

Databehandler-aftale

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

Kunden

(herefter "den dataansvarlige")

&

Visma Acubiz A/S

CVR: 20 95 05 87

Gærtorvet 1-5

1799 København

Danmark

(herefter "databehandleren")

Den dataansvarlige og databehandleren herefter hver især benævnt en "part" og tilsammen "parterne") HAR AFTALT, som et tillæg til parternes kontrakt, følgende kontraktbestemmelser (herefter "Bestemmelserne") med henblik på at overholde databeskyttelsesforordningen og sikre beskyttelse af privatlivets fred og fysiske personers grundlæggende rettigheder og frihedsrettigheder.

1. Indholdsfortegnelse

2. Præambel.....	2
3. Den dataansvarliges rettigheder og forpligtelser.....	3
4. Databehandleren handler efter instruks.....	3
5. Fortrolighed.....	4
6. Behandlingssikkerhed.....	5
7. Anvendelse af underdatabehandlere.....	6
8. Overførsel til tredjelande eller internationale organisationer.....	7
9. Bistand til den dataansvarlige.....	7
10. Underretning om brud på persondatasikkerheden.....	8
11. Sletning af oplysninger.....	9
12. Revision, herunder inspektion.....	10
13. Parternes aftale om andre forhold.....	10
14. Ikrafttræden og ophør.....	10
15. Kontaktpersoner hos den dataansvarlige og databehandleren.....	11
Bilag A: Oplysninger om behandlingen.....	12
Bilag B: Underdatabehandlere.....	14
Bilag C: Instruks vedrørende behandling af personoplysninger.....	16
Bilag D: Parternes regulering af andre forhold.....	22

2. Præambel

1. Disse Bestemmelser fastsætter databehandlerens rettigheder og forpligtelser, når denne foretager behandling af personoplysninger på vegne af den dataansvarlige.
2. Disse bestemmelser er udformet med henblik på parternes efterlevelse af artikel 28, stk. 3, i Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (databeskyttelsesforordningen).
3. I forbindelse med leveringen af tjenesten Acubiz behandler databehandleren personoplysninger på vegne af den dataansvarlige i overensstemmelse med disse Bestemmelser.
4. Bestemmelserne supplerer, og skal anses at udgøre et tillæg til, den mellem parterne indgåede kontrakt om den dataansvarliges adgang til Acubiz -tjenesten (pågældende kontrakt inklusive alle tillæg dertil, herefter benævnt "Hovedaftalen"). Bestemmelserne har forrang i forhold til eventuelle konfliktende vilkår i Hovedaftalen, ligesom Bestemmelserne har forrang for tilsvarende bestemmelser i andre aftaler mellem parterne, som vedrører databehandlerens behandling af personoplysninger i forbindelse med levering af Acubiz-tjenesten under Hovedaftalen. For at undgå tvivl bemærkes, at idet Bestemmelserne udgør et tillæg til Hovedaftalen, finder de i Hovedaftalen indeholdte rammevilkår, herunder reguleringen i Hovedaftalen af misligholdelse, erstatning (herunder i særdeleshed de i Hovedaftalen indeholdte fraskrivelse og -begrænsninger af erstatningsansvar), lovvalg og tvistigheder, også anvendelse i relation til Bestemmelserne, herunder i forbindelse med en eventuel misligholdelse af Bestemmelserne.
5. Der hører fire bilag til disse Bestemmelser, og bilagene udgør en integreret del af Bestemmelserne.
6. Bilag A indeholder nærmere oplysninger om behandlingen af personoplysninger, herunder om behandlingens formål og karakter, typen af personoplysninger, kategorierne af registrerede og varighed af behandlingen.
7. Bilag B indeholder den dataansvarliges betingelser for databehandlerens brug af underdatabehandlere og en liste af underdatabehandlere, som den dataansvarlige har godkendt brugen af.
8. Bilag C indeholder den dataansvarliges instruks for så vidt angår databehandlerens behandling af personoplysninger, en beskrivelse af de sikkerhedsforanstaltninger, som databehandleren som minimum skal gennemføre, og hvordan der føres tilsyn med databehandleren og eventuelle underdatabehandlere.
9. Bilag D indeholder bestemmelser vedrørende visse andre forhold i relation til Bestemmelserne.
10. Bestemmelserne med tilhørende bilag såvel som Hovedaftalen og eventuelle øvrige aftaler, som er af betydning for eller supplerer disse aftaler, skal opbevares skriftligt, herunder elektronisk, af begge parter.
11. Disse Bestemmelser frigør ikke databehandleren fra forpligtelser, som databehandleren er pålagt efter databeskyttelsesforordningen eller enhver anden lovgivning. Ligeledes frigør disse Bestemmelser ikke den dataansvarlige fra forpligtelser, som den dataansvarlige er pålagt efter databeskyttelsesforordningen eller enhver anden lovgivning.

3. Den dataansvarliges rettigheder og forpligtelser

1. Den dataansvarlige er ansvarlig for at sikre, at behandlingen af personoplysninger sker i overensstemmelse med databeskyttelsesforordningen (se forordningens artikel 24), databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes¹ nationale ret og disse Bestemmelser.

2. Den dataansvarlige har ret og pligt til at træffe beslutninger om, til hvilke(t) formål og med hvilke hjælpemidler der må ske behandling af personoplysninger.

3. Den dataansvarlige er ansvarlig for, blandt andet, at sikre, at der er et behandlingsgrundlag for behandlingen af personoplysninger, som databehandleren instrueres i at foretage. Den dataansvarlige er derfor over for databehandleren navnlig ansvarlig for, at:

- a. Den dataansvarlige har fornøden hjemmel til at behandle og til at overlade det til databehandleren og dennes underdatabehandlere at foretage de aftalte behandlinger af de personoplysninger, der behandles i forbindelse med levering af Acubiz-tjenesten;
- b. Den dataansvarliges instrukser, sådan som de kommer til udtryk gennem disse Bestemmelser, Hovedaftalen og eventuelle øvrige aftaler, er lovlige; og
- c. Den dataansvarlige ikke overlader andre typer af personoplysninger til databehandlerens behandling, end hvad følger af den dataansvarliges instruks, og at de overladte personoplysninger ikke relaterer sig til andre kategorier af registrerede end de i instruksen angivne.

4. Databehandleren handler efter instruks

1. Databehandleren må kun behandle personoplysninger efter dokumenteret instruks fra den dataansvarlige, medmindre det kræves i henhold til EU-ret eller medlemsstaternes nationale ret, som databehandleren er underlagt. Denne instruks er specificeret i bilag A og C.

2. 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.

- a. Bortset fra som anført i Bestemmelse 4.2.b nedenfor gælder dog, at databehandleren frit kan vælge mellem at acceptere eller afslå enhver efterfølgende instruks, ligesom databehandleren er berettiget til at betinge en eventuel accept af en efterfølgende instruks af, at den dataansvarlige betaler et af databehandleren fastsat vederlag til databehandleren for opfyldelse af instruksen, og/eller at der sker en nærmere af databehandleren fastsat forhøjelse af det almindelige vederlag, den dataansvarlige betaler under Hovedaftalen.
- b. Databehandleren kan dog ikke (medmindre det vil være ulovligt for databehandleren at efterkomme instruksen, se herved Bestemmelse 4.3 nedenfor) nægte at acceptere en efterfølgende instruks omfattende af nr. i (dvs. en instruks om at udlevere til den dataansvarlige kopi af den dataansvarliges personoplysninger) eller ii (dvs. en instruks om at ophøre med at foretage videre behandling af personoplysningerne) umiddelbart nedenfor:
 - i. En instruks om at udlevere til den dataansvarlige en kopi af den dataansvarliges personoplysninger. Databehandleren er imidlertid berettiget til at kræve et særskilt vederlag for at gennemføre en sådan instruks. Vederlaget beregnes på

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

grundlag af det tidsforbrug, databehandleren anvender på at gennemføre instruks, samt databehandlerens almindeligt gældende timesats for sådant arbejde (hvis særlige timesatser for arbejde af den pågældende art fremgår af Hovedaftalen, finder disse timesatser anvendelse), og databehandleren har derudover krav på, at den dataansvarlige dækker eventuelle eksterne omkostninger afholdt af databehandleren til at gennemføre instruks, herunder omkostninger afholdt til eventuelt fornøden bistand fra underdatabehandlere. De nærmere detaljer om udleveringen, herunder vedrørende det format, udleveringen af dataene sker i, aftales nærmere mellem parterne i forbindelse med den dataansvarliges afgivelse af instruks.

- ii. En instruks om at ophøre med at foretage videre behandling af personoplysningerne. I tilfælde af en sådan instruks skal databehandleren, uanset at Hovedaftalen endnu ikke er ophørt i henhold til Hovedaftalens vilkår om opsigelse, agere i henhold til Bestemmelse 11 ("Sletning af oplysninger") nedenfor. For at undgå tvivl bemærkes, at databehandleren fra og med tidspunktet, hvor en sådan instruks efterkommes af databehandleren, frigøres fra sine forpligtelser til at levere sine ydelser i henhold til Hovedaftalen, idet det ikke lader sig gøre at levere Acubiz-tjenesten uden at behandle personoplysningerne. Uanset dette vil den dataansvarlige fortsat i perioden frem til det tidspunkt, hvor Hovedaftalen ville være ophørt, hvis den dataansvarlige på tidspunktet for instruksens afgivelse i stedet havde afgivet et opsigelsesvarsel i henhold til Hovedaftalens opsigelsesvilkår (dvs. med det i henhold til Hovedaftalen krævede opsigelsesvarsel og med respekt af eventuelle vilkår i Hovedaftalen om, hvornår et varsel om opsigelse tidligst kan få virkning), være forpligtet til at betale vederlag til databehandleren i henhold til Hovedaftalens vilkår. Vederlaget for den pågældende periode beregnes til det vederlag, den dataansvarlige skulle have betalt for ydelserne under Hovedaftalen, hvis den dataansvarlige i perioden havde aftaget det minimumsforbrug af ydelserne, som den dataansvarlige i henhold til Hovedaftalen ville have været forpligtet til.

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

5. Fortrolighed

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

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

6. Behandlingssikkerhed

1. Databeskyttelsesforordningens artikel 32 fastslår, at den dataansvarlige og databehandleren, under hensyntagen til det aktuelle tekniske niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder, gennemfører passende tekniske og organisatoriske foranstaltninger for at sikre et beskyttelsesniveau, der passer til disse risici.

Den dataansvarlige skal vurdere risiciene for fysiske personers rettigheder og frihedsrettigheder som behandlingen udgør og gennemføre foranstaltninger for at imødegå disse risici. Afhængig af deres relevans kan det omfatte:

- a. Pseudonymisering og kryptering af personoplysninger
- b. evne til at sikre vedvarende fortrolighed, integritet, tilgængelighed og robusthed af behandlingssystemer og -tjenester
- c. evne til rettidigt at genoprette tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse
- d. En procedure for regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske foranstaltninger til sikring af behandlingssikkerhed.

2. Efter forordningens artikel 32 skal databehandleren – uafhængigt af den dataansvarlige – også vurdere risiciene for fysiske personers rettigheder som behandlingen udgør og gennemføre foranstaltninger for at imødegå disse risici. Med henblik på denne vurdering skal den dataansvarlige stille den nødvendige information til rådighed for databehandleren som gør vedkommende i stand til at identificere og vurdere sådanne risici.

3. Derudover skal databehandleren bistå den dataansvarlige med vedkommendes overholdelse af den dataansvarliges forpligtelse efter forordningens artikel 32, ved bl.a. at stille den nødvendige information til rådighed for den dataansvarlige vedrørende de tekniske og organisatoriske sikkerhedsforanstaltninger, som databehandleren allerede har gennemført i henhold til forordningens artikel 32, og – mod særskilt vederlag til databehandleren – al anden information, der er nødvendig for den dataansvarliges overholdelse af sin forpligtelse efter forordningens artikel 32. Et eventuelt særskilt vederlag til databehandleren i henhold til det foranstående beregnes på grundlag af det tidsforbrug, databehandleren anvender på fremskaffelsen af informationen, samt databehandlerens almindeligt gældende timesatser, og databehandleren har derudover krav på, at den dataansvarlige dækker eventuelle eksterne omkostninger afholdt af databehandleren til fremskaffelse af informationen, herunder omkostninger afholdt til eventuelt fornøden bistand fra underdatabehandlere.

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.

Såfremt den dataansvarlige efter indgåelsen af disse Bestemmelser fremfører, at der bør gennemføres yderligere foranstaltninger end dem, som allerede ved indgåelsen af Bestemmelserne fremgår af bilag C (eller som databehandleren i øvrigt allerede måtte have gennemført), drøftes det mellem parterne, om der kan opnås enighed mellem parterne om en gennemførelse af sådanne yderligere foranstaltninger, herunder om tidsplan og vederlag til databehandleren herfor (samt eventuelt forhøjelse af det vederlag, som den dataansvarlige løbende betaler for ydelserne under Hovedaftalen). Kan parterne ikke nå til enighed herom, skal

den dataansvarlige, hvis denne ikke kan acceptere fortsat at lade personoplysningerne behandle uden gennemførelse af de pågældende foranstaltninger, instruere databehandleren om at ophøre med videre behandling af oplysningerne. I givet fald gælder det i Bestemmelse 4.2.b.ii ovenfor anførte.

7. Anvendelse af underdatabehandlere

1. Databehandleren skal opfylde de betingelser, der er omhandlet i databeskyttelsesforordningens artikel 28, stk. 2, og stk. 4, for at gøre brug af en anden databehandler (en underdatabehandler).

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

3. Databehandleren har den dataansvarliges generelle godkendelse til brug af underdatabehandlere. Databehandleren skal skriftligt underrette den dataansvarlige om eventuelle planlagte ændringer vedrørende tilføjelse eller udskiftning af underdatabehandlere med mindst 30 dages varsel og derved give den dataansvarlige mulighed for at gøre indsigelse mod sådanne ændringer inden brugen af de(n) omhandlede underdatabehandler(e), jf. herom nærmere i bilag B.2. En liste over underdatabehandlere, som den dataansvarlige ved Bestemmelsernes ikrafttræden har godkendt brugen af, fremgår af bilag B.1.

4. Når databehandleren gør brug af en underdatabehandler i forbindelse med udførelse af specifikke behandlingsaktiviteter på vegne af den dataansvarlige, skal databehandleren, gennem en kontrakt eller andet retligt dokument i henhold til EU-retten eller medlemsstaternes nationale ret, pålægge underdatabehandleren de samme databeskyttelsesforpligtelser som dem, der fremgår af disse Bestemmelser, hvorved der navnlig stilles de fornødne garantier for, at underdatabehandleren vil gennemføre de tekniske og organisatoriske foranstaltninger på en sådan måde, at behandlingen overholder kravene i disse Bestemmelser og databeskyttelsesforordningen. Databehandleren er derfor ansvarlig for at kræve, at underdatabehandleren som minimum overholder databehandlerens forpligtelser efter disse Bestemmelser og databeskyttelsesforordningen.

5. Underdatabehandleraftale(r) og eventuelle senere ændringer hertil sendes – efter den dataansvarliges anmodning herom – i kopi til den dataansvarlige, som herigennem har mulighed for at sikre sig, at tilsvarende databeskyttelsesforpligtelser som følger af disse Bestemmelser er pålagt underdatabehandleren. Bestemmelser om kommercielle vilkår, som ikke påvirker det databeskyttelsesretlige indhold af underdatabehandleraftalen, skal ikke sendes til den dataansvarlige.

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

8. Overførsel til tredjelande eller internationale organisationer

1. Enhver overførsel af personoplysninger til tredjelande eller internationale organisationer må kun foretages af databehandleren på baggrund af dokumenteret instruks herom fra den dataansvarlige og skal altid ske i overensstemmelse med databeskyttelsesforordningens kapitel V.

2. Hvis overførsel af personoplysninger til tredjelande eller internationale organisationer, som databehandleren ikke er blevet instrueret i at foretage af den dataansvarlige, kræves i henhold til EU-ret eller medlemsstaternes nationale ret, som databehandleren er underlagt, skal databehandleren underrette den dataansvarlige om dette retlige krav inden behandling, medmindre den pågældende ret forbyder en sådan underretning af hensyn til vigtige samfundsmæssige interesser.

3. Uden dokumenteret instruks fra den dataansvarlige kan databehandleren således ikke inden for rammerne af disse Bestemmelser:

- a. overføre personoplysninger til en dataansvarlig eller databehandler i et tredjeland eller en international organisation
- b. overlade behandling af personoplysninger til en underdatabehandler i et tredjeland
- c. behandle personoplysningerne i et tredjeland

4. Den dataansvarliges instruks vedrørende overførsel af personoplysninger til et tredjeland, herunder det eventuelle overførselsgrundlag i databeskyttelsesforordningens kapitel V, som overførslen er baseret på, skal angives i bilag C.6.

5. Disse Bestemmelser skal ikke forveksles med 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

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

2. I tillæg til databehandlerens forpligtelse til at bistå den dataansvarlige i henhold til Bestemmelse 6.3., bistår databehandleren endvidere, under hensyntagen til behandlingens karakter og de oplysninger, der er tilgængelige for databehandleren, den dataansvarlige med:

- a. den dataansvarliges forpligtelse til uden unødigt forsinkelse og om muligt senest 72 timer, efter at denne er blevet bekendt med det, at anmelde brud på persondatasikkerheden til den kompetente tilsynsmyndighed, Datatilsynet, medmindre at det er usandsynligt, at bruddet på persondatasikkerheden indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder;
- b. den dataansvarliges forpligtelse til uden unødigt forsinkelse at underrette den registrerede om brud på persondatasikkerheden, når bruddet sandsynligvis vil medføre en høj risiko for fysiske personers rettigheder og frihedsrettigheder;
- c. den dataansvarliges forpligtelse til forud for behandlingen at foretage en analyse af de påtænkte behandlingsaktiviteters konsekvenser for beskyttelse af personoplysninger (en konsekvensanalyse);
- d. den dataansvarliges forpligtelse til at høre den kompetente tilsynsmyndighed, Datatilsynet, inden behandling, såfremt en konsekvensanalyse vedrørende databeskyttelse viser, at behandlingen vil føre til høj risiko i mangel af foranstaltninger truffet af den dataansvarlige for at begrænse risikoen.

3. Parterne skal i bilag C angive de fornødne tekniske og organisatoriske foranstaltninger, hvormed databehandleren skal bistå den dataansvarlige samt i hvilket omfang og udstrækning. Det gælder for de forpligtelser, der følger af Bestemmelse 9.1. og 9.2.

4. Databehandleren er berettiget til særskilt vederlag for den bistand, der ydes til opfyldelse af den dataansvarliges anmodninger under denne Bestemmelse 9 ("Bistand til den dataansvarlige"). Vederlaget beregnes på grundlag af det tidsforbrug, databehandleren anvender, samt databehandlerens almindeligt gældende timesats for sådant arbejde (hvis særlige timesatser for arbejde af den pågældende art fremgår af Hovedaftalen, finder disse timesatser anvendelse), og databehandleren har derudover krav på, at den dataansvarlige dækker eventuelle eksterne omkostninger afholdt af databehandleren til opfyldelse af den dataansvarliges anmodninger, herunder omkostninger afholdt til eventuelt fornøden bistand fra underdatabehandlere. For så vidt angår bistand til opfyldelse af den dataansvarliges forpligtelser efter databeskyttelsesforordningens artikel 33-34 har databehandleren dog ikke krav på vederlag for opfyldelse af de forpligtelser, databehandleren har efter Bestemmelse 10 ("Underretning om brud på persondatasikkerheden") nedenfor.

10. Underretning om brud på persondatasikkerheden

1. Databehandleren underretter uden unødigt forsinkelse den dataansvarlige efter at være blevet opmærksom på, at der er sket et brud på persondatasikkerheden hos databehandleren eller en anvendt underdatabehandler i forhold til de personoplysninger, den dataansvarlige har overladt til databehandleren at behandle. Underretning kan fremsendes på e-mail til den af den dataansvarlige angivne kontaktadresse. Underretning kan gives via en standardformular.

2. 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.

3. Databehandlerens underretning til den dataansvarlige skal om muligt ske så betids, at de samlede oplysninger tilvejebringes sådan, at den dataansvarlige kan foretage den komplette anmeldelse til tilsynsmyndigheden inden for de tidskrav til anmeldelse af brud på persondatasikkerheden, som er indeholdt i databeskyttelsesforordningens artikel 33.

4. Hvis det ikke er muligt for databehandleren at give oplysningerne samlet, kan oplysningerne meddeles trinvist uden unødigt yderligere forsinkelse. I forlængelse af den indledende underretning til den dataansvarlige skal databehandleren derfor om nødvendigt løbende ajourføre og komplettere informationer til den dataansvarlige, sådan at denne om nødvendigt kan opdatere en anmeldelse af brud på persondatasikkerheden ved tilsynsmyndigheden, jf. databeskyttelsesforordningens artikel 33, stk. 4.

5. Databehandlerens meddelelse om brud på persondatasikkerheden udgør ikke en anerkendelse af skyld eller ansvar i forhold til et indtruffet brud på persondatasikkerheden.

6. 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 af oplysninger

1. Ved ophør af Hovedaftalen er databehandleren forpligtet til at slette alle personoplysninger, der er blevet behandlet på vegne af den dataansvarlige og bekræfte over for den dataansvarlige, at oplysningerne er slettet.

2. Databehandleren kan dog fortsat opbevare den dataansvarliges personoplysninger efter ophør af Hovedaftalen, hvis databehandleren er underlagt en retlig forpligtelse efter EU-retten eller medlemsstaternes nationale ret, som foreskriver, at databehandleren skal foretage sådan opbevaring af personoplysningerne. Databehandleren forpligter sig i sådanne situationer til alene at behandle personoplysningerne til de(t) formål, i den periode og under de betingelser, som sådanne regler foreskriver.

3. Såfremt den dataansvarlige efter indgåelsen af Bestemmelserne giver skriftlig besked til databehandleren om, at den dataansvarlige ønsker, at databehandleren ved Hovedaftalens ophør i stedet for blot at slette personoplysningerne skal tilbagelevere personoplysningerne til den dataansvarlige, skal databehandleren respektere et sådant ønske om ændring af Bestemmelserne (ændringen skal være dokumenteret og opbevares skriftligt, herunder elektronisk, af begge parter i tilknytning til Bestemmelserne), og databehandleren skal da ved Hovedaftalens ophør naturligvis først slette sine kopier af personoplysningerne i henhold til Bestemmelse 11.1, når tilbageleveringen af personoplysninger til den dataansvarlige er blevet gennemført. I relation til tilbageleveringen finder Bestemmelse 4.2.b.i, herunder vilkårene deri om særskilt vederlag til databehandleren, anvendelse.

12. Revision, herunder inspektion

1. Databehandleren stiller på den dataansvarliges anmodning alle oplysninger, der er nødvendige for at påvise overholdelsen af databeskyttelsesforordningens artikel 28 og disse Bestemmelser, til rådighed for den dataansvarlige og giver mulighed for og bidrager til revisioner, herunder inspektioner, der foretages af den dataansvarlige eller en anden revisor, som er bemyndiget af den dataansvarlige.
2. Procedurene for den dataansvarliges revisioner, herunder inspektioner, med databehandleren og underdatabehandlere er nærmere angivet i Bilag C.7. og C.8.
3. Databehandleren er forpligtet til at give tilsynsmyndigheder, som efter gældende 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

1. Parterne kan aftale andre bestemmelser i relation til tjenesten Acubiz vedrørende behandling af personoplysninger, så længe disse andre bestemmelser ikke direkte eller indirekte strider imod databeskyttelsesforordningen eller forringer den registreredes grundlæggende rettigheder og frihedsrettigheder, som følger af databeskyttelsesforordningen.

14. Ikrafttræden og ophør

1. Bestemmelserne træder i kraft på datoen for begge parters underskrift heraf. Hvis parterne tidligere har indgået en databehandleraftale mellem sig om den af Bestemmelserne omhandlede behandling af personoplysninger, skal Bestemmelserne fra og med datoen for begge parters underskrift af Bestemmelserne gælde i stedet for en sådan tidligere indgået databehandleraftale.
2. Begge parter kan kræve Bestemmelserne (inklusive bilagene hertil) genforhandlet, hvis lovændringer eller u hensigtsmæssigheder i Bestemmelserne giver anledning hertil. Hvis der ved en ændring af Bestemmelserne (inklusive bilagene) sker ændring af databehandlerens forpligtelser på en måde, så det bliver mere omkostningsfuldt for databehandleren at efterleve Bestemmelserne, er databehandleren i forbindelse med tilpasningen af Bestemmelserne berettiget til at kræve, at databehandlerens vederlæggelse for ydelserne under Hovedaftalen forhøjes, og/eller at der indsættes yderligere vilkår om særskilt vederlæggelse af databehandleren i Bestemmelserne, så databehandlerens forøgede omkostninger dækkes.
3. Bestemmelserne er gældende, så længe Hovedaftalen varer og derefter indtil databehandleren har slettet den dataansvarliges personoplysninger i overensstemmelse med reguleringen i Bestemmelserne. I denne periode kan Bestemmelserne ikke opsiges, medmindre andre bestemmelser, der regulerer levering af tjenesten vedrørende behandling af personoplysninger, aftales mellem parterne.
4. Databehandleraftalen er underskrevet af begge parter. En elektronisk underskrevet kopi af aftalen betragtes som et originalt eksemplar og har samme juridiske gyldighed som en fysisk underskrift.

15. Kontaktpersoner hos den dataansvarlige og databehandleren

1. Parterne kan kontakte hinanden via nedenstående kontaktpersoner.
2. Parterne er forpligtet til løbende at orientere hinanden om ændringer vedrørende kontaktpersoner.

Kontaktoplysninger for dataansvarlige:

Navn	Stilling	Telefonnummer	Email

Kontaktoplysninger for databehandler:

Navn	Stilling	Telefonnummer	Email
Rebecca Løssl	Data Protection Manager	+45 2340 2613	dpa.acubiz@visma.com
Henrik Malling	Managing Director	+45 4030 3797	dpa.acubiz@visma.com

Bilag A: Oplysninger om behandlingen

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

Databehandlerens behandling af den dataansvarliges personoplysninger sker med det aftalte formål at levere Acubiz-tjenesten og eventuelle dertil relaterede services som nærmere beskrevet i Hovedaftalen. Behandlingen sker primært i forbindelse med den dataansvarliges (inkl. den dataansvarliges oprettede Acubiz-brugere) brug af Acubiz-tjenesten.

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

Databehandlerens behandling af personoplysninger for den dataansvarlige har den karakter, som følger af Hovedaftalen, og kan herunder især omfatte følgende aktiviteter:

- Import og upload af den dataansvarliges kreditkorttransaktioner til Acubiz (NB: Acubiz står kun for transport af transaktionerne) samt opbevaring af dataene i Acubiz løsningen.
- Stille Acubiz med deri opbevarede data til rådighed for den dataansvarliges brugere.
- Tilgang til data i forbindelse med fejlrettelser i Acubiz løsningen.
- Opbevaring af data til arkivformål.

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

Behandlingen omfatter udelukkende almindelige personoplysninger (jf. databeskyttelsesforordningens artikel 6), herunder nærmere bestemt (afhængig af den dataansvarliges konkrete opsætning og brug af Acubiz løsningen): Navn, initialer, e-mailadresse, telefonnummer, adresse, medarbejdernr., company-ID, konfigurationsoplysninger (typisk sprogvælger, brugernavn, password/pass code, approval limit, etc.), betalingskortoplysninger, bankoplysninger og transaktionsdata (typisk informationer om beløb, valuta, dato, land, typen af omkostning, udsnit af kreditkortnummer samt kortindehaver-identifikator, kontoart, dimensioner og eventuelt kommentarer, samt foto af betalingsbilag).

Såfremt den dataansvarlige under Hovedaftalen har tilkøbt servicen Mileage, omfatter behandlingen også almindelige personoplysninger om kørsel, herunder (afhængig af den dataansvarliges konkrete opsætning og brug af Acubiz løsningen) formål med kørslen, bilens nummerplade (registreringsnummer), distance, start- og slutadresse og, hvis der er valgt location service, GPS-trackingdata.

Såfremt den dataansvarlige under Hovedaftalen har tilkøbt servicen TIME, omfatter behandlingen også almindelige personoplysninger om tidsregistreringer. Disse oplysningers nærmere sammensætning beror på informationskrav angivet af den dataansvarlige, men kan (afhængig af den dataansvarliges konkrete opsætning og brug af Acubiz løsningen) f.eks. være timeforbrug angivet på konto, art, dimensioner og dato.

Acubiz løsningen er kun beregnet på behandling af almindelige personoplysninger

Den dataansvarlige (herunder ved de af den dataansvarlige oprettede brugere af

Acubiz-tjenesten) må IKKE indlæse eller lade indlæse i Acubiz løsningen personoplysninger, der hører til nogen af følgende kategorier, idet løsningen ikke er beregnet på behandling af sådanne personoplysninger:

- Følsomme personoplysninger (oplysninger omfattet af databeskyttelsesforordningens artikel 9), dvs. oplysninger om race eller etnisk oprindelse, politisk, religiøs eller filosofisk overbevisning, fagforeningsmæssigt tilhørsforhold, genetiske data, biometriske data med det formål entydigt at identificere en fysisk person, helbredsoplysninger eller oplysninger om en fysisk persons seksuelle forhold eller seksuelle orientering
- Personoplysninger om straffedomme og lovovertrædelser (oplysninger omfattet af databeskyttelsesforordningens artikel 10)
- Oplysninger om CPR-numre (eller om andre nationale identifikationsnumre eller andre almene midler til identifikation, for hvilke specifikke betingelser for behandling måtte være fastsat i medlemsstaternes nationale ret, jf. databeskyttelsesforordningens artikel 87)

Databehandleren fraskriver sig ethvert ansvar for behandling af personoplysninger i de nævnte kategorier, som måtte ske som konsekvens af den dataansvarliges manglende overholdelse af det ovenfor anførte.

A.4. Behandlingen omfatter følgende kategorier af registrerede

Der behandles oplysninger om den dataansvarliges oprettede Acubiz brugere, som f.eks. kan være den dataansvarliges ansatte, bestyrelsesmedlemmer, non-staff (frivillige) og undervisere.

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

Se Bestemmelse 14.1 og 14.3.

Bilag B: Underdatabehandlere

B.1. Godkendte underdatabehandlere

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

Navn	Overførselsgrundlag	Beskrivelse af behandling	Lokation for behandling
Visma Software International AS CVR-nr. NO 980858073 Karenslyst Allé 56, 0277 Oslo, Norge	Ikke relevant inden for EU/EØS	Hosting Center Visma Connect: Login to Customer Cloud SmartScan: Automatisk aflæsning	Hosting Center: Norge Visma Connect: Norge SmartScan: Belgien/Holland
Cloudflare Inc. CVR-nr. 4710875 101 Townsend Street San Francisco CA 94107, USA	Ikke relevant inden for EU/EØS SCC, EU-U.S. Data Privacy Framework (DPF)	Web application firewall i cloud	Kundetrafik bliver scannet globalt i det data center , som ligger tættest på slutbrugeren.
Scaleway SAS CVR-nr. FR 35 33115904 8 Rue de la Ville l'Evêque, 75008 Paris, Frankrig	Ikke relevant inden for EU/EØS	Hosting af krypterede filer	Frankrig/Holland
Zendesk Inc. CVR-nr. 26-4411091 989 Market Street, San Francisco, CA 94103, USA	Ikke relevant inden for EU/EØS	Kundesupport ticket system	Irland

B.2. Planlagte ændringer vedrørende tilføjelse eller udskiftning af underdatabehandlere

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 30 dages varsel og derved give den dataansvarlige mulighed for at gøre indsigelse mod sådanne ændringer inden brugen af de(n) omhandlede underdatabehandler(e). Hvis databehandleren ikke umiddelbart eller uden at skulle afholde uforholdsmæssigt store omkostninger kan opfylde sine leveranceforpligtelser efter Hovedaftalen i en sådan varslingsperiode, er databehandleren ansvarsfri herfor.

Såfremt den dataansvarlige gør indsigelse, jf. ovenfor, kan den dataansvarlige, uanset hvad der normalt gælder af opsigelsesvarsler i henhold til Hovedaftalen, bringe Hovedaftalen til ophør ved at opsiges denne til at ophøre umiddelbart før det af databehandleren varslede tidspunkt for påbegyndelsen af brugen af den nye underdatabehandler. Hvis den dataansvarlige ønsker at benytte sig af denne opsigelsesadgang, skal skriftlig meddelelse herom gives til databehandleren senest 2 uger efter databehandlerens fremsendelse af varsel om den planlagte ændring. I tilfælde af, at den dataansvarlige benytter sig af den foranstående opsigelsesret, skal den dataansvarlige uanset opsigelsen være forpligtet til i perioden fra ophøret af Hovedaftalen og frem til det tidligste tidspunkt, på hvilket Hovedaftalen ville være ophørt, hvis den dataansvarliges opsigelsesvarsel i stedet havde været afgivet i medfør af de i selve Hovedaftalen (dvs. Hovedaftalen eksklusiv nærværende databehandleraftale) indeholdte bestemmelser om opsigelse (dvs. med det i henhold til Hovedaftalen krævede opsigelsesvarsel og med respekt af eventuelle vilkår i Hovedaftalen om, hvornår et varsel om opsigelse tidligst kan få virkning), at fortsætte med at betale vederlag til databehandleren i henhold til Hovedaftalens vilkår. Vederlaget for den pågældende periode beregnes til det vederlag, den dataansvarlige skulle have betalt for ydelserne under Hovedaftalen, baseret på den dataansvarliges faktiske forbrug de foregående tre måneder, forholdsmæssigt fordelt pr måned i hele opsigelsesperioden, dog mindst det aftalte aconto/minimumsforbrug, som hvis den dataansvarlige i perioden havde aftaget af ydelserne, som den dataansvarlige i henhold til Hovedaftalen ville have været forpligtet til.

Ud over at bringe Hovedaftalen til ophør ved opsigelse i henhold til det foranstående har den dataansvarlige ikke nogen beføjelser i anledning af sin indsigelse. Opsiger den dataansvarlige ikke Hovedaftalen i henhold til det foranstående, må den dataansvarlige således acceptere, at databehandleren på det varslede tidspunkt påbegynder brug af den nye underdatabehandler i relation til behandlingen af den dataansvarliges personoplysninger.

Bilag C: Instruks vedrørende behandling af personoplysninger

C.1. Behandlingens genstand/instruks

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

C.2. Behandlingssikkerhed

Sikkerhedsniveauet skal afspejle følgende: Bl.a. henset til, (i) at behandlingen udelukkende omfatter personoplysninger i kategorien almindelige personoplysninger (jf. databeskyttelsesforordningens artikel 6), (ii) at der endvidere er tale om ret begrænsede typer af oplysninger, og (iii) at oplysningerne – henset til formålet med Acubiz løsningen – angår transaktioner foretaget af den dataansvarliges brugere i erhvervsmæssigt regi, er risikoen for fysiske personers rettigheder og frihedsrettigheder lav. Databehandlerens sikkerhedsniveau skal afspejle denne risikovurdering (og den dataansvarlige er således indforstået med, at databehandleren ikke behøver at etablere et højere sikkerhedsniveau end et, som afspejler denne risikovurdering).

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

Databehandlerens informationssikkerhed er baseret på ISO 27001 rammeværket.

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

- Informationssikkerhedspolitikker
 - Overordnede retningslinjer og krav til informationssikkerhed
- Organisering af informationssikkerhed herunder
 - Udpeget Data Protection Manager
 - Implementeret Information Security Board
- Medarbejdersikkerhed herunder
 - Baggrundstjek
 - Gennemgang af straffeattest
 - Fortrolighedserklæringer
 - Awarenessstræning
- Styring af aktiver herunder
 - Register over aktiver samt klassificering af disse
- Adgangsstyring herunder
 - Begrænsning af adgang til data ud fra arbejdsbetinget behov således at forpligtelser i henhold til Hovedaftalen kan opfyldes.
- Kryptografi herunder
 - Kryptering eller anonymisering af data
- Fysisk sikring og miljøsikring herunder
 - Beskyttelse af fysiske adgangsveje til databehandlerens lokationer
- Driftssikkerhed herunder
 - Implementerede processer til håndtering af udviklings- og ændringsstyring

- Backup
- Logning
- Overvågning af og beskyttelse mod tekniske sårbarheder
- Kommunikationssikkerhed herunder
 - Beskyttelse og opdeling af netværk
 - Etablerede sikre kommunikationsformer
- Anskaffelse, udvikling og vedligeholdelse af systemer herunder
 - Proces for sikker udvikling
- Leverandørforhold herunder
 - Proces til sikring af at leverandører lever op til samme forpligtelser som fastsat i denne databehandlersaftale
 - Proces for løbende opfølgning
- Styring af informationssikkerhedsbrud og brud på persondatasikkerheden herunder
 - "Incident response" proces
 - Proces for underretning af den dataansvarlige
- Informationsikkerhedsaspekter ved nød-, beredskabs- og reetableringsstyring herunder
 - Implementeret Business Continuity Management process
- Overensstemmelse (compliance) herunder
 - Proces for identifikation af lovgivningsmæssige eller kontraktuelle krav

Hvis den dataansvarlige anmoder om oplysninger om sikkerhedsforanstaltninger, dokumentation eller andre former for oplysninger omkring hvordan databehandleren behandler Personoplysninger, og sådanne overskrider de standardoplysninger, beskrevet i bilag C.7, som databehandleren har stillet til rådighed for opfyldelse af gældende lovgivning om behandling af personoplysninger som databehandler, og dette medfører ekstra arbejde for databehandleren, er databehandleren berettiget til at opkræve et særskilt vederlag. Vederlaget opgøres på baggrund af databehandlerens forbrugte arbejdstid og databehandlerens gældende timesatser

C.3 Bistand til den dataansvarlige

Databehandleren skal så vidt muligt – inden for det nedenstående omfang og udstrækning – bistå den dataansvarlige i overensstemmelse med Bestemmelse 9.1 og 9.2 ved at bistå den dataansvarlige med følgende oplysninger i tilfælde af brud på persondatasikkerheden:

- Beskrivelse af hændelsesforløb
- Identifikation af de registrerede, som er berørt af hændelsen
- Typer af personoplysninger, som er omfattet af hændelsen.

C.4 Opbevaringsperiode/sletterutine

Mens Hovedaftalen er i kraft, gælder, at personoplysninger som udgangspunkt, jf. nærmere nedenfor, opbevares i mindst 5 + 1 år:

Opbevaring:

- Indeværende kalenderårs data
- Mindst de 5 forudgående kalenderårs data
- Ovenstående er en del af det almindelige abonnement under Hovedaftalen

Sletning:

- Alle data, der er ældre end de ovennævnte 5+1 år, er databehandleren berettiget – men ikke forpligtet – til at slette.
- Dette gælder dog ikke, hvis der i Hovedaftalen (f.eks. via et tillæg til denne) er truffet skriftlig aftale om den dataansvarliges tilkøb af en længerevarende arkivopbevaring, i hvilket fald databehandleren først er berettiget til at slette i henhold til den dermed aftalte længere arkivopbevaringsperiode.
- Sletning kan i øvrigt ske i henhold til konkret skriftlig instruks, som den dataansvarlige måtte afgive til databehandleren. En sådan instruks – med specifik angivelse af de data, der ønskes slettet – kan afgives ved brug af en blanket, som kan rekvireres hos databehandleren. For gennemførelse af sletning i henhold til konkret instruks er databehandleren berettiget til at opkræve et særskilt vederlag, som beregnes på grundlag af det tidsforbrug, databehandleren anvender på sletningen, samt databehandlerens almindeligt gældende timesatser.

Tilpasset opbevaring:

- For at imødekomme specifikke behov, har den dataansvarlige mulighed for at tilpasse opbevaringsperioden via løsningens indstillinger eller ved at anmode databehandleren herom. En sådan tilpasning kan medføre en opbevaringsperiode, der afviger fra standarden. Den dataansvarliges valg af en tilpasset opbevaringsperiode erstatter enhver tidligere aftale vedrørende opbevaringsperioden.

Ved ophør af Hovedaftalen skal databehandleren slette personoplysningerne i overensstemmelse med Bestemmelse 11.1. For god ordens skyld bemærkes, at såfremt det i Hovedaftalen (typisk i form af et tillæg til Hovedaftalen om tilkøb af en særlig arkivløsning) er aftalt, at dataene i en periode efter ophør i øvrigt af Hovedaftalens ydelser fortsat skal opbevares af databehandleren i en arkivløsning, vil sletning fra en sådan særlig arkivløsning i henhold til Bestemmelse 11.1 naturligvis først ske på tidspunktet for arkivløsningens ophør (idet Hovedaftalen jo i en sådan situation, uanset at den i øvrigt måtte være ophørt, netop for så vidt angår arkivløsningen forbliver i kraft frem til den særlige arkivløsnings ophør).

C.5 Lokaltet for behandling

Databehandlerens behandling af de af Bestemmelserne omfattede personoplysninger sker fra databehandlerens egen side på en eller flere adresser beliggende inden for EU/EØS, samt fra underdatabehandleres side inden for de lokationer (områder), som fremgår af bilag B.1, eller som – hvor der er tale om en ny underdatabehandler, som udpeges i henhold til bilag B.2 – måtte blive oplyst af databehandleren i forbindelse med varslet om, at databehandleren vil begynde at benytte den nye underdatabehandler. Såfremt den dataansvarlige ønsker mere præcise oplysninger om de på et givet tidspunkt gældende adresser for behandlingen af personoplysninger, henvises den dataansvarlige til at kontakte databehandleren.

C.6 Instruks vedrørende overførsel af personoplysninger til tredjelande

Den dataansvarlige giver instruks til, at personoplysninger behandles af de underdatabehandlere og på de lokationer, som fremgår af bilag B.1.

Hvis den dataansvarlige ikke i disse Bestemmelser eller efterfølgende giver en dokumenteret instruks vedrørende overførsel af personoplysninger til et tredjeland, er databehandleren ikke berettiget til inden for rammerne af disse Bestemmelser at foretage sådanne overførsler.

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

Revisionserklæring

Databehandleren får årligt udarbejdet en ISAE 3402 II- og ISAE 3000 I-revisionserklæring (eller anden tilsvarende revisionserklæring) fra en tredjepart vedrørende forhold, der angår overholdelse af databeskyttelsesforordningen. Den dataansvarlige kan hente en kopi af erklæringerne vederlagsfrit på databehandlerens hjemmeside her:

<https://acubiz.com/da/legal/revisionserklaeringer/>

Den dataansvarlige er indforstået med, at eventuelle revisionserklæringer i henhold til det foranstående vil være erklæringer af generel karakter, der således ikke omhandler kundespecifikke forhold (og således ikke omhandler forhold, som måtte være specifikke for netop den behandling af personoplysninger, som databehandleren foretager for den dataansvarlige).

Tilsyn

Den dataansvarlige har, når denne finder det nødvendigt, ret til at gennemføre et tilsyn med databehandlerens behandling af personoplysninger på den dataansvarliges vegne.

Den dataansvarlige kan vælge at gennemføre et tilsyn enten som et skriftligt tilsyn eller ved fysisk inspektion.

Tilsynet kan udføres af den dataansvarlige selv eller i samarbejde med tredjepart. Databehandleren kan fremsætte indsigelse mod en af den dataansvarlige udpeget tredjepart til gennemførelse af tilsynet, hvis den udpegede person/organisation efter databehandlerens rimelige vurdering ikke er egnet eller kvalificeret til at kunne gennemføre inspektionen, herunder at vedkommende (i) ikke er uafhængig, (ii) er, eller er tilknyttet eller har relationer til, en direkte konkurrent til databehandleren eller (iii) af anden grund oplagt er uegnet til varetagelse af opgaven. Fremsætter databehandleren en sådan indsigelse mod den udpegede person/organisation, må den dataansvarlige udpege en anden til gennemførelse af tilsynet.

Et tilsyn skal tage udgangspunkt i de sikkerhedsforanstaltninger, der er aftalt mellem parterne (se bilag C.2), databehandlerens overholdelse af instruksen, herunder brug af underdatabehandlere, samt opfyldelse af eventuelle krav til bistand til den dataansvarlige.

Ved fysisk inspektion skal den dataansvarlige give mindst ti (10) dages forudgående varsel. Den dataansvarlige og/eller den repræsentant for den dataansvarlige, som deltager i inspektionen, skal endvidere underlægge sig databehandlerens almindelige sikkerhedsforanstaltninger og tiltræde en fortrolighedsklausul på sædvanlige vilkår direkte over for databehandleren. Den dataansvarlige eller dennes repræsentant kan herefter få adgang til at foretage fysiske inspektioner med lokaliteterne, hvorfra databehandleren foretager behandling af personoplysninger, herunder fysiske lokaliteter og systemer, der benyttes til eller i forbindelse med behandlingen.

Omkostninger og vederlag

Den dataansvarliges eventuelle udgifter i forbindelse med gennemførelse af tilsyn/revision, herunder eventuel fysisk inspektion, afholdes af den dataansvarlige selv. Databehandleren har ret til at opkræve et vederlag i forbindelse med den dataansvarliges udøvelse af tilsyn/revision.

Vederlaget opgøres på baggrund af databehandlerens forbrugte arbejdstid og databehandlerens gældende timesatser med tillæg af eventuelt afholdte positive omkostninger, herunder også omkostninger afholdt af databehandleren for eventuel bistand fra underdatabehandlere.

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

Databehandleren skal for egen regning udføre passende kontrol med underdatabehandleres overholdelse af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser, i forhold til de behandlingsaktiviteter, som sådanne underdatabehandlere udfører for databehandleren.

Kontrol (revision/tilsyn) med databehandlerens anvendte underdatabehandlere sker dermed gennem databehandleren, som selv fastsætter den nærmere procedure (herunder om kontrollen eventuelt gennemføres via indhentelse af revisionserklæringer) og frekvens. På anmodning fra den dataansvarlige skal databehandleren fremsende dokumentation for kontrollen (herunder kopi af eventuelle relevante revisionserklæringer, databehandleren måtte have modtaget via underdatabehandleren).

Uanset det ovenfor anførte gælder, at den dataansvarlige – hvis det er begrundet og rimeligvis nødvendigt – kan vælge at initiere og/eller deltage i et skriftligt tilsyn eller på en fysisk inspektion hos underdatabehandleren, når underdatabehandleren tillader dette. Dette kan blive aktuelt, hvis den dataansvarlige rimeligvis vurderer, at databehandlerens kontrolførelse med underdatabehandleren ikke har givet den dataansvarlige tilstrækkelig sikkerhed for, at behandlingen hos underdatabehandleren sker i overensstemmelse med databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser. Tilsyn med en underdatabehandler skal ske under overholdelse af underdatabehandlerens opsatte vilkår for tilsyn og inspektion. Ved den dataansvarliges initiering og/eller deltagelse i tilsyn eller inspektion i forhold til en underdatabehandler finder de i bilag C.7 ovenfor anførte regler angående tilsyn/inspektion i øvrigt tilsvarende anvendelse.

Omkostninger og vederlag

Den dataansvarliges eventuelle udgifter i forbindelse med gennemførelse af et tilsyn/revision, herunder eventuelt fysisk inspektion, af en underdatabehandler, som er initieret af den dataansvarlige og/eller som den dataansvarlige har deltaget i, afholdes af den dataansvarlige selv. Databehandleren er berettiget til vederlag i forbindelse med udøvelse af et sådant tilsyn/revision, herunder eventuelt fysisk inspektion, som er initieret af den dataansvarlige og/eller som den dataansvarlige har deltaget i. Vederlaget opgøres på baggrund af den forbrugte arbejdstid og databehandlerens og underdatabehandleren gældende timesatser med tillæg af eventuelt afholdte positive omkostninger, herunder også omkostninger afholdt af databehandleren for underdatabehandleres bistand.

Bilag D: Parternes regulering af andre forhold