollerne skal foretages af en neutral tredjepartskontrollant efter Underdatabehandlers valg.

Hvis det anmodede kontrolomfang er behandlet i ISAE, ISO eller lignende sikkerhedsrapport, varetaget af en kvalificeret tredjepartskontrollant inden for de sidste 12 måneder, og Underdatabehandler bekræfter, at der ikke er foretaget nogle væsentlige ændringer i de kontrollerede foranstaltninger, bekræfter Databehandler, at sådanne resultater accepteres i

stedet for at anmode om en ny kontrol af de foranstaltninger, der er omfattet af rapporten.

I alle tilfælde skal kontroller foretages inden for normal arbejdstid på det pågældende sted, i medfør af Underdatabehandlers politikker og må ikke på urimelig måde gribe forstyrrende ind i Underdatabehandlers forretningsdrift.

Databehandler afholder alle omkostninger i forbindelse med Databehandlers anmodede kontroller.

Ligeledes fakturerer Underdatabehandler Databehandler for bistand, som overstiger den standardydelse, som Underdatabehandler eller Visma-koncernen stiller til rådighed for opfyldelse af gældende lovgivning om behandling af personoplysninger.

8. Brug af under-underdatabehandlere og overførsel af data

Som en del af leveringen af tjenester til Databehandler har Underdatabehandler Databehandlers generelle tilladelse til at gøre brug af under-underdatabehandlere. Disse under-underdatabehandlere kan være andre selskaber i Visma-koncernen eller eksterne tredjepartsleverandører.

Underdatabehandler skal sikre, at under-underdatabehandlere pålægges de samme forpligtelser, som fastsat i denne Databehandleraftale. Enhver brug af under-underdatabehandlere er underlagt Visma-koncernens Privacy Statement.

Databehandler har ret til at anmode om at få et overblik over under-underdatabehandlere, der aktuelt gøres brug af, med adgang til Personoplysninger, som angivet i underbilag B. Desuden har Databehandler ret til at anmode om at få fuldt overblik og mere detaljerede oplysninger om disse under-underdatabehandlere.

Databehandler skal på forhånd underrettes om eventuel udskiftning af under-underdatabehandlere, som behandler Personoplysninger. Databehandler kan gøre indsigelse mod ændringerne, såfremt Databehandler har rimelige, konkrete årsager hertil.

Underdatabehandler må ikke lade behandling af Personoplysninger foregå uden for EU/EØS uden Databehandlers samtykke.

Såfremt Databehandler giver samtykke til, at Underdatabehandleren foretager behandling af Personoplysninger uden for EU/EØS, fremgår dette af underbilag B. Underdatabehandler skal sikre et korrekt juridisk grundlag for overførsel af Personoplysninger uden for EU/EØS på vegne af Databehandler, herunder ved indgåelse af EU-kommissionens Standardkontrakt eller overførsel af Personoplysninger i henhold til Privacy Shield.

9. Varighed og ophør

Denne Databehandleraftale er gældende, så længe Underdatabehandler behandler Personoplysninger på vegne af Databehandler i henhold til Aftalen. Databehandleraftalen ophører automatisk ved opsigelse af Aftalen.

Ved Aftalens ophør sletter, returnerer eller opbevarer Underdatabehandler, de på vegne af Databehandler behandlede Personoplysninger efter aftale med Databehandler.

Medmindre andet er skriftligt aftalt, tager omkostninger til sådanne foranstaltninger udgangspunkt i:

- Timetakst for den tid Underdatabehandler har brugt, og
- Sværhedsgraden af den anmodede behandling.

Underdatabehandler 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.

10. Ændringer og tilføjelser

Ændringer til dette bilag skal udfærdiges i et nyt bilag til Aftalen.

Hvis nogen bestemmelse i denne Databehandleraftale bliver ugyldig, påvirker dette ikke gyldigheden af de øvrige bestemmelser. Parterne skal erstatte den ugyldige bestemmelse med en lovlig bestemmelse, der afspejler formålet med den ugyldige bestemmelse.

11. Ansvar

Ansvaret for brud på bestemmelserne i denne Databehandleraftale reguleres af ansvarsbestemmelserne i Regler for Lønpartners brug af DataLøn. Dette gælder også for eventuelle brud begået af Underdatabehandlers under-underdatabehandlere.

Underbilag A - Kategorier af Persondata og Registrerede

1.Kategorier af Registrerede og Persondata, der er underlagt behandling, i henhold til nærværende Aftale

a.Kategorier af registrerede

i. Lønpartners brugere

ii. Lønpartners kontaktpersoner

iii. Kundevirksomhedens Medarbejdere

b.Kategorier af Personoplysninger

i. Kontaktoplysninger, som navn, adresse, mail, telefon

ii. CPR-nr.

iii. Stillingskategori, oplysninger om løn, arbejdstid, fravær, pension, skat, bankkonto

iv. evt. øvrige Personoplysninger, der er nødvendige for, at den Dataansvarlige kan administrere ansættelsesforholdet.

c. Behandlingsaktiviteter

Underdatabehandleren varetager via it-systemer håndteringen af Databehandlers lønadministration for den Dataansvarlige, udarbejdelse af lønsedler, opbevaring og lagring af Personoplysninger om Databehandlers brugere og kontaktpersoner, den Dataansvarlige og den Dataansvarliges medarbejdere, rapportering og overførsel af information til Databehandler, den Dataansvarlige, Nets Denmark A/S, pengeinstitutter, pensionsselskaber, evt. pligtige rapporteringer i arbejdsgiverforeninger, offentlige styrelser (SKAT, statistik m.m.).

Herudover forestår Underdatabehandleren drift, test, vedligeholdelse, udvikling samt fejlretning af systemer og applikationer.

2.Typer af Følsomme persondata, der er underlagt behandling, i henhold til Aftalen

Databehandler skal give Underdatabehandler meddelelse om, og angive nedenfor, eventuelle typer Følsomme persondata i henhold til gældende lovgivning om Behandling af personoplysninger.

Underdatabehandler skal på vegne af Databehandler behandle oplysninger om:	**Ja**	**Nej**
Race eller etnisk, politisk, filosofisk eller religiøs overbevisning		X
At en person er mistænkt, sigtet eller dømt for en forbrydelse		X
Helbredsoplysninger		X
Seksuel orientering		X
Medlemskab af fagforening		X
Genetiske eller biometriske data		X

Underbilag B - Oversigt over aktuelle under-underdatabehandlere

Underdatabehandlers aktuelle under-underdatabehandlere, der kan få adgang til den Dataansvarliges Personoplysninger, omfatter ved ikrafttrædelsen af denne Databehandleraftale:

Navn	Sted/land	Juridisk overdragelsesmekanisme, hvis underdatabehandleren har adgang til Personoplysninger fra lande uden for EU	Bistår Underdatabehandleren med
Nets Denmark A/S Lautrupbjerg 10 2750 Ballerup CVR 20016175	Danmark	Ikke relevant	Datalagring Lønkørsler
Atea A/S Lautrupvang 6 2750 Ballerup CVR 25511484	Danmark	Ikke relevant	Datalagring
Solipsis Marktplein 2 5306 BA Brakel	Holland	Ikke relevant	Datalagring, E-arkiv
NetNordic Enterprise Communications A/S Lyskær 1 2730 Herlev CVR 29797056	Danmark	Ikke relevant	Datalagring, telefonsamtaler
Cohaesio A/S Per Henrik Lings Allé 4, 4. 2100 København Ø CVR 26079209	Danmark	Ikke relevant	Infrastruktur
Visma ITC AS Karenlyst alle 56 0277 Oslo	Norge	Ikke relevant	Infrastruktur
OnlineCity ApS Buchwaldsgade 50 5000 Odense C CVR 27364276	Danmark	Ikke relevant	Udsendelse af sms i forbindelse med log-on
Cim Mobilty Fælledvej 17 7600 Struer CVR 27913334	Danmark	Ikke relevant	Udsendelse af sms i forbindelse med log-on
Visma Labs SIA Sporta Street 11 Riga LV 1013 Latvia	Letland	Ikke relevant	Udvikling og fejlretning

Underbilag C – Underdatabehandlerens sikkerhedsprocedurer

Sikkerhedsprocedurer

Informationssikkerheden i Visma Dataløn er baseret på standarden ISO / IEC 27001: 2013 Informationsteknologi – Sikkerhedsteknikker.

Standarden indeholder Statement of Applicability (SOA), som er en del af Visma Dataløn Information Security Management System (ISMS). SOA udgør politikker, procedurer, processer, organisatoriske beslutningsprocesser og aktiviteter inden for følgende informationssikkerhedskontrolområder i Visma DataLøn:

- Organisering af informationssikkerhed
- Personalesikkerhed
- Styring af aktiver
- Adgangsstyring
- Kryptografi
- Fysisk sikring og miljøsikring
- Driftssikkerhed
- Kommunikationssikkerhed
- Anskaffelse, udvikling og vedligeholdelse af systemer
- Leverandørforhold
- Styring af informationssikkerhedsbrud
- Informationssikkerhedsaspekter ved nødberedskabs- og reetableringsstyring
- Compliance

Informationssikkerhed

Visma Dataløn har implementeret politikker, kontroller og processer, som dækker de nedenfor beskrevne informationssikkerhedsområder:

- **Fortrolighed**

Sikre at uautoriserede personer ikke kan få adgang til data, som kan misbruges til skade for Visma DataLøns kunder, forretningsforbindelser og ansatte.

- **Integritet**

Sikre at systemer indeholder akkurat og komplet information.

- **Tilgængelighed**

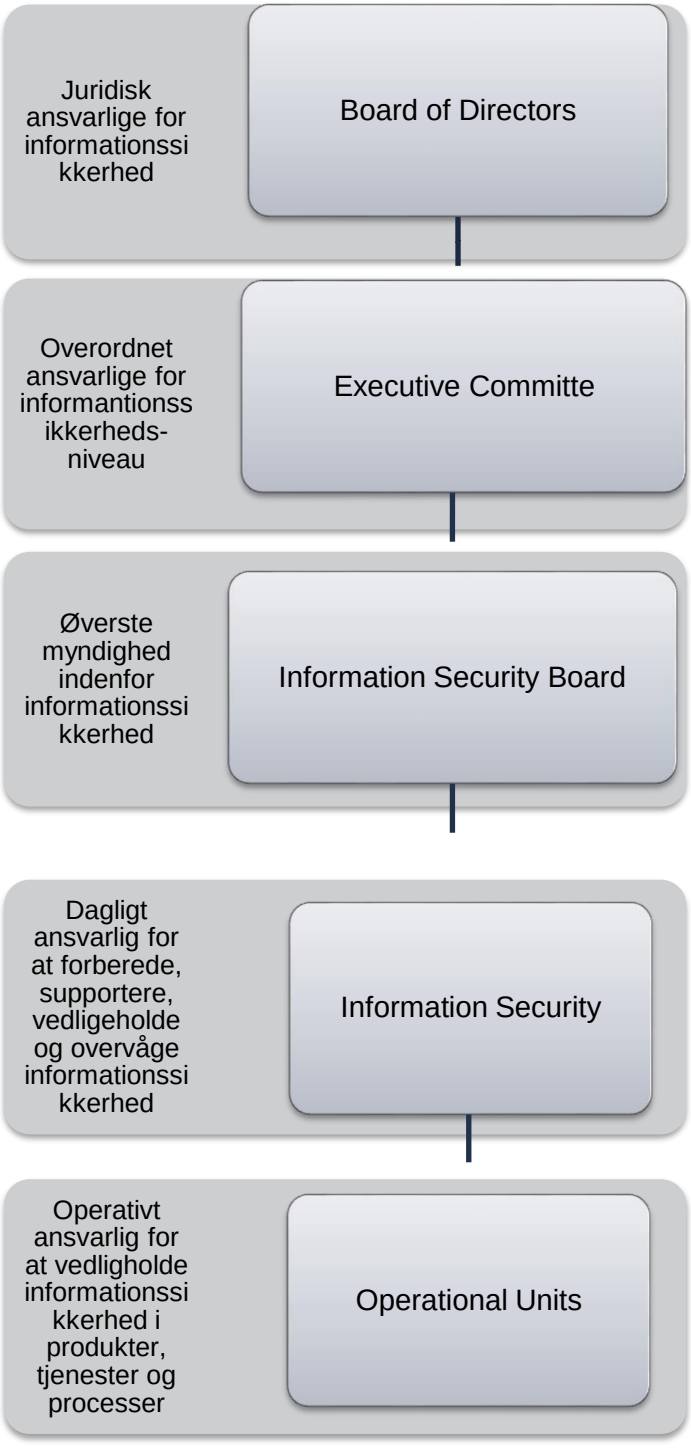
Sikre at relevant information og relevante systemer er tilgængelige og stabile.

Styring af informationssikkerhed

Styring af informationssikkerhed i Visma Dataløn er baseret på ISO 27005 Informationsteknologi - Sikkerhedsteknikker - Risikostyring af informationssikkerhed.

Informationssikkerhed, Organisation

Visma Dataløn har etableret et ledelsesrammeværk til initiering og styring af implementering samt drift af informationssikkerhed.



Personalesikkerhed

Visma Dataløn har sikret, at medarbejdere og aftaleparter har forstået deres ansvar og er kompetente til at varetage deres roller.

Asset management

Visma Dataløn har identificeret organisatoriske aktiver og defineret passende beskyttelse.

Adgangsstyring

Visma Dataløn har via godkendelses- og autorisationsprocesser sikret, at det kun er muligt at opnå en arbejdsrelateret adgang til informations- og informationsbehandlingsfaciliteter.

Kryptografi

Visma Dataløn har sikret en korrekt og effektiv brug af kryptografi for at beskytte fortrolighed, autenticiteten og integriteten af information.

Fysisk sikring og miljøsikring

Visma Dataløn forhindrer uautoriseret fysisk adgang, skade og forstyrrelse i virksomhedens informationer og databehandlingslokationer.

Driftsikkerhed

Visma Dataløn har sikret korrekt og sikker drift gennem dokumenterede procedurer og processer.

Kommunikationssikkerhed

Visma Dataløn har sikret beskyttelse af information på netværk og databehandlingslokationer.

Anskaffelse, udvikling og vedligeholdelse af systemer

Al ekstern erhvervelse eller forbedring/fornyelse af informationssystemer, tjenester og komponenter i Visma Dataløn er centralt evalueret og godkendt for at sikre compliance.

Politik til udvikling og vedligeholdelse af services er etableret og anvendes til udviklingen i organisationen.

Leverandørforhold

Visma Dataløn har sikret beskyttelse af virksomhedens aktiver, der er tilgængelige for leverandører, herunder regelmæssig overvågning og revision af leverandørleverancer.

Styring af informationssikkerhedsbrud

Visma Dataløn har en konsekvent og effektiv tilgang til styring af informationssikkerhedshændelser, herunder kommunikation om sikkerhedshændelser og svagheder.

Informationssikkerhedsaspekter ved nødberedskabs- og reetableringsstyring

Visma DataLøn sikrer kontinuitet og rettidig genopretning af forretningskritiske processer og systemer i tilfælde af en kritisk situation og sikrer, at kritiske processer virker på et hensigtsmæssigt niveau.

Compliance

Visma Dataløn har implementeret procedurer for at undgå brud på juridiske, lovmæssige eller kontraktlige forpligtelser i forbindelse med informationssikkerhed og eventuelle sikkerhedskrav.