Databehandleraftale

Version 2.0

mellem

den dataansvarlige (Kunden)

og

Azets ATB ApS
Lyskær 3C
DK-2730 Herlev
Danmark
CVR 25 22 96 49

herefter ”databehandleren”

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

Vedrørende behandling af personoplysninger

Erstatter alle tidligere indgåede databehandleraftaler mellem parterne

Indholdsfortegnelse

1. Baggrund og formål

1.1 Databehandleren (Leverandøren) og den dataansvarlige (Kunden) har aftalt følgende standard-kontraktbestemmelser (Bestemmelserne) med henblik på at overholde databeskyttelsesforordningen og sikre beskyttelse af privatlivets fred og fysiske personers grundlæggende rettigheder og friheds-rettigheder.

1.2 Bestemmelserne tager udgangspunkt i Datatilsynets standardkontraktbestemmelser (version 1.1 - januar 2020) i henhold til artikel 28, stk. 3 i forordning 2016/679 med henblik på databehandlerens behandling af personoplysninger.

2. Præambel

2.1 Disse Bestemmelser fastsætter databehandlerens rettigheder og forpligtelser, når denne foretager behandling af personoplysninger på vegne af den dataansvarlige.

2.2 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).

2.3 I forbindelse med leveringen af Services behandler databehandleren personoplysninger på vegne af den dataansvarlige i overensstemmelse med disse Bestemmelser.

2.4 Bestemmelserne har forrang i forhold til eventuelle tilsvarende bestemmelser i andre aftaler mellem parterne.

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

2.6 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.

2.7 Bilag B indeholder den dataansvarliges betingelser for databehandlerens brug af underdatabehandlere og en liste af underdatabehandlere, som den dataansvarlige har godkendt brugen af.

2.8 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.

2.9 Bilag D indeholder bestemmelser vedrørende andre aktiviteter, som ikke af omfattet af Bestemmelserne.

2.10 Bestemmelserne med tilhørende bilag skal opbevares skriftligt, herunder elektronisk, af begge parter.

2.11 Disse Bestemmelser frigør ikke databehandleren fra forpligtelser, som databehandleren er pålagt efter databeskyttelsesforordningen eller enhver anden lovgivning.

3. Den dataansvarliges rettigheder og forpligtelser

3.1 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.

3.2 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.

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

3.3 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

4.1 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.

4.2 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

5.1 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.

5.2 Databehandleren skal efter anmodning fra den dataansvarlige kunne påvise, at de pågældende personer, som er underlagt databehandlerens instruktionsbeføjelser, er underlagt ovennævnte tavshedspligt.

6. Behandlingssikkerhed

6.1 Databeskyttelsesforordningens 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:

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.

6.2 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.

6.3 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 al anden information, der er nødvendig for den dataansvarliges overholdelse af sin forpligtelse efter forordningens 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.

7. Anvendelse af underdatabehandlere

7.1 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).

7.2 Databehandleren må således ikke gøre brug af en underdatabehandler til opfyldelse af disse Bestemmelser uden forudgående generel skriftlig godkendelse fra den dataansvarlige.

7.3 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 to (2) ugers 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.

7.4 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.

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

7.6 Udgået (valgfrit).

7.7 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 databeskyttelsesforordningen, herunder særligt forordningens artikel 79 og 82, over for den dataansvarlige og databehandleren, herunder underdatabehandleren.

8. Overførsel til tredjelande eller internationale organisationer

8.1 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.

8.2 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.

8.3 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

8.4 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.

8.5 Disse Bestemmelser skal ikke forveksles med standardkontraktsbestemmelser 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

9.1 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. indsigtsretten
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

9.2 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 unødig 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 unødig 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.

9.3 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

10.1 Databehandleren underretter uden unødig forsinkelse den dataansvarlige efter at være blevet opmærksom på, at der er sket et brud på persondatasikkerheden.

10.2 Databehandlerens underretning til den dataansvarlige skal om muligt ske senest 48 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.

10.3 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.

10.4 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

11.1 Ved ophør af Services vedrørende behandling af personoplysninger, er databehandleren forpligtet til at tilbagelevere alle personoplysningerne og slette eksisterende kopier, medmindre EU-retten eller medlemsstaternes nationale ret foreskriver opbevaring af personoplysningerne.

11.2 Følgende regler i EU-retten eller medlemsstaternes nationale ret foreskriver opbevaring af personoplysningerne efter ophør af tjenesterne vedrørende behandling af personoplysninger:

a. Bogføringsloven (Danmark)

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

12.1 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.

12.2 Procedurerne for den dataansvarliges revisioner, herunder inspektioner, med databehandleren og underdatabehandlere er nærmere angivet i Bilag C.7. og C.8.

12.3 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.

13. Parternes aftale om andre forhold

13.1 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

14.1 Bestemmelserne træder i kraft på datoen for begge parters underskrift heraf.

14.2 Begge parter kan kræve Bestemmelserne genforhandlet, hvis lovændringer eller uhensigtsmæssigheder i Bestemmelserne giver anledning hertil.

14.3 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.

14.4 Hvis levering af tjenesterne vedrørende behandling af personoplysninger ophører, og personoplysningerne er slettet eller returneret til den dataansvarlige i overensstemmelse med Bestemmelse 11.1 og Bilag C.4, kan Bestemmelserne opsiges med skriftlig varsel af begge parter.

15. Kontaktpersoner hos den dataansvarlige og databehandleren

15.1 Parterne kan kontakte hinanden via nedenstående kontaktpersoner.

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

På vegne af den dataansvarlige:

I henhold til hoveddokument i indgået Aftale.

På vegne af databehandleren:

Telefonnummer	+45 70 27 31 30
E-mail	gdpr-dk@azets.com

Bilag A Oplysninger om behandlingen

A.1 Formålet med databehandlerens behandling af personoplysninger på vegne af den dataansvarlige og **A.2** Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige drejer sig primært om (karakteren af behandlingen)	Databehandleren må alene behandle personoplysninger til de formål, som er nødvendige for at opfylde aftalen med den dataansvarlige herunder opbevaring, indsamling, registrering, systematisering, samkøring, sletning, arkivering etc. Hvor de i aftale om levering af Services involverede IT-systemer tilbyder den dataansvarlige mulighed for API integration er følgende aftalt: • Den dataansvarlige accepterer at dataansvarlig og dennes medarbejdere m.fl. har mulighed for at installere og gøre brug af tredjeparts-app(s), der kan kommunikere og udveksle den enkeltes oplysninger herunder personoplysninger med involverede IT-systemer og at sådan databehandling er omfattet af omstående instruks • Den dataansvarlige indlæser de oplysninger, som er nødvendige for brug af tjenesterne samt instruerer databehandleren i løbende og automatisk at indhente og/eller udveksle indtastede, indlæste og/eller de af involverede IT-systemer genererede oplysninger herunder personoplysninger • Ved den dataansvarliges installation og accept af tredjeparts-app(s), opstår et selvstændigt retsforhold mellem den dataansvarlige og leverandøren af tredjeparts-app(s) • Brugen af tredjeparts-app(s) er således underlagt de pågældende app-leverandørers vilkår og databehandleren er uden ansvar for den dataansvarliges brug af sådanne tredjeparts-apps samt de pågældende app-leverandørers behandling og opbevaring af personoplysninger efter, at disse er overført Databehandleren er forpligtet til løbende og automatisk at indhente personoplysninger fra relevante myndigheder for at sikre, at oplysninger til brug for Services til stadighed er opdaterede. Databehandleren er forpligtet til at behandle personoplysninger som påkrævet i henhold til lovgivningen, herunder i forbindelse med retlig afgørelse, myndighedskrav, den dataansvarliges konkurs, dødsfald eller lignende. Databehandleren er således forpligtet til at efterleve udleveringspligten i bogføringsloven ved at give myndigheder adgang til data. Databehandleren er desuden berettiget til at anonymisere personoplysninger til statistiske formål. Databehandleren er berettiget til at lade personoplysninger indgå i databehandlerens sædvanlige backup-procedure. Databehandleren og dennes underdatabehandlere forbeholder sig retten til at udlevere data til den dataansvarliges tegningsberettigede så længe serviceaftale er aktiv. Under igangværende serviceaftale og efter serviceaftalens ophør er underdatabehandler berettiget til at behandle applikationsdata i anonymiseret form til at vedligeholde og udvikle applikation herunder sikkerhedsforanstaltninger og brugeroplevelser.
A.3 Behandlingen kan omfatte følgende typer af personoplysninger om de registrerede	Behandlingen kan omfatte: • almindelige personoplysninger • følsomme personoplysninger • fortrolige personoplysninger Konkrete personoplysninger er anført i Bilag D.2 i sammenhæng med Services.

	Behandlingen omfatter ikke: • genetiske eller biometriske data • racemæssig eller etnisk baggrund eller politisk, filosofisk eller religiøs overbevisning • seksuel orientering
A.4 Behandlingen omfatter følgende kategorier af registrerede	Behandlingen kan omfatte den dataansvarliges: • nuværende og tidligere medarbejdere • honorarmodtagere • potentielle medarbejdere • kunder, leverandører og øvrige samarbejdspartnere • medlemmer af boligforening (andelsboligforening, ejerforening, grundejerforening og lignende) samt boligforeningens ansatte, bestyrelsesmedlemmer, lejere/beboere/fremlejere, leverandører og øvrige samarbejdspartnere • ejere af udlejningsejendomme/lejemål samt disses ansatte, bestyrelsesmedlemmer. lejere/beboere/fremlejere, leverandører og øvrige samarbejdspartnere Sammenhæng med Services er anført i Bilag D.3.
A.5. Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige kan påbegyndes efter disse Bestemmelsers ikrafttræden. Behandlingen har følgende varighed	Databehandlingen af personoplysninger følger varigheden anført i enhver aktiv serviceaftale, samt dataansvarliges instruktion i Bestemmelse 11.1 og 11.2. Jf. dog undtagelser i C.4 (Opbevaringsperioder/sletterutiner).

Bilag B Underdatabehandlere

B.1. Godkendte underdatabehandlere

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

NAVN	CVR	ADRESSE	BESKRIVELSE AF BEHANDLING
Azets Insight SRL	VAT RO24813426 Org. J32/1906/2008	Str. Nicolaus Olahus, nr. 5 Et. 9-10 550370 Sibiu, Rumænien	Administrativ assistance
Azets Insight AS	Org. Nr. 983 338 917	Drammensveien 151 NO-0101 Oslo	Hosting/drift af applikationerne: • Azets Invoice/Reporting • Visma Business hvor alle data opbevares hos dennes underdatabehandler AWS i Stockholm (EU-North-1) og Ireland (EU-West-1)
Azets Labs A/S	CVR nr. 10 40 77 45	Lyskær 3 CD DK-2730 Herlev	SaaS: Hosting/drift, udvikling og vedligeholdelse af applikationerne: • Azets EPOS Løn, hvor alle data opbevares hos dennes underdatabehandler AWS i Stockholm (EU-North-1) og Ireland (EU-West-1) • Workcyclus APV-produkter, hvor alle data opbevares hos dennes underdatabehandler Azure i West Europe (Holland)
Azets Perspektiv A/S	CVR nr. 43 09 57 57	Lyskær 3C, st. DK-2730 Herlev	SaaS: Hosting/drift, udvikling og vedligeholdelse af applikationen Azets Perspektiv inklusive MIT Perspektiv moduler samt applikationen Azets Perspektiv Tid. Alle data opbevares i Danmark, hvor underdatabehandlerens maskinel er placeret på to (2) eksterne datacentre (housing).
Azets Software AB	Org. nr. 559273-6937	Ekensbergvägen 113 SE-171 41 Solna	SaaS: Hosting/drift, udvikling og vedligeholdelse af applikationen Azets Cozone Portal/Activity/Drive/ Employee. Alle data opbevares hos dennes underdatabehandler AWS i Stockholm (EU-North-1) og Europe Ireland (EU-West-1)
e-Boks A/S	CVR nr. 25 67 41 54	Hans Bekkevolds Allé 7 DK-2900 Hellerup	Digital modtagelse af lønsedler fra PostNord Strålfors A/S (metode 2 ”Azets” og 3 ”kundenavn”, midlertidig opbevaring og distribution til modtagere i e-Boks i forbindelse med lønadministration i applikationerne EPOS Løn, Azets EPOS Løn og Azets Perspektiv. Alle data opbevares hos dennes underdatabehandler i Danmark
EG Danmark A/S (EG Bolig)	CVR nr. 84 66 78 11	Lautrupvang 24 DK-2750 Ballerup	SaaS: Hosting/drift, udvikling, vedligeholdelse og support af ejendomsadministrationssystemet ProBo Alle data opbevares hos dennes underdatabehandler i Europa
Findity AB	Org. nr. 556838-8200	Engelbrektsgatan 20 SE-771 30 Ludvika	SaaS: Hosting/drift, udvikling og vedligeholdelse af rejseafregningssystemet Azets Expense. Alle data opbevares i Sverige, hvor underdatabehandlerens maskinel er placeret på to (2) eksterne datacentre (housing)

NAVN	CVR	ADRESSE	BESKRIVELSE AF BEHANDLING
Freshworks Inc.	Org. Nr. 33-1218825	2950 S. Delaware Street, Suite 201,94403 San Mateo, CA USA	SaaS: Hosting/drift, udvikling og vedligeholdelse af Freshdesk (supportsystem). Alle data opbevares hos dennes underdatabehandler AWS i flere tilgængelighedszoner i Frankfurt (EU-Central-1), hver med mindst 35 km's afstand
PostNord Strålfors A/S	CVR nr. 10 06 86 57	Hedegaardsvej 88 DK-2300 København S	• Digital modtagelse, midlertidig opbevaring og videreforsendelse af lønsedler til E-Boks A/S *(metode 2 "Azets" og metode 3 "Kundenavn")* i forbindelse med lønadministration på applikationerne EPOS Løn, Azets Epos Løn og Azets Perspektiv • Digital modtagelse, midlertidig opbevaring og distribution af lønsedler til modtagere i e-Boks *(metode 1 "Din arbejdsgiver")* i forbindelse med lønadministration på applikationerne EPOS Løn, Azets EPOS Løn og Azets Perspektiv • Digital modtagelse, midlertidig opbevaring og distribution af lønsedler til modtagere i mit.dk i forbindelse med lønadministration på applikationerne EPOS Løn, Azets EPOS Løn og Azets Perspektiv • SaaS: Hosting/drift, udvikling, vedligeholdelse og support af eDistributionsløsning af henvendelser til den dataansvarlige i offentlige digitale postkasser (eksempelvis Virk.dk, e-Boks og mit.dk) Alle data opbevares i Danmark og hos dennes underdatabehandler i Sverige
Twoday Danmark A/S	CVR nr. 29 97 33 34	Sundkaj 125 DK-2150 Nordhavn	SaaS: Hosting/drift, udvikling, vedligeholdelse og support af applikationen Addo Sign til juridisk gyldig digital signering og distribution af dokumenter efter validering af brugernes identitet. Alle data opbevares hos dennes underdatabehandler i Danmark
Unik System Design A/S	CVR. nr. 17 51 26 92	Boulevarden 19E, DK-7100 Vejle	SaaS: Hosting/drift, udvikling, vedligeholdelse og support af ejendomsadministrationssystemet Unik Bolig CE / HabiCen. Alle data opbevares hos dennes underdatabehandler i Danmark
Visma e-conomic A/S	CVR nr. 29 40 34 73	Gærtorvet 1-5 DK-1799 København V	SaaS: Hosting/drift, udvikling, vedligeholdelse og support af applikationen e-conomic. Alle data opbevares hos dennes underdatabehandlere i Holland (Google Cloud).
Visma IMS A/S	CVR nr. 25 86 20 15	Søren Frichs Vej 440 DK-8230 Åbyhøj	SaaS: Hosting/drift, udvikling og vedligeholdelse af ESDH-system IMS Case. Alle data opbevares hos dennes underdatabehandlere i henholdsvis Danmark og Schweiz
Wolters Kluwer Danmark A/S	CVR nr. 13 38 62 93	Sturlasgade 3 DK-2300 København S	Support I udnyttelse af følgende licenserede produkter: • Årsafslutning Professionel til udarbejdelse af årsrapport inklusive manuel upload til indberetning af regnskabsdata via iXBRL til Erhvervsstyrelsen • Skat Professionel Nova til udarbejdelse af selvangivelser samt opstilling af indkomst- og formueopgørelser Alt data opbevares i Danmark hos databehandleren; dog således at data i undtagelsesvise support

NAVN	CVR	ADRESSE	BESKRIVELSE AF BEHANDLING
			situationer kortvarigt udveksles til underdatabehandler med henblik på analyse og test af systemmæssigt problem.
Zebon ApS	CVR nr. 32 36 64 49	Nordre Strandvej 119 A DK-3150 Hellebæk	SaaS: Hosting/drift, udvikling og vedligeholdelse af rejseafregningssystemet zExpense. Alt data opbevares i Danmark, hvor underdatabehandlerens maskinel er placeret på to (2) eksterne datacentre (housing).
Zenegy Danmark ApS	CVR nr. 38 36 60 41	Slotsmarken 16 DK-2970 Hørsholm	SaaS: Hosting/drift, udvikling og vedligeholdelse af applikationen Azets Simplify. Alle data opbevares hos dennes underdatabehandler Microsoft Azure i Holland.

Sammenhæng med Services er anført i Bilag D.4.

Ved Bestemmelsernes ikrafttræden har den dataansvarlige godkendt brugen af ovennævnte underdata-behandlere 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

C.1 Behandlingens genstand/instruks	Databehandlerens behandling af data på vegne af den dataansvarlige sker ved, at databehandleren udfører følgende: Se Bilag A punkt A.1/A.2. Den dataansvarlige accepterer at der i forbindelse med eventuelle kundespecifikke- og fritekstfelter i IT-løsning(er) inklusive tilhørende dokumenter ikke angives andre personoplysninger end de, der er angivet i Bilag A punkt A.3. Såfremt den dataansvarlige angiver andre personoplysninger end de, der er angivet i Bilag A, skal den dataansvarlige straks underrette databehandleren herom og opdatere instruksen i Bestemmelserne. Den dataansvarlige accepterer i forbindelse med databehandlerens håndtering af digitale dokumenter fra offentlige digitale postkasser til den dataansvarlige, at det er afsender, som bestemmer indhold. Derved kan digitale dokumenter indeholde både almindelige og følsomme personoplysninger i et ikke nærmere afgrænset omfang ud over de, der er angivet i Bilag A punkt 3.
C.2 Behandlingssikkerhed. Sikkerhedsniveauet skal afspejle:	Behandlingen af data omfatter personoplysninger, som nævnt i Bilag A punkt A.3/A.4 og som kan være - men ikke nødvendigvis er - omfattet af Databeskyttelsesforordningen artikel 9 om "særlige kategorier af personoplysninger", hvorfor der skal etableres et "højt" sikkerhedsniveau. Databehandleren er 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 garanterer over for den dataansvarlige, at databehandleren vil gennemføre de passende tekniske og organisatoriske foranstaltninger på en sådan måde, at databehandlerens behandling af personoplysninger opfylder kravene i den til enhver tid gældende persondataretlige regulering. Databehandleren skal dog - under alle omstændigheder og som minimum - gennemføre foranstaltningerne beskrevet i punkt C.2.1-C.2.15, som er aftalt med den dataansvarlige.
C.2.1 Pseudonymisering og kryptering af personoplysninger	Databehandleren er forpligtet til at gennemføre og opretholde passende tekniske og organisatoriske foranstaltninger, der sikrer, at personoplysninger pseudonymiseres, hvor relevant for services. Databehandleren er forpligtet til at gennemføre og opretholde passende tekniske og organisatoriske foranstaltninger, der sikrer, at personoplysningerne krypteres eller på anden vis beskyttes mod bl.a. uvedkommendes adgang og/eller manipulation, herunder særligt i forbindelse med transmission via åbne netværk og/eller eksterne kommunikationsforbindelser. Niveauet af kryptering skal være passende for effektivt at forhindre uvedkommende i at få adgang til personoplysninger. Se punkt C.2.7.

C.2.2 Sikring af fortrolighed, integritet, tilgængelighed og robusthed af behandlingssystemer og -services	Databehandlerens medarbejderes tavshedspligt er specificeret i punkt C.2.6. Databehandlerens tekniske sikkerhed: • Virusdefinitioner opdateres dagligt • Lokal firewall på Pc'er og servere er aktiveret • Netværk er beskyttet af firewall • Løbende interne og eksterne sårbarhedsscanninger for at sikre optimal konfiguration • Medarbejdere og eksternt tilknyttede konsulenter har ekstern adgang til netværk via krypterede forbindelser med MFA • Data på alle Pc'er er krypteret • Der anvendes komplekse passwords • Udveksling af persondata med dataansvarlig m.fl. sker via krypterede forbindelser, for eksempel SFTP eller webportaler • Løbende backup af data Databehandlerens organisatoriske sikkerhed: • Autorisationsprocedurer, adgangsrettigheder, logning mv. i henhold til databehandlerens interne IT-procedurer • Medarbejdere og eksternt tilknyttede konsulenter modtager sikkerhedstræning og fyldestgørende instruktioner i og retningslinjer for behandling af personoplysninger og IT-sikkerhed
C.2.3 Genoprettelse af personoplysningerne og drift (omfatter alle systemer medmindre de er anført med særlig kommentar)	Databehandleren er forpligtet til at gennemføre og opretholde passende tekniske og organisatoriske foranstaltninger, der sikrer rettidig genoprettelse af tilgængelighed til personoplysningerne i tilfælde af fysiske hændelser (f.eks. strømafbrydelse, brand, oversvømmelse, lynnedslag mv.) og/eller tekniske hændelser (systemnedbrud mv.), herunder i form af beredskabsplaner, procedurer mv. Databehandler er forpligtet til at gennemføre og opretholde dokumenterede beredskabsprocedurer, der sikrer genetablering af services uden ugrundet ophold i tilfælde af driftsafbrydelser. Lønadministration på Applikationen Perspektiv inklusive Mit Perspektiv moduler og applikationen Perspektiv Tid: • Databehandleren har beredskab samt disaster recovery løsning. Løsningen er "standby", hvorved forstås at hardware platformen er etableret og parat til at blive anvendt til reetablering/restore. Målet er reetablering indenfor fireogtyve (24) timer Applikationen Azets Expense (rejseafregninger): • Databehandleren har beredskab samt disaster recovery løsning. Løsningen er "standby", hvorved forstås at hardware platformen er etableret og parat til at blive anvendt til reetablering/restore. Målet er reetablering indenfor fireogtyve (24) timer
C.2.4 Procedure for regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske foranstaltninger til sikring af behandlingssikkerhed	Databehandleren er forpligtet til at gennemføre og opretholde passende tekniske og organisatoriske foranstaltninger for regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske foranstaltninger til sikring af behandlingssikkerhed. Databehandleren gennemfører årlig kontrol med underleverandører ved gennemgang af databehandleraftaler for de enkelte underleverandører samt en risikovurdering. Eventuelle problemstillinger følges op (jf. punkt C.8).

C.2.5 Personalets adgang til personoplysninger	Databehandleren sikrer via formelle godkendelsesprocesser samt tilbagevendende kontrol af adgange, at kun personer med et dokumenteret arbejdsrelateret behov, har adgang til personoplysninger. Databehandleren skal uden ugrundet ophold annullere autorisationer (og herunder adgange) for brugere, der ikke længere har et arbejdsbetinget behov for autorisation.
C.2.6 Tavshedspligt (omfatter alle systemer medmindre de er anført med særlig kommentar)	Alle medarbejdere hos databehandleren og eksternt tilknyttede konsulenter er underlagt kontraktuel tavshedspligt med hensyn til alt, hvad medarbejderen under sit arbejde for databehandleren erfarer om alle forretningsmæssige og fortrolige oplysninger, som vedrører parter, som databehandleren har forbindelse med. Tavshedspligten er også gældende efter ansættelsesforholdets ophør. Monitering og tømning af digitale postkasser med Applikationen eDistribution: • Alle underdatabehandlerens egne medarbejdere i Danmark med adgang til personoplysninger skal være underlagt PET sikkerhedsgodkendelse til klassifikation "Fortroligt". Sikkerhedsgodkendelsen skal kunne opretholdes under hele medarbejderens ansættelse hos underdatabehandleren
C.2.7 Beskyttelse af data under transmission og opbevaring (omfatter alle systemer medmindre de er anført med særlig kommentar)	Databehandleren er forpligtet til at gennemføre og opretholde passende tekniske og organisatoriske foranstaltninger, der sikrer, at personoplysninger beskyttes mod bl.a. uvedkommendes adgang og/eller manipulation. Kryptering af transportlaget skal til enhver tid opfylde Datatilsynets minimumskrav. Lønadministration på applikationen EPOS Løn: • Ekstern fillevering til og fra løsningen sker via SFTP • Webservice mellem EPOS Løn og EPOS HR er krypteret • Løsningen er en client-server-løsning, som tilgås via databehandlerens netværk. Data i løsningen er beskyttet via adgangskontrol på flere niveauer. Via Cisco ISE sikres det, at kun autoriserede medarbejdere kan tilgå lønmiljøet. Adgang kræver desuden logisk adgang til data via AD-grupper og via brugeradgange direkte i databasen Lønadministration på applikationen Perspektiv inklusive Mit Perspektiv moduler: • Ekstern fillevering til og fra løsningen sker via SFTP Applikationen EPOS Løn, EPOS HR og EPOS Rekruttering: • Ekstern fillevering til og fra løsningen sker via SFTP • For hostede kunder tilgås dedikeret database via sikker portal med MFA af navngivne brugere. Al kommunikation til og fra løsningen er krypteret, enten via webservices, HTTPS-forespørgsler eller webløsningen Applikationen EPOS Management: • Applikationen er krypteret add-on mellem Kundens Excel og EPOS HR. Data fødes alene fra EPOS HR Applikationen Addo Sign: • Løsningen tilgås i krypteret form via web • Al kommunikation til og fra løsningen er krypteret, enten via HTTPS-forespørgsler via webløsningen eller kommunikation via API ved brug af VOCES-certifikater Applikationen IMS Case (ESDH-system): • Løsningen tilgås i krypteret form via web

	• Al kommunikation til og fra løsningen er krypteret, enten via HTTPS-forespørgsler via webløsningen eller kommunikation via API
C.2.8 Fysisk sikring af lokaliteter, hvor der behandles persondata	Databehandleren er forpligtet til at gennemføre og opretholde passende fysiske, tekniske og organisatoriske foranstaltninger, der sikrer de fysiske lokaliteter, hvor personoplysninger behandles mod blandt andet uvedkommendes adgang og/eller manipulation af data. Der er etableret fysisk adgangssikkerhed, således at kun autoriserede personer kan opnå fysisk adgang til lokaler og datacentre, hvori der opbevares og behandles personoplysninger.
C.2.9 Sikkerhedskopiering	Sikkerhedskopiering af systemer, konfigurationsfiler og data skal finde sted således, at relevant data kan reetableres. Sikkerhedskopierne opbevares således, at de ikke hændeligt eller ulovligt (eksempelvis ved brand, oversvømmelse, uheld, tyveri eller lignende) tilintetgøres, fortabes, forringes, kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med de til enhver tid gældende regler og forskrifter for behandling af personoplysninger. Herunder bl.a.: • Der gælder de samme retningslinjer for sikkerhedskopier, som for al anden behandling af personoplysninger i medfør af aftale og denne databehandleraftale • Sikkerhedskopier opbevares geografisk adskilt fra det primære datacenter • Databehandleren kontrollerer løbende, at sikkerhedskopier er læsbare Sikkerhedskopiering finder sted af databehandlerens samlede miljø inklusive database med det formål at kunne rekonstruere dette. Backup har således ikke til formål at kunne genetablere enkelte kunders data.
C.2.10 Passwordpolitik og kontrol med afviste adgangsforsøg (omfatter alle systemer medmindre de er anført med særlig kommentar)	Databehandleren er forpligtet til at gennemføre og opretholde passende tekniske og organisatoriske foranstaltninger, som sikrer at adgangskoder har passende længde og kompleksitet for at forhindre, at de kan gættes. Adgangskoder skal være unikke for den enkelte medarbejder og eksternt tilknyttede konsulent. Databehandleren er forpligtet til at registrere afviste adgangsforsøg og blokere for yderligere forsøg efter fastlagt antal på hinanden følgende afviste adgangsforsøg. Applikationen Azets Simplify: • Passwords er SHA256 krypteret med unik salt Applikationen Addo Sign: • Passwords er hashed og saltet
C.2.11 Anvendelse af hjemmearbejdspladser	Databehandleren er forpligtet til at gennemføre og opretholde passende tekniske og organisatoriske foranstaltninger, der sikrer, at personoplysninger beskyttes mod blandt andet uvedkommendes adgang og/eller manipulation, når disse tilgås fra hjemme- og fjernarbejdspladser, og at der ved adgang til personoplysninger fra hjemme- og fjernarbejdspladser anvendes kryptering af kommunikationsforbindelser samt autentifikation af personer, som får adgang. Alle computere er krypterede og adgangskodebeskyttede. Adgang til databehandlerens systemer sker via VPN-forbindelse med MFA. Eventuelt print minimeres i videst muligt omfang og skal makuleres efter brug.

	Medarbejdere og eksterne konsulenter skal regelmæssigt gennemgå obligatorisk awareness træning i henhold til punkt C.2.12.
C.2.12 Awareness træning	Databehandleren er forpligtet til at sikre, at medarbejdere og eksternt tilknyttede konsulenter regelmæssigt (og mindst årligt) gennemgår obligatorisk undervisning om IT-sikkerhed og databeskyttelse.
C.2.13 Ændringshåndtering	Databehandleren er forpligtet til at have formelle procedurer for ændringshåndtering med henblik på at sikre, at enhver ændring er behørigt autoriseret, testet og godkendt inden implementering.
C.2.14 Logning (omfatter alle systemer medmindre de er anført med særlig kommentar)	Databehandleren er forpligtet til at gennemføre og opretholde passende tekniske og organisatoriske foranstaltninger, som sikrer logning, så hændelser kan spores. Logs skal indeholde tidsstempling og hvor relevant, bruger-id, terminal-ID samt netværks adresser. Som minimum skal følgende sikkerhedshændelser logges: • afviste adgangsforsøg • succesfulde og afviste autentifikationsforsøg som følge af konto lockout udløst af adgangskontrolsystem Tilgang til personoplysningerne skal logges i et sådant omfang, at logoplysningerne kan anvendes til at afværge og forebygge uberettiget adgang til personoplysninger. Hvor relevant, skal adgang til personoplysninger logges, herunder, hvilke data der tilgås, behandlingen af data samt tid og identitetsoplysninger. Log opbevares maksimalt i tretten (13) måneder. I tilfælde af hændelser, kan opbevaring forlænges. Backup arkiv gemmes maksimalt i seks (6) år (jf. Bilag D vedrørende Bestemmelse 11.1 og 11.2). I samme periode er databehandleren berettiget til at lade personoplysningerne indgå i databehandlerens sædvanlige backupprocedure. Lønadministration på applikationen Perspektiv Løn inklusive Mit Perspektiv moduler samt applikationen Perspektiv Tid: • Log opbevares maksimalt i hundredefirs (180) dage. I tilfælde af hændelser, kan opbevaring forlænges. • I samme periode er databehandleren berettiget til at lade personoplysninger indgå i databehandlerens sædvanlige backupprocedure. Ejendomsadministration på applikationen Unik Bolig CE / HabiCen: • Log opbevares i minimum seks (6) måneder. • I samme periode er databehandleren berettiget til at lade personoplysninger indgå i databehandlerens sædvanlige backupprocedure. Applikationen Azets Expense (rejseafregninger): • Log opbevares maksimalt i tredive (30) dage. I tilfælde af hændelser, kan opbevaring forlænges. • I samme periode er databehandleren berettiget til at lade personoplysninger indgå i databehandlerens sædvanlige backupprocedure.
C.2.15 Databeskyttelsesrådgiver og IT-sikkerhedspersonale	Databehandleren skal sikre, at der er fokus på informationssikkerheden i egen organisation med defineret rolle- og ansvarsfordeling. Databehandleren er forpligtet til at have udpeget en, eller flere, databeskyttelsesrådgivere, som beskrevet i Databeskyttelsesforordningen. Databehandleren er forpligtet til at have dedikerede ressourcer til at opretholde databehandlerens IT-sikkerhed.

C.3 Bistand til den dataansvarlige	Databehandleren skal i nødvendigt og rimeligt omfang bistå ved den dataansvarliges opfyldelse af dennes forpligtelser ved behandling af personoplysninger, der er omfattet af Bestemmelserne i punkt 9 og 10 ved at gennemføre sådanne tekniske og organisatoriske foranstaltninger, som kan bidrage til den dataansvarliges mulighed for at besvare anmodninger om udøvelse af de registreredes rettigheder.
C.4 Opbevaringsperiode/sletterutiner (omfatter alle systemer medmindre de er anført med særlig kommentar)	Personoplysninger opbevares i maksimalt seks (6) år i henhold bogføringslovens krav (jf. Bilag D vedrørende Bestemmelse 11.1 og 11.2). Ved ophør af Services vedrørende behandling af personoplysninger, skal databehandleren enten slette eller tilbagelevere personoplysningerne i overensstemmelse med Bestemmelse 11.1, medmindre den dataansvarlige – efter underskriften af disse bestemmelser – har ændret det oprindelige valg. Sådanne ændringer skal være dokumenteret og opbevares skriftligt, herunder elektronisk, i tilknytning til Bestemmelserne. Udarbejdelse af årsrapport og selvangivelse på applikationerne Årsafslutning Professionel og Skat Professionel Nova: • For data, som databehandleren undtagelsesvis stiller til rådighed for underdatabehandler til brug for løsning af supportopgave, slettes data hos underdatebehandler ultimo den måned, hvor supportopgave har været afsluttet i tre (3) måneder. Ejendomsadministration på applikationen Unik Bolig CE / HabiCen: • Ved ophør skal databehandleren slette alle personoplysninger, som databehandleren behandler på vegne af den dataansvarlige, senest halvfems (90) dage efter serviceaftalens ophør, såfremt den dataansvarlige ikke senest tredive (30) dage efter serviceaftalens ophør instruerer databehandleren i alt tilbagelevere personoplysningerne Applikationen Workcyclus (arbejdspladsvurdering): • Personoplysninger opbevares som standard i tre (3) måneder efter serviceaftalens ophør, hvorefter de slettes hos underdatabehandler Applikationerne zExpense (rejseafregninger) og Azets Expense (rejseafregninger): • Ved ophør skal den dataansvarlige senest tre (3) måneder efter serviceaftalens ophør via applikationens eksportfacilitet eksportere alle data inklusive billeder af fakturaer, kvitteringer og lignende til Excel med henblik på overholdelse af bogføringsloven og/eller overførsel til andet system Digital modtagelse, midlertidig opbevaring og videreforsendelse af lønsedler til e-Boks A/S og/eller leverance af lønsedler i e-Boks og mit.dk (PostNord): • Personoplysninger opbevares som standard i tredive (30) dage, hvorefter de slettes hos underdatabehandleren. Datebehandleren har dog indgået aftale med underdatabehandleren om mulighed for anvendelse af ”Resend funktion” defineret med en slettefrist på et (1) år via underdatabehandlerens Connect løsning. • Metadata (som kan indeholde personoplysninger) slettes i henhold til underdatabehandleres standard sletteprocedurer efter halvfems (90) dage. Digital modtagelse af lønsedler fra PostNord Strålfors A/S og/eller databehandleren, midlertidig opbevaring og distribution til modtagere (e-Boks og mit.dk): • Personoplysninger opbevares indtil lønseddel er overført til slutbrugerens digitale postkasse. Når lønsedlen placeres i slutbrugerens digitale postkasse, ophører underdatabehandlerens behandling af personoplysninger på vegne af den dataansvarlige.

	Monitering og tømning af digitale postkasser med applikationen eDistribution: • Personoplysninger opbevares efter distribution til den dataansvarliges digitale postkasser i halvfems (90) dage, hvorefter de slettes. Applikationen Addo Sign: • Personoplysninger opbevares som standard i fyrre (40) dage efter, at dokumentet er blevet underskrevet af alle parter, hvorefter de slettes hos underdatabehandleren. Uanset det foranstående er databehandleren berettiget til, i det omfang det er nødvendigt for at kunne dokumentere levering af Services omfattet af serviceaftalen eller forsvare sig mod retskrav, at gemme en kopi af den dataansvarliges personoplysninger. Personoplysningerne må i så fald udelukkende behandles til det anførte formål.
C.5 Lokalitet for behandling (omfatter alle systemer medmindre de er anført med særlig kommentar)	Behandling af de af Bestemmelserne omfattede personoplysninger kan ikke uden den dataansvarliges forudgående skriftlige godkendelse ske på andre lokaliteter end følgende ud over hos de i Bilag B anførte underdatabehandlere og/eller disses underdatabehandlere: • Databehandlerens til enhver tid værende lokationer i Danmark • Hjemme- og fjernarbejdspladser (databehandlerens medarbejdere og eksternt tilknyttede konsulenter) Applikationerne EPOS Løn, EPOS HR, EPOS Rekruttering og EPOS Management: • Housing af databehandlerens maskinel er placeret på datacenter hos: ○ Global Connect A/S, Hørskætten 5, DK-2630 Taastrup, Hall 11.
C.6 Instruks vedrørende overførsel af personoplysninger til tredjelande	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.6.1 Cloud-leverandør og dataoverførselsmekanisme	Såfremt databehandleren anvender cloud-leverandør i forbindelse med levering af Services (jf. Bilag B) må der udelukkende anvendes datacentre inden for EU/EØS.
C.7 Procedurer for den dataansvarliges revisioner, herunder inspektioner, med behandlingen af personoplysninger, som er overladt til databehandleren (omfatter alle systemer medmindre de er anført med særlig kommentar)	Den dataansvarlige eller en repræsentant for den dataansvarlige har 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 gennemføres, når den dataansvarlige finder det nødvendigt. Dette gælder dog ikke databehandlerens hjemmearbejdspladser. Den dataansvarlige skal give databehandleren et varsel på mindst tredive (30) dage inden inspektion. Såfremt dataansvarlig eller en repræsentant for den dataansvarlige foretager inspektion hos databehandler, skal vedkommende fremvise gyldig billedidentifikation. Vedkommendes identitet og formål skal bekræftes af dataansvarliges kontaktperson, forinden vedkommende får adgang til fortrolige oplysninger. Dataansvarlig eller repræsentant for den dataansvarlige skal overholde alle sikkerhedskrav, som måtte være gældende for lokationen.

	Den dataansvarliges udgifter i forbindelse med en fysisk inspektion afholdes af den dataansvarlige. Databehandleren er forpligtet til mod vederlag at afsætte de ressourcer (hovedsageligt den tid), der er nødvendig(e) for, at den dataansvarlige kan gennemføre sin inspektion. Den dataansvarlige har ret til at gennemføre et årligt skriftlig tilsyn med databehandlerens overholdelse af disse Bestemmelser såfremt der ikke foreligger årlig ISAE 3000 og/eller ISAE 3402 eller tilsvarende erklæring. Metoden for skriftligt tilsyn baseres på den dataansvarliges spørgeskema, som fremsendes til databehandleren. Afhængig af omfang kan skriftligt tilsyn være en betalbar ydelse, hvilket aftales mellem parterne før gennemførelse. Hvis den dataansvarlige kræver information eller assistance omkring sikkerhedsforanstaltninger, dokumentation eller information om, hvordan databehandleren behandler personoplysninger generelt, og en sådan anmodning indeholder information, som går ud over, hvad der er nødvendigt ifølge gældende databeskyttelseslovgivning, må databehandleren kræve betaling for sådanne yderligere services. Lønadministration på applikationen EPOS Løn samt EPOS HR med tilknytning til BPO lønbehandling i applikationen EPOS Løn: • Databehandleren kan årligt for egen regning indhente en revisionserklæring fra uafhængig tredjepart vedrørende databehandlerens overholdelse af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser • Parterne er enige om, at følgende type af revisionserklæring (eller erklæring, der måtte træde i stedet) kan anvendes i overensstemmelse med disse Bestemmelser på følgende områder: o BPO lønbehandling på applikationen EPOS Løn: ISAE 3402 Type II o EPOS HR med tilknytning til BPO lønbehandling på applikationen EPOS Løn: ISAE 3402 Type I • Revisionserklæringerne fremsendes på anmodning uden unødig forsinkelse til den dataansvarlige til orientering • Databehandleren skal, på anmodning og uden unødig forsinkelse fremsende en mitigeringsplan for eventuelle undtagelser som måtte være angivet i revisionserklæringerne • Såfremt den dataansvarlige anfægter rammerne for og/eller metoden i erklæringerne og anmoder om ny erklæring under andre rammer og/eller under anvendelse af anden metode, så gøres dette mod vederlag • Revisionserklæringerne er fortrolige og må ikke deles med uvedkommende Lønadministration på applikationen Azets EPOS Løn: • Databehandleren kan årligt for egen regning indhente en revisionserklæring fra uafhængig tredjepart vedrørende databehandlerens overholdelse af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser • Parterne er enige om, at følgende type af revisionserklæring (eller erklæring, der måtte træde i stedet) kan anvendes i overensstemmelse med disse Bestemmelser på følgende områder: o BPO lønbehandling på applikationen Azets EPOS Løn: ISAE 3402 Type II (opstarts år dog Type I) • Revisionserklæringen fremsendes på anmodning uden unødig forsinkelse til den dataansvarlige til orientering • Databehandleren skal, på anmodning og uden unødig forsinkelse fremsende en mitigeringsplan for eventuelle undtagelser som måtte være angivet i revisionserklæringerne • Såfremt den dataansvarlige anfægter rammerne for og/eller metoden i erklæringerne og anmoder om ny erklæring under andre rammer og/eller under anvendelse af anden metode, så gøres dette mod vederlag • Revisionserklæringerne er fortrolige og må ikke deles med uvedkommende

C.8 Procedurer for revisioner, herunder inspektioner, med behandling af personoplysninger, som er overladt til underdatabehandlere (omfatter alle systemer med-mindre de er anført med særlig kommentar)	Databehandleren eller en repræsentant for databehandleren kan årligt foretage en fysisk inspektion af lokaliteterne, hvorfra underdatabe-handlere foretager behandling af personoplysninger, herunder fysiske lokaliteter og systemer, der benyttes til eller i forbindelse med be-handlingen, med henblik på at fastslå underdatabehandlerens over-holdelse af databeskyttelsesforordningen, databeskyttelsesbestem-melser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser. Ud over det årlige tilsyn, skal databehandleren gennemføre en inspektion med underdatabehandleren, når databehandleren finder det nødvendigt. Baseret på resultaterne af tilsynet, er den dataansvarlige berettiget til for egen regning og risiko at anmode om gennemførelse af yderligere foranstaltninger med henblik på at sikre overholdelse af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser. Den dataansvarlige kan anfægte rammerne for og/eller metoden af inspektionen og kan i sådanne tilfælde for egen regning og risiko anmode om gennemførelsen af en ny inspektion under andre rammer og/eller under anvendelse af anden metode. Parterne er enige om, at følgende type revisionserklæring (eller erklæring, der måtte træde i stedet) kan anvendes i overensstemmelse med disse Bestemmelser på følgende områder med underdatabehandler: Lønadministration på applikationen EPOS Løn: • ISAE 3402 Type II Datacenter (backup) • ISO/ISEC 27001 Lønadministration på applikationen Azets EPOS Løn: • AWS ISO/IEC 27001 • AWS ISO/IEC 27017 • AWS ISO/IEC 27018 • AWS ISO/IEC 9001 • AWS SOC 1 Rapport • AWS SOC 2 Sikkerhed, tilgængelighed & fortrolighed • AWS SOC 2 Fortrolighed Type I • AWS SOC 3 Sikkerhed, tilgængelighed & fortrolighed Lønadministration på applikationen Perspektiv inklusive Mit Perspektiv moduler samt applikationen Perspektiv Tid: • ISAE 3402 Type II Generelle IT-kontroller housing & firewall • ISAE 3402 Type II Generelle IT-kontroller drift/kapacitet/netværksservices • ISAE 3402 Type II Generelle IT-kontroller applikation • ISAE 3000 Type II Databehandlererklæring housing & firewall • ISAE 3000 Type II Datahandlererklæring applikation Løn- og økonomiadministration på applikationen Azets Simplify: • ISAE 3402 Type II Økonomiadministration på applikationen Visma Business: • AWS ISO/IEC 27001 • AWS ISO/IEC 27017 • AWS ISO/IEC 27018 • AWS ISO/IEC 9001 • AWS SOC 1 Rapport • AWS SOC 2 Sikkerhed, tilgængelighed & fortrolighed • AWS SOC 2 Fortrolighed Type I

	• AWS SOC 3 Sikkerhed, tilgængelighed & fortrolighed • ISO 9001 (QMS) Økonomiadministration på applikationen e-conomic: • ISO 27001 (data center) • ISAE 3000 type II • ISAE 3402 type II Ejendomsadministration på applikationen ProBo: • ISAE 3402 Type II eller • ISAE 3000 Type II Applikationen Azets Cozone Portal/Activity/Drive/Employee: • AWS ISO/IEC 27001 • AWS ISO/IEC 27017 • AWS ISO/IEC 27018 • AWS ISO/IEC 9001 • AWS SOC 1 Rapport • AWS SOC 2 Sikkerhed, tilgængelighed & fortrolighed • AWS SOC 2 Fortrolighed Type I • AWS SOC 3 Sikkerhed, tilgængelighed & fortrolighed Applikationerne EPOS Løn, EPOS HR og EPOS Rekruttering: • ISAE 3402 Type II Datacenter • ISO/ISEC 27001-2013 Information Security Management System Applikationen Azets EPOS Løn: • AWS ISO/IEC 27001 • AWS ISO/IEC 27017 • AWS ISO/IEC 27018 • AWS ISO/IEC 9001 • AWS SOC 1 Rapport • AWS SOC 2 Sikkerhed, tilgængelighed & fortrolighed • AWS SOC 2 Fortrolighed Type I • AWS SOC 3 Sikkerhed, tilgængelighed & fortrolighed Applikationen Workcyclus (arbejdspladsvurdering): • Microsoft Azure med SOC 2 Type II erklæring om adgangssikring Applikationen zExpense (rejseafregninger): • ISAE 3000 Type II Applikationen Azets Expense (rejseafregninger): • PCI DSS Leverance af lønsedler til e-Boks og mit.dk: • ISAE 3000 Type II (PostNord Strålfors A/S) • ISO27001 og ISO27701 (e-Boks A/S og Netcompany A/S Applikationen Addo Sign: • ISAE 3402 Type II for datacenter • IAE 3000 Type II for datacenter • ISO 27001 for datacenter Applikationen IMS Case (ESDH-system): • ISAE 3000 Type I Applikationen Freshdesk (supportsystem): • ISO/IEC 27001 • ISO/IEC 27001 • ISO/IEC 27701 • SOC 2 Fortrolighed Type II • SOC 3 Sikkerhed, tilgængelighed & fortrolighed • AWS ISO/IEC 27001 • AWS ISO/IEC 27017 • AWS ISO/IEC 27018

	• AWS ISO/IEC 9001 • AWS SOC 1 Rapport • AWS SOC 2 Sikkerhed, tilgængelighed & fortrolighed • AWS SOC 2 Fortrolighed Type I • AWS SOC 3 Sikkerhed, tilgængelighed & fortrolighed Ovenstående revisionserklæringer fremsendes på anmodning uden vederlag og unødig forsinkelse til den dataansvarlige til orientering. Revisionserklæringer er fortrolige og må ikke deles med uvedkommende.

Bilag D Parternes regulering af andre forhold

Bilag D.1 Supplement til Bestemmelserne

Som supplement til Bestemmelserne har parterne aftalt følgende:

Vedrørende Bestemmelse 11.1 og 11.2:

Databehandleren opbevarer bogførings- og regnskabsmateriale på betryggende vis i fem (5) år fra udgangen af det regnskabsår, som materialet vedrører, med mindre den dataansvarlige skriftligt bekræfter at overtage ansvaret herfor. Hvis den dataansvarlige ønsker adgang til historiske data opbevaret efter serviceaftalens ophør, må databehandleren kræve betaling herfor.

Vedrørende Bestemmelse 13.1:

Ansvar:

Den dataansvarlige er ansvarlig for skader forårsaget af behandling, der er i strid med gældende databeskyttelseslovgivning. Databehandleren er kun ansvarlig for direkte og dokumenterede skader forårsaget af behandling, hvor databehandleren har overtrådt disse Bestemmelser og/eller gældende databeskyttelseslovgivning, der specifikt er rettet mod databehandlerens forpligtelser.

For at undgå tvivl er parterne enige om og anerkender, at hver part skal være ansvarlig for og holdes ansvarlig for at betale alle administrative bøder og skader påført den registrerede, som en part er blevet pålagt at betale i overensstemmelse med gældende databeskyttelseslovgivning.

Vedrørende Bestemmelse 14.3 - Ændringer til databehandleraftale

Databehandleraftalen opdateres løbende på databehandlerens Trust Centre med nye Services, Datatilsynets tilpasninger af standardkontraktbestemmelserne samt relateret opdatering af sammenhænge og versionshistorik. Seneste version af databehandleraftalen vil til enhver tid kunne tilgås i Trustcenter og er gældende medmindre konkrete bestemmelser udtrykkeligt er fraveget i serviceaftale eller i skriftligt tillæg til serviceaftale. Fortsat brug af Services efter opdatering af databehandleraftalen udgør accept heraf.

Vedrørende Bestemmelse 14.5

Da Bestemmelserne indgås som bilag til parternes Aftale, underskrives nuværende dokument ikke særskilt mellem parterne.

Vedrørende Bestemmelse 15.2

Den dataansvarliges kontaktperson(er) er nærmere angivet i Aftalen.

Bilag D.2 Sammenhæng mellem Services og persondata

Der er følgende sammenhæng mellem kontraherede Services og persondata angivet i Bilag A.3:

	Lønadministration på applikationen EPOS Løn	Lønadministration på applikationen Azets EPOS Løn	Lønadministration på applikationen Azets Perspektiv	Lønadministration på applikationen Azets Simplify	Lønadministration på den dataansvarliges lønsystem	Refusionsansøgning	Pensionshåndtering	eKapital indberetning af medarbejderaktieordning	Økonomiadministration på applikationen Azets Simplify	Økonomiadministration på applikationen Visma Business	Økonomiadministration på applikationen e-conomics	Økonomiadministration på den dataansvarliges ERP-system	Ejendomsadministration inklusive formandsassistance mv.	HR-assistance	Monitering og tømning af digitale postkasser	SaaS Applikationen Azets Cozone Employee (dataudveksling)	SaaS Applikationen EPOS Løn	SaaS Applikationen Azets EPOS Løn	SaaS Applikationen EPOS HR, Rekruttering og Management	SaaS Applikationen Workcyclus (arbejdspladsvurdering)	SaaS Applikationen Azets Expense	SaaS Applikationen zExpense
Almindelige personoplysninger herunder bl.a.:																						
Medarbejdernavn, nummer og organisatorisk tilhørsforhold	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
Ansættelses- og fratrædelsesdato	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
Kontaktoplysninger, herunder navn, telefon, e-mail, titel, adresse	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
Navn og kontaktoplysninger på medarbejderens pårørende	+	+	+	+	+	-	-	-	-	-	-	-	+	-	-	-	+	+	-	-	-	-
Fødselsdato, køn og civilstand	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	-	-	-
Lønoplysninger og arbejdstid	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	-	-	-	-
Pensions-, bank- og skatteoplysninger herunder ATP-bidrag og sociale bidrag	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	-	+	+	-	-	-	-
Tids- og fraværsoplysninger herunder: - sygdom, barns sygdom, barsel, militærtjeneste, borgerligt ombud, periodiske ansættelser mv. - ferie og fri (feriefri, omsorgsdage mv.) - oplysninger på §56-aftaler og delvis rask- eller sygemeldinger	+	+	+	+	+	+	-	-	+	+	+	+	+	+	+	+	+	+	-	-	-	-
Løntillæg herunder rejseudlæg, kørselsgodtgørelse mv.	+	+	+	+	+	-	-	-	+	+	+	+	+	+	-	+	+	+	-	-	-	-
Lønfradrag herunder kantine, personalekøb, A-kassebidrag mv.	+	+	+	+	+	-	-	-	+	+	+	+	+	+	-	+	+	+	-	-	-	-
Projektregistreringer	+	+	+	+	+	-	-	-	+	+	+	+	+	+	-	+	+	+	-	-	+	+
Bilregistreringsnummer tilknyttet medarbejder	+	+	+	+	+	-	-	-	+	+	+	+	+	+	+	-	+	+	-	-	+	+
Kørte kilometer inklusive rute (GPS-oplysninger)	+	+	+	+	+	-	-	-	+	+	+	+	+	-	-	-	+	+	-	-	+	+
Elektroniske udlæg/rejseafregninger	-	-	-	+	+	-	-	-	+	+	+	+	+	+	-	-	-	-	-	-	+	+
Enheder og adgange, som er tildelt medarbejder	+	+	+	-	-	-	-	-	+	+	+	+	+	+	-	-	+	+	-	-	-	-
Kurser, som medarbejder har deltaget i samt øvrige kompetencer	+	+	+	-	-	-	-	-	-	-	-	-	-	+	-	-	+	+	+	-	-	-
Kontrakter og andre ansættelsesrelaterede dokumenter (f.eks. notat i forbindelse med prøvetidssamtale, advarsler, opsigelser mv.)	-	-	+	-	-	-	-	-	+	+	+	+	+	+	-	-	-	-	+	-	-	-+
MUS-handlingsplaner	-	-	+	-	-	-	-	-	-	-	-	-	-	+	-	-	-	-	+	-	-	-
Filer uploadet af den dataansvarliges kandidater med persondata, herunder ansøgning, CV, eksamens- og kursusbeviser, eventuelt lønkrav mv.	-	-	-	-	-	-	-	-	-	-	-	-	-	+	-	-	-	-	+	-	-	-
Betalingsoplysninger	-	-	-	-	-	-	-	-	+	+	+	+	+	+	+	-	-	-	-	-	+	+
Billeder samt IP- og cookie-information uploadet af den dataansvarlige	-	-	-	-	-	-	-	-	-	-	-	-	+	-	-	-	-	-	+	-	-	-
Pasoplysninger, sundhedskortoplysninger og lignende legitimation	-	-	-	-	-	-	-	-	-	-	-	-	+	+	-	-	-	-	-	-	-	-
Inkassooplysninger, herunder RKI-registrering	-	-	-	-	-	-	-	-	+	+	+	+	+	-	+	-	-	-	-	-	-	-
Oplysninger, som i øvrigt indgår i dialog med potentielle eller eksisterende andelshavere, lejere, fremlejere, beboere og ejere mv.	-	-	-	-	-	-	-	-	-	-	-	-	+	-	-	-	-	-	-	-	-	-

	Lønadministration på applikationen EPOS Løn	Lønadministration på applikationen Azets EPOS Løn	Lønadministration på applikationen Azets Perspektiv	Lønadministration på applikationen Azets Simplify	Lønadministration på den dataansvarliges lønsystem	Refusionsansøgning	Pensionshåndtering	eKapital indberetning af medarbejderaktieordning	Økonomiadministration på applikationen Azets Simplify	Økonomiadministration på applikationen Visma Business	Økonomiadministration på applikationen e-conomics	Økonomiadministration på den dataansvarliges ERP-system	Ejendomsadministration inklusive formandsassistance mv.	HR-assistance	Monitering og tømning af digitale postkasser	SaaS Applikationen Azets Cozone Employee (dataudveksling)	SaaS Applikationen EPOS Løn	SaaS Applikationen Azets EPOS Løn	SaaS Applikationen EPOS HR, Rekruttering og Management	SaaS Applikationen Workcyclus (arbejdspladsvurdering)	SaaS Applikationen Azets Expense	SaaS Applikationen zExpense
Øvrige medlemsdata i boligforeninger/udlejningsejendomme herunder husstandens størrelse, lejemålshistorik, opnoteringer, forbrugsoplysninger (eksempelvis vand, varme og el) mv.	-	-	-	-	-	-	-	-	-	-	-	-	+	-	+	-	-	-	-	-	-	-
Følsomme personoplysninger herunder bl.a.:																						
Fraværsoplysninger, hvis de indeholder helbredsoplysninger, herunder information om barselsperioder	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	-	-	-
Helbredsoplysninger i form af elektroniske bilag	-	-	-	+	-	-	-	-	+	+	+	+	+	+	+	-	-	-	-	-	+	+
Oplysninger om fysisk og psykisk arbejdsmiljø herunder social kapital	-	-	+	-	-	-	-	-	-	-	-	-	-	+	+	-	-	-	-	+	-	-
Dokumentation af den lovpligtige arbejdsmiljødrøftelse	-	-	+	-	-	-	-	-	-	-	-	-	-	+	-	-	-	-	-	+	-	-
Handlingsplaner på ethvert organisatorisk niveau	-	-	-	-	-	-	-	-	-	-	-	-	-	+	-	-	-	-	-	+	-	-
Oplysninger om private forhold, såsom oplysninger om økonomiske og sociale forhold	+	+	+	+	+	-	-	-	+	+	+	+	+	+	-	+	+	+	+	+	-	-
Fagforeningsmæssigt tilhørsforhold herunder lønfradrag til fagforeningskontingent	+	+	+	+	+	-	-	-	+	+	+	+	+	+	+	-	+	+	+	-	-	-
Strafbare forhold	-	-	-	-	-	-	-	-	-	-	-	-	-	+	+	-	-	-	+	-	-	-
Fortrolige personoplysninger:																						
CPR-nummer	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	-	+	+

Bilag D.3 Sammenhæng mellem Services og kategorier af registrerede

Der er følgende sammenhæng mellem kontraherede Services og kategorier af registrerede angivet i Bilag A.4:

	Lønadministration på applikationen EPOS Løn	Lønadministration på applikationen Azets EPOS Løn	Lønadministration på applikationen Azets Perspektiv	Lønadministration på applikationen Azets Simplify	Lønadministration på den dataansvarliges lønsystem	Refusionsansøgning	Pensionshåndtering	eKapital indberetning af medarbejderaktieordning	Økonomiadministration på applikationen Azets Simplify	Økonomiadministration på applikationen Visma Business	Økonomiadministration på applikationen e-conomics	Økonomiadministration på den dataansvarliges ERP-system	Ejendomsadministration inklusive formandsassistance mv.	HR-assistance	Monitering og tømning af digitale postkasser	SaaS Applikationen Azets Cozone Employee (dataudveksling)	SaaS Applikationen EPOS Løn	SaaS Applikationen Azets EPOS Løn	SaaS Applikationen EPOS HR, Rekruttering og Management	SaaS Applikationen Workcyclus (arbejdspladsvurdering)	SaaS Applikationen Azets Expense	SaaS Applikationen zExpense
Nuværende og tidligere medarbejdere	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
Honorarmodtagere	-	-	+	-	-	-	-	-	-	-	-	-	-	+	+	+	-	-	-	-	-	-
Potentielle medarbejdere	-	-	-	-	-	-	-	-	-	-	-	-	-	+	+	-	-	-	+	-	-	-
Kunder, leverandører og øvrige samarbejds-partnere	-	-	-	-	-	-	-	-	+	+	+	+	+	+	+	-	-	-	-	-	+	+
Medlemmer af boligforening (andelsboligforening, ejerforening, grundejerforening og lignende) samt boligforeningens ansatte, bestyrelsesmedlemmer, lejere/beboere/fremlejere, leverandører og øvrige samarbejdspartnere	-	-	-	+	-	-	-	-	-	-	-	-	+	-	+	-	-	-	-	-	-	-
Ejere af udlejningsejendomme/lejemål samt disses ansatte, bestyrelsesmedlemmer. lejere/beboere/fremlejere, leverandører og øvrige samarbejdspartnere	-	-	-	+	-	-	-	-	-	-	-	-	+	-	+	-	-	-	-	-	-	-

Bilag D.4 Sammenhæng mellem Services og godkendte underdatabehandlere

Der er følgende sammenhæng mellem kontraherede Services og godkendte underdatabehandlere i Bilag B.1:

	Lønadministration på applikationen EPOS Løn	Lønadministration på applikationen Azets EPOS Løn	Lønadministration på applikationen Azets Perspektiv	Lønadministration på applikationen Azets Simplify	Lønadministration på den dataansvarliges lønsystem	Refusionsansøgning	Pensionshåndtering	eKapital indberetning af medarbejderaktieordning	Økonomiadministration på applikationen Azets Simplify	Økonomiadministration på applikationen Visma Business	Økonomiadministration på applikationen e-conomics	Økonomiadministration på den dataansvarliges ERP-system	Ejendomsadministration inklusive formandsassistance mv.	HR-assistance	Monitering og tømning af digitale postkasser	SaaS Applikationen Azets Cozone Employee (dataudveksling)	SaaS Applikationen EPOS Løn	SaaS Applikationen Azets EPOS Løn	SaaS Applikationen EPOS HR, Rekruttering og Management	SaaS Applikationen Workcyclus (arbejdspladsvurdering)	SaaS Applikationen Azets Expense	SaaS Applikationen zExpense
Azets Insight SRL	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	-	-	-	-	-	-	-
Azets Insight AB	-	-	-	-	-	-	-	+	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Azets Insight AS: Azets Invoice/Reporting	-	-	-	-	-	-	-	-	-	+	-	-	-	-	-	-	-	-	-	-	-	-
Azets Insight AS: Visma Business	-	-	-	-	-	-	-	-	-	+	-	-	-	-	-	-	-	-	-	-	-	-
Azets Labs A/S: Azets EPOS Løn	-	+	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	+	-	-	-	-
Azets Labs A/S: Workcyclus APV-produkter	-	-	-	-	-	-	-	-	-	-	-	-	-	+	-	-	-	-	-	+	-	-
Azets Perspektiv A/S	-	-	+	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Azets Software AB	+	+	-	+	+	+	+	+	+	+	+	+	+	-	-	+	-	-	-	-	-	-
e-Boks A/S	+	+	+	-	-	-	-	-	-	-	-	-	-	-	-	-	-	+	+	-	-	-
EG Danmark A/S: EG Bolig	-	-	-	-	-	-	-	-	-	-	-	-	+	-	-	-	-	-	-	-	-	-
Findity AB	+	+	-	-	-	-	-	-	-	+	-	+	-	-	-	-	-	-	-	-	+	-
Freshworks Inc.	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
PostNord Strålfors A/S: Digital forsendelse lønsedler	+	+	+	-	-	-	-	-	-	-	-	-	-	-	-	-	-	+	+	-	-	-
PostNord Strålfors A/S: eDistributionsløsning	-	-	-	+	+	-	-	-	+	+	+	+	+	-	+	-	-	-	-	-	-	-
Twoday Danmark A/S	-	-	-	-	-	-	-	-	+	+	+	+	+	+	-	-	-	-	-	-	-	-
Unik System Design A/S	-	-	-	-	-	-	-	-	-	-	-	-	+	-	-	-	-	-	-	-	-	-
Visma e-conomic A/S	-	-	-	-	-	-	-	-	-	-	+	-	-	-	-	-	-	-	-	-	-	-
Visma IMS A/S	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	-	-	-	-	-	-	-
Wolters Kluwer Danmark A/S	-	-	-	-	-	-	-	-	+	+	+	+	+	-	-	-	-	-	-	-	-	-
Zebon ApS	+	+	-	-	-	-	-	-	-	+	-	+	-	-	-	-	-	-	-	-	-	+
Zenegy Danmark ApS	-	-	-	+	-	-	-	-	+	-	-	-	+	-	-	-	-	-	-	-	-	-

Bilag E Versionshistorik

Version	Ændringer
1.2 Tilpasset af Datatilsynet	Ændringer i Bestemmelse 7.6 *(Bestemmelsen er gjort valgfri og ordlyden er blevet modificeret).*
2.0 Tilpasset af Azets ATB ApS 4. juni 2025	• Ændret placering af baggrund og formål • 7.2: Valg af mulighed 2 • 7.3: Valg af mulighed 2 og min. to (2) uger • 7.6: Fravalg af valgfri Bestemmelse • 9.2: Valg af tilsynsmyndighed (Datatilsynet) • 10.2: Valg af 48 timer, om muligt • 11.1: Valg af mulighed 2 • 11.2: Tilføjelse af den danske Bogføringslov • Bilag A-C tilpasset behandlingen • Bilag B Fravalg af valgfrit afsnit B.2 • Bilag D tilpasset databehandleren specifikt • Bilag E Versionshistorik tilføjet