Databehandleraftale

Dækker GDPR-databehandling, NIS2-leverandørkædesikkerhed og DORA-tredjepartsforpligtelser

1. maj 2026

Indholdsfortegnelse

DBA version 2026.05. Gældende fra 1. maj 2026. Denne version erstatter alle tidligere versioner.

Denne DBA findes også på engelsk på /en/dpa. Ved fortolkningskonflikt mellem den danske og den engelske version har den danske version forrang, i overensstemmelse med dansk lovvalg i Punkt 17.1.

Overensstemmelse med Datatilsynets standarddatabehandleraftale

Denne DBA er udformet til at opfylde de materielle krav i Datatilsynets standarddatabehandleraftale (marts 2024-version, tilgængelig på www.datatilsynet.dk). Følgende afvigelser fra standardskabelonen er bevidste og dokumenterede:

Punkt	Standardskabelon	Denne DBA	Begrundelse
Varsel ved ny underdatabehandler	30 dage	14 dage, kan forlænges til 30 dage på skriftlig anmodning (Punkt 7.5(b))	Hurtigere operationelt standard; 30-dages beskyttelse tilgængelig på anmodning
Insolvens- eller begunstigelsesklausul	Valgfri (marts 2024)	Inkluderet i Punkt 7.4(c)-(d) som en per-engagement-efterfølgermekanisme	Giver tilsvarende eller stærkere beskyttelse via en udpeget Stedfortræder
Bilagsstruktur	Datatilsynets skabelonstruktur	Tilsvarende indhold i Bilag 1-5; udvidet til at dække DORA (Bilag 4) og britiske overførsler (Bilag 5)	Omfangsudvidelser; kerneforpligtelser er identiske

Enhver offentlig dataansvarlig, der kræver streng skabelonoverensstemmelse, kan anmode om en version af denne DBA, hvor 14-dages varslet erstattes af 30 dage; jeg leverer en sådan på skriftlig anmodning inden for 5 arbejdsdage.

Hvem gør hvad under denne DBA

Du er den Dataansvarlige. Du bestemmer, hvorfor personoplysninger indsamles, og hvad de bruges til. Du er ansvarlig over for Datatilsynet og over for de personer, hvis data behandles. Denne DBA ændrer ikke på det.

Jeg er Databehandleren. Jeg behandler personoplysninger kun, fordi du instruerer mig til det, som led i levering af de ydelser, der er beskrevet i Hovedaftalen. Jeg må ikke anvende dine data til egne formål. Jeg er ansvarlig over for dig for, hvordan jeg håndterer dem.

Denne sondring er vigtig: hvis noget går galt med personoplysninger, jeg håndterer på dine vegne, skal jeg fortælle dig det. Du beslutter herefter, om og hvordan du informerer Datatilsynet og de berørte personer. Jeg hjælper dig med det.

Resumé (for læseren der kun læser denne side)

Denne databehandleraftale ("DBA") regulerer, hvordan Accel Comply (Behzad Motaghi, enkeltmandsvirksomhed, Vejle, Danmark) behandler personoplysninger ved levering af IT-sikkerhedsrådgivning, NIS2-parathedsanalyse, ISO 27001-parathedsanalyse, gennemgang af cloud-omkostninger eller AI-parathedsanalyse til en kundeorganisation ("Dataansvarlig").

Hvad denne DBA gør: - Bekræfter, at Accel Comply optræder som databehandler under GDPR Artikel 28. - Beskriver præcist, hvilke personoplysninger der behandles, hvorfor og på hvilket retsgrundlag. - Lister de aktuelle underdatabehandlere og overførselsmekanismerne, som dækker amerikanske værktøjer (EU-US Data Privacy Framework + EU's Standardkontraktbestemmelser, Kommissionens afgørelse (EU) 2021/914). - Jeg underretter dig om ethvert brud på persondatasikkerheden inden for **24 timer** efter, jeg er blevet bekendt med det (hvis du er en NIS2-omfattet enhed) eller inden for **48 timer** (for alle andre dataansvarlige). Begge frister er strengere end GDPR Art. 33(2)'s baseline om "uden unødigt ophold." For NIS2-omfattede dataansvarlige er 24-timers-fristen udformet for at give dig arbejdstid, inden din egen Art. 23-tidlig-varslingsforpligtelse til den nationale CSIRT forfalder; den forpligtelse påhviler dig, ikke mig. I praksis sigter jeg efter at underrette inden for 2-4 timer. For alle andre dataansvarlige giver 48-timers-fristen dig tid til at vurdere, inden GDPR Art. 33(1)'s 72-timers controller-til-myndighed-frist udløber. - Forpligter mig til konkrete, navngivne sikkerhedsforanstaltninger (Bilag 3). - Sikrer sletning eller tilbagelevering af alle kundedata inden for **30 dage** efter aftalens ophør.

Denne DBA supplerer og erstatter ikke Hovedaftalen mellem parterne.

Lovvalg: Kongeriget Danmark. **Tilsynsmyndighed:** Datatilsynet (www.datatilsynet.dk).

Del A: Hovedaftale

1. Parter og indledende bestemmelser

Sådan udfyldes denne DBA

Denne DBA er en skabelon. Den er ikke bindende, før begge parter har underskrevet en udfyldt version med alle pladsholdere udfyldt. De felter, der kræver udfyldning, er:

- Punkt 1.1: Dataansvarliges fulde juridiske navn, CVR-nummer og registrerede adresse.
- Punkt 1.2(a): Dato for Hovedaftalen og kort beskrivelse af de engagerede ydelser.

- Bilag 1: Behandlingens genstand og formål, specifikke kategorier af personoplysninger og kategorier af registrerede for engagementet.
- Punkt 16.1 og Bilag 3 §9.1: Forsikringsselskabets navn og policenummer (angivet i hver underskrevet Hovedaftale).

Indtil en udfyldt, underskrevet version foreligger, har dette dokument ingen kontraktuel bindingskraft. Behandl ikke den offentliggjorte version som en eksekveret DBA.

1.1 Parterne i denne DBA er:

Dataansvarlig ("Dataansvarlig")	[KUNDENS JURIDISKE NAVN], [KUNDENS CVR-NR], [KUNDENS ADRESSE] ("du", "den Dataansvarlige")
Databehandler ("Databehandler")	Behzad Motaghi, der driver virksomhed under navnet **Accel Comply**, CVR DK37260312, Vejle, Danmark ("jeg", "Accel Comply", "Databehandleren")

1.2 Indledende bestemmelser

(a) Du har antaget mig under en hovedaftale (i form af et aftalebrev, en rådgivningsaftale eller en rammekontrakt) dateret [DATO] ("Hovedaftalen") til at levere [kort beskrivelse af tjenesten, f.eks. NIS2-parathedsanalyse].

(b) Som led i levering af disse ydelser vil jeg behandle personoplysninger på dine vegne. GDPR Artikel 28 kræver, at det forhold dokumenteres ved en skriftlig aftale.

(c) Denne DBA opfylder det krav. Den udgør en del af Hovedaftalen. Hvis denne DBA og Hovedaftalen er i konflikt om databeskyttelsesforhold, gælder denne DBA.

(d) Begge parter er forpligtet til at behandle personoplysninger i overensstemmelse med Forordning (EU) 2016/679 ("GDPR") og databeskyttelsesloven (Lov nr. 502 af 23. maj 2018 med senere ændringer).[1]

---

[1] Databeskyttelsesloven (Lov nr. 502 af 23. maj 2018 med senere ændringer). Den danske lov supplerer GDPR på områder, hvor forordningen giver medlemsstaterne skønsmargen, herunder undtagelser for offentlige myndigheder, oplysninger om strafbare forhold og journalistiske formål. Den skaber ikke selvstændige forpligtelser for databehandlere ud over dem i GDPR i kommercielle B2B-rådgivningssammenhænge. Se https://www.datatilsynet.dk/english/the-danish-data-protection-act

2. Definitioner

Følgende udtryk har den betydning, der er tildelt dem i GDPR, og er gengivet her for læsevenlighedens skyld:

"DBA": denne databehandleraftale, inklusive bilag, der regulerer min behandling af personoplysninger på dine vegne.

"Personoplysninger" (Personal Data): enhver form for information om en identificeret eller identificerbar fysisk person ("registreret"); GDPR Art. 4(1).

"Følsomme personoplysninger" (Special Category Data): personoplysninger om race eller etnisk oprindelse, politiske, religiøse eller filosofiske overbevisninger eller fagforeningsmæssige tilhørsforhold, genetiske data, biometriske data med henblik på entydig identifikation af en fysisk person, helbredsoplysninger eller oplysninger om en fysisk persons seksuelle forhold eller seksuelle orientering; GDPR Art. 9.

"Behandling" (Processing): enhver aktivitet eller række af aktiviteter, som personoplysninger gøres til genstand for, hvad enten det er ved automatiserede midler eller ej; GDPR Art. 4(2).

"Dataansvarlig" (Data Controller): den fysiske eller juridiske person, offentlige myndighed, agentur eller andet organ, der alene eller sammen med andre afgør, til hvilke formål og med hvilke hjælpemidler der må foretages behandling af personoplysninger; GDPR Art. 4(7).

"Databehandler" (Data Processor): en fysisk eller juridisk person, offentlig myndighed, agentur eller andet organ, der behandler personoplysninger på den dataansvarliges vegne; GDPR Art. 4(8).

"Underdatabehandler" (Sub-processor): enhver tredjepart, jeg engagerer til at udføre specifikke behandlingsaktiviteter på dine personoplysninger; GDPR Art. 28(2).

"Brud på persondatasikkerheden" (Personal Data Breach): et brud på sikkerheden, der fører til hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger; GDPR Art. 4(12).

"Registreret" (Data Subject): den identificerede eller identificerbare fysiske person, som personoplysningerne vedrører; GDPR Art. 4(1).

"Tilsynsmyndighed": Datatilsynet, Carl Jacobsens Vej 35, 2500 Valby, Danmark.

"SKB": Standardkontraktbestemmelserne for overførsel af personoplysninger til tredjelande, vedhæftet Kommissionens gennemførelsesafgørelse (EU) 2021/914 af 4. juni 2021.[2]

[2] Kommissionens gennemførelsesafgørelse (EU) 2021/914 af 4. juni 2021 om standardkontraktbestemmelser for overførsel af personoplysninger til tredjelande i henhold til Forordning (EU) 2016/679. Offentliggjort i EU-Tidende L 199, 7.6.2021, s.

"DPF": EU-US Data Privacy Framework-tilstrækkelighedsafgørelsen vedtaget af Europa-Kommissionen den 10. juli 2023.[3]

"Hovedaftale": den aftale, der regulerer ydelserne, som omtalt i Punkt 1.2(a) (uanset om den i praksis benævnes aftalebrev, hovedaftale, rådgivningsaftale eller rammekontrakt).

"TOF": Tekniske og Organisatoriske Foranstaltninger som beskrevet i Bilag 3 til denne DBA.

"NIS2-loven": Lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau, i kraft 1. juli 2025.

"DORA": Forordning (EU) 2022/2554 om digital operationel modstandsdygtighed for finanssektoren, anvendelig fra 17. januar 2025.

---

3. Behandlingens omfang og formål

3.1 Jeg behandler kun dine personoplysninger:

(a) til de formål, der er beskrevet i Bilag 1 (Beskrivelse af behandlingen); og

(b) efter dine dokumenterede instrukser, herunder som fastsat i denne DBA og Hovedaftalen.

3.2 Jeg behandler ikke personoplysninger til andre formål, herunder mine egne kommercielle formål (såsom markedsføring, serviceforbedring eller benchmarking), uden dit forudgående skriftlige samtykke.

3.3 Hvis jeg vurderer, at en af dine instrukser bryder med GDPR eller dansk databeskyttelseslovgivning, oplyser jeg dig om det med det samme, skriftligt, med begrundelse. Jeg kan sætte den pågældende instruks på pause, indtil vi har afklaret det, men jeg fortsætter med at følge dine øvrige lovlige instrukser.

31-61. Tilgængelig: https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj/eng. Modul 3 (Databehandler til underdatabehandler) er det operative modul for overførsler fra Accel Comply (Databehandler) til operationelle underdatabehandlere.

[3] Kommissionens gennemførelsesafgørelse (EU) 2023/1795 af 10. juli 2023, EU-US Data Privacy Framework-tilstrækkelighedsafgørelsen. Pr. april 2026 forbliver DPF i kraft: EU's Ret afviste Latombe-udfordringen 3. september 2025; Latombe indgav appel til EU-Domstolen i oktober 2025, som er under behandling. PCLOB mistede sit beslutningsdygtige medlemstal i januar 2025 efter politisk motiverede bestyrelsesfjernelser, hvilket rejser bekymringer om det tilsynsorgan, EU-Domstolen tidligere stolede på i Schrems II. Parallel SKB-dækning opretholdes efter Punkt 9. Se https://www.dataprivacyframework.gov. EDPB DPF FAQ opdateret 15. januar 2026.

3.4 Hvor jeg behandler personoplysninger i forbindelse med en NIS2-parathedsanalyse, ISO 27001-parathedsanalyse, gennemgang af cloud-omkostninger eller AI-parathedsanalyse, er omfanget yderligere begrænset til data, der med rimelighed er nødvendige for at gennemføre den specifikke ydelse. Jeg anvender dataminimering som standard: hvis en opgave kan gennemføres på anonymiserede eller pseudonymiserede data, anmoder jeg om data i den form.

3.5 Ændring af instrukser. Du kan ændre dine instrukser ved skriftlig meddelelse, der henviser til denne DBA og specificerer eventuelle ændringer i omfanget i Bilag 1. Jeg bekræfter modtagelsen og opdaterer Bilag 1 i overensstemmelse hermed inden for 5 arbejdsdage.

---

4. Varighed

4.1 Denne DBA træder i kraft på den dato, hvor Hovedaftalen underskrives, og forbliver i kraft, så længe jeg behandler personoplysninger på dine vegne.

4.2 Denne DBA ophører, når Hovedaftalen ophører, dog således at:

(a) fortrolighedsforpligtelserne i Punkt 7.2 består på ubestemt tid efter ophør; og

(b) sletnings- eller tilbageleveringsforpligtelserne i Punkt 15 består i 30 dage efter ophør.

---

5. Personoplysningernes karakter og kategorier

5.1 Jeg forventer at behandle følgende kategorier af personoplysninger i typiske engagementer, som yderligere specificeret i Bilag 1:

Kategori	Typisk kontekst	Eksempler
Medarbejderkatalog	Adgangsgennemgange; IAM-audits; udtræk af brugerlister til omfangskortlægning	Navn, arbejds-e-mail, jobtitel, afdeling, systemadgangsrettigheder
Kontaktdata for leverandører	Tredjepartsrisikogennemgange; sikkerhedsspørgeskemaer til leverandører	Navn, forretnings-e-mail, telefonnummer, rolle eller titel
Personoplysninger om kunder	Omfangsfastsættelse af kundevendte processer; DPIA-bistand	Kan omfatte navn, e-mail, kontoidentifikatorer, kun hvor strengt nødvendigt for omfanget
System- og	NIS2-parathedsanalyse;	Brugernavne, IP-adresser,

Kategori	Typisk kontekst	Eksempler
netværksloggene	cloud-sikkerhedsgennemgange	enhedsidentifikatorer i logfiler
Autentifikationsdata	MFA-audit; gennemgang af adgangskontrol	Brugernavne, tildelt MFA-metode (ikke selve credentials)

5.2 Følsomme personoplysninger. Følsomme personoplysninger er ikke omfattet af denne DBA, medmindre de udtrykkeligt er medtaget i Hovedaftalen sammen med de yderligere foranstaltninger, der vil gælde.

Inden et engagement påbegyndes, hvor en af parterne med rimelighed forventer, at omfanget kan omfatte følsomme personoplysninger (f.eks. engagementer med sundhedsudbydere, sociale organisationer, HR-systemgennemgange eller arbejdsmedicinsk data), rejser jeg Art. 9-klassificeringen udtrykkeligt under scoping-processen, dokumenterer kategorierne af følsomme personoplysninger i Bilag 1 og aftaler de yderligere foranstaltninger skriftligt, inden sådanne data tilgås. Hvor engagementet er med en sundheds- eller socialorganisation, er dette pre-engagement-klassifikationstrin obligatorisk, ikke valgfrit.

Hvis jeg utilsigtet får adgang til følsomme personoplysninger under et engagement, underretter jeg dig uden unødigt ophold og hverken opbevarer, kopierer eller behandler de pågældende oplysninger yderligere.

5.3 Børns data. Personoplysninger om børn (registrerede under 16 år, eller under en sådan anden aldersgrænse, som gælder efter medlemsstatslovgivning, jf. GDPR Art. 8(1)) er ikke omfattet af denne DBA, medmindre de udtrykkeligt er medtaget i Hovedaftalen sammen med de yderligere foranstaltninger, der vil gælde (herunder verifikation af forældresamtykke, hvor det er relevant).

---

6. Kategorier af registrerede

Afhængigt af engagementets omfang kan registrerede omfatte:

(a) **Dine medarbejdere:** hvis data optræder i systemer, adgangsgennemgange eller brugerkataloger, jeg gennemgår.

(b) **Dine kunder:** fysiske personer, som er kunder hos dig, hvor deres personoplysninger optræder i systemer eller processer inden for engagementets omfang.

(c) **Dine leverandører og samarbejdspartnere:** individuelle kontakter hos tredjepartsorganisationer, som du har en relation til.

(d) **Systemadministratorer og IT-personale:** indehavere af privilegerede konti, hvis adgangsrettigheder gennemgås som led i en sikkerhedsvurdering.

7. Databehandlerens forpligtelser

7.1 Behandling efter dokumenterede instrukser (Art. 28(3)(a))

Jeg behandler kun personoplysninger efter dine dokumenterede instrukser, medmindre andet kræves efter EU-ret eller dansk ret. Hvis det sker, oplyser jeg dig om det retlige krav før behandlingen, medmindre loven forbyder en sådan oplysning af vigtige samfundsinteresser.

7.2 Personalets fortrolighed (Art. 28(3)(b))

Jeg sikrer, at alle personer, der er bemyndiget til at behandle personoplysninger, er underlagt en passende fortrolighedsforpligtelse. Da Accel Comply er en enkeltmandsvirksomhed, er jeg den eneste person med adgang til dine personoplysninger i det daglige engagement. Denne bestemmelse omfatter også enhver afløser eller midlertidig medarbejder, der måtte blive engageret under særlige omstændigheder, og som skal underskrive en skriftlig fortrolighedsforpligtelse, før vedkommende får adgang.

7.3 Sikkerhedsforanstaltninger (Art. 28(3)(c); Art. 32)

Jeg implementerer og opretholder de Tekniske og Organisatoriske Foranstaltninger, der er beskrevet i Bilag 3. Jeg gennemgår, om foranstaltningerne er tilstrækkelige, mindst én gang årligt og i øvrigt efter et brud på persondatasikkerheden eller en væsentlig ændring i behandlingsmiljøet.

Jeg anerkender, at udvælgelse og opretholdelse af sikkerhedsforanstaltninger er en løbende forpligtelse.

7.4 Tilgængelighed, modstandsdygtighed og forretningskontinuitet (Art. 32(1)(b)-(c))

(a) Jeg opretholder forretningskontinuitetsforanstaltninger, der beskytter tilgængeligheden af dine personoplysninger og giver mig mulighed for at genoprette adgang efter en fysisk eller teknisk hændelse.

(b) Personoplysninger om kunden opbevares på steder, hvor du kan hente dem uden min aktive medvirken, enten i systemer, hvor du har egne adgangsoplysninger, eller i filarkiver, hvortil jeg vil oplyse adgangsdetaljer på skriftlig anmodning inden for 24 timer.

(c) For ethvert engagement med honorar på DKK 100.000 eller derover skal Hovedaftalen udpege en efterfølger eller anden kvalificeret IT- eller sikkerhedsrådgiver (en “Stedfortræder”), som vil modtage en overdragelse af alle personoplysninger, leverancer og arbejdsdokumenter i tilfælde af, at jeg er ude af stand til at arbejde, ophører med at virke i mere end **5 arbejdsdage** eller bliver insolvent. For engagementer under DKK 100.000 anbefales udpegning af en Stedfortræder, men er valgfri; ved manglende udpegning returneres data til dig. Overdragelsen omfatter alle leverancer fra engagementet,

arbejdsdokumenter, adgangsdetaljer og foreløbige fund. Stedfortræderen forpligter sig skriftligt til en tilsvarende fortrolighedsforpligtelse, før en overdragelse finder sted.

(d) Hvis jeg bliver insolvent eller likvideres, har du ret til at anmode om øjeblikkelig tilbagelevering eller sletning af alle personoplysninger, der opbevares under denne DBA, og jeg forpligter mig til at sikre, at en overdragelsesmekanisme er på plads som beskrevet ovenfor. Denne bestemmelse supplerer og har, i forhold til personoplysninger, forrang for ethvert insolvensretligt forbud mod aktivoverdragelse.[4]

7.5 Underdatabehandlere (Art. 28(2) og (4))

(a) Du giver hermed generel skriftlig bemyndigelse til, at jeg engagerer de underdatabehandlere, der er anført i Bilag 2 på tidspunktet for underskrivelsen af denne DBA.

(b) Jeg engagerer ikke en ny underdatabehandler eller ændrer væsentligt rollen for en eksisterende underdatabehandler uden at give dig mindst **14 dages forudgående skriftlig varsel** (e-mail til din udpegede kontaktperson er tilstrækkelig) med angivelse af underdatabehandlerens navn, etableringsland og behandlingens art. Efter skriftlig anmodning fra dig, før 14-dages-fristen begynder at løbe, forlænges varslet til **30 dage**.

(c) Hvis du gør indsigelse inden for 14 dage, skal du give mig skriftlig besked. Jeg har derefter yderligere 14 dage til at finde en løsning. Hvis det ikke kan lade sig gøre, kan du opsige den relevante del af engagementet uden bod.

(d) Jeg pålægger, som krævet af Art. 28(4) og som yderligere fortolket af EDPB Opinion 22/2024 om databehandleres og underdatabehandleres forpligtelser[5],

---

[4] Datatilsynets opdatering fra marts 2024 af standarddatabehandleraftalen gjorde insolvens- eller begunstigelsesklausulen valgfri (tidligere obligatorisk), i tråd med EU-Kommissionens SKB 2021/914. Marts 2024-opdateringen bemærker, at selvom klausulen er valgfri, har dataansvarlige fortsat ansvaret for at sikre, at personoplysninger er tilstrækkeligt beskyttet, hvis databehandleren ophører med at virke. Se https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2024/mar/aendring-i-datatilsynets-standarddatabehandleraftale. Den per-engagement efterfølgermekanisme i Punkt 7.4(c) implementerer et praktisk alternativ til standardskabelonens klausul.

[5] EDPB Opinion 22/2024 af 8. oktober 2024 om visse forpligtelser, der følger af tilliden til databehandlere og underdatabehandlere. Udtalelsen klarlægger, at dataansvarlige bevarer due-diligence-forpligtelser gennem hele underdatabehandlerkæden, og at databehandlere skal støtte den dataansvarliges evne til at opfylde denne forpligtelse. Oplysningsforpligtelserne i Punkt 7.5(e) og 9.4 i denne DBA er udformet til at operationalisere denne dataansvarlig-side-forpligtelse. Tilgængelig:

hver underdatabehandler de samme databeskyttelsesforpligtelser, som er fastsat i denne DBA, ved skriftlig kontrakt. Jeg forbliver fuldt ansvarlig over for dig for underdatabehandlerens opfyldelse af disse forpligtelser.

(e) Jeg vedligeholder en opdateret liste over underdatabehandlere og gør den tilgængelig for dig på anmodning inden for 3 arbejdsdage.

7.6 De registreredes rettigheder (Art. 28(3)(e))

Jeg bistår dig med at besvare anmodninger fra registrerede, som udøver deres rettigheder efter GDPR Kapitel III (herunder retten til indsigt, berigtigelse, sletning, begrænsning, dataportabilitet og indsigelse). Når jeg modtager en sådan anmodning, vil jeg:

(a) Videresende den til dig uden unødigt ophold (og under alle omstændigheder inden for 2 arbejdsdage);

(b) Fremlægge en kopi af eventuelle personoplysninger, jeg har, som vedrører den registrerede, inden for 5 arbejdsdage efter din skriftlige anmodning; og

(c) Ikke svare den registrerede direkte, medmindre du skriftligt instruerer det.

Hvis en registreret kontakter mig direkte for at udøve sine rettigheder, underretter jeg dig straks og bekræfter, at jeg har henvist den registrerede tilbage til dig.

7.7 Bistand vedrørende sikkerhed, brud og DPIA'er (Art. 28(3)(f))

Jeg bistår dig med at opfylde dine forpligtelser efter Art. 32 (sikkerhed), Art. 33-34 (anmeldelse af brud) og Art. 35-36 (konsekvensanalyser vedrørende databeskyttelse). På din skriftlige anmodning om DPIA-bistand leverer jeg inden for **10 arbejdsdage**:

(a) En beskrivelse af de engagementsspecifikke datastrømme;

(b) En liste over de involverede kategorier af personoplysninger, registrerede og underdatabehandlere;

(c) En vurdering af de engagementsspecifikke risici, jeg har identificeret;

(d) En beskrivelse af de tekniske og organisatoriske foranstaltninger, der er anvendt til at imødegå disse risici (med krydshenvisning til Bilag 3).

Detaljerede forpligtelser om anmeldelse af brud er fastsat i Punkt 11.

---

https://www.edpb.europa.eu/system/files/2024-10/edpb_opinion_202422_relianceonprocessors-sub-processors_en.pdf

7.8 Fortegnelse over behandlingsaktiviteter (Art. 30(2))

Jeg vedligeholder den fortegnelse over behandlingsaktiviteter, der kræves efter GDPR Art. 30(2), og gør den tilgængelig for dig eller for Datatilsynet på skriftlig anmodning inden for 5 arbejdsdage.

7.9 Sletning eller tilbagelevering ved behandlingens ophør (Art. 28(3)(g))

Forpligtelser til sletning og tilbagelevering er fastsat i Punkt 15.

7.10 Auditrettigheder (Art. 28(3)(h))

Auditrettigheder er fastsat i Punkt 12.

7.11 Personoplysninger anvendes ikke til træning af AI/ML-modeller

(a) Jeg anvender ikke dine personoplysninger og tillader ikke mine underdatabehandlere at anvende dine personoplysninger til at træne, finjustere eller evaluere kunstig intelligens-modeller (AI) eller maskinlæringsmodeller (ML), medmindre du udtrykkeligt instruerer mig skriftligt om at gøre det til et specifikt engagementsformål (f.eks. når selve engagementet er din egen AI-parathedsanalyse, og dine data anvendes til at teste en defineret model).

(b) Jeg bekræfter, at de underdatabehandlere, der er anført i Bilag 2, i de kontraktuelle indstillinger, jeg har valgt, er konfigureret således, at de ikke anvender dine personoplysninger til træning af generiske AI- eller ML-modeller til underdatabehandlerens egen fordel. Hvor en underdatabehandler tilbyder en opt-in til AI-træning, har jeg fravalgt denne. Jeg genbekræfter denne konfiguration årligt og efter enhver væsentlig ændring i underdatabehandlerens vilkår.

(c) Hvor jeg anvender generative AI-værktøjer (herunder store sprogmodeller) til at udarbejde leverancer i engagementet, oplyser jeg i Hovedaftalen værktøjets navn, kategorierne af input, jeg leverer til værktøjet, og de forpligtelser om databehandling, som leverandøren af værktøjet har afgivet. Jeg leverer ikke dine personoplysninger til sådanne værktøjer som input, medmindre det udtrykkeligt er tilladt i Hovedaftalen.

(d) Denne bestemmelse supplerer og erstatter ikke eventuelle AI-specifikke forpligtelser efter EU's AI-forordning (Forordning (EU) 2024/1689), der gælder for nogen af parterne. For EU AI-forordningens formål optræder jeg som **bruger** (deployer) af AI-systemer leveret af tredjepartsudbydere (herunder enhver stor sprogmodel identificeret i Hovedaftalen). Jeg er ikke udbyder af disse AI-systemer. Mine forpligtelser som bruger efter AI-forordningens Art. 26 gælder, hvor AI-systemet anvendes i en professionel kontekst under et engagement.

---

8. Underdatabehandlere

Aktuelle underdatabehandlere er anført i Bilag 2. Processen for at engagere nye eller ændrede underdatabehandlere er fastsat i Punkt 7.5.

---

9. Overførsler til tredjelande

9.1 Overførsler til underdatabehandlere etableret i USA er dækket af:

(a) **EU-US Data Privacy Framework** (Kommissionens gennemførelsesafgørelse (EU) 2023/1795 af 10. juli 2023), hvor underdatabehandleren er certificeret under DPF-programmet; og

(b) **EU's Standardkontraktbestemmelser** (Kommissionens afgørelse (EU) 2021/914, **Modul 3: Databehandler til underdatabehandler**), som anvendes parallelt som en uafhængig overførselsmekanisme.

Hvis EU-Domstolen erklærer DPF ugyldig eller suspenderer den, som det skete med Safe Harbor (2015) og Privacy Shield (2020), fortsætter SKB som den eneste operative overførselsmekanisme uden yderligere handling fra din side og uden ændring af denne DBA. Inden for **10 arbejdsdage** efter en sådan ugyldighedserklæring eller suspension underretter jeg dig skriftligt og bekræfter, om der kræves supplerende foranstaltninger (jf. EDPB-anbefalinger 01/2020) for at opretholde et i det væsentlige tilsvarende beskyttelsesniveau.

9.2 Det korrekte SKB-modul for alle overførsler fra mig (som Databehandler) til mine operationelle underdatabehandlere (HubSpot og Microsoft) er **Modul 3 (Databehandler til underdatabehandler)**. Det gælder hele denne DBA og Bilag 2. Hvor en underdatabehandlers egen databehandleraftale med mig anvender Modul 2 (Dataansvarlig til Databehandler), f.eks. hvor en leverandør betragter sig selv som dataansvarlig for visse behandlinger, dokumenteres det forhold separat i den relevante fodnote.

9.3 Ingen personoplysninger omfattet af denne DBA overføres til et tredjeland uden for EØS, medmindre der er etableret en lovlig overførselsmekanisme efter GDPR Kapitel V. Jeg dokumenterer den anvendte mekanisme for hver underdatabehandler i Bilag 2.

9.4 Konsekvensanalyse vedrørende overførsel (TIA). For hver overførsel af personoplysninger til en underdatabehandler etableret uden for EØS, der bygger på SKB som den operative overførselsmekanisme (uanset om det er som primær mekanisme eller som DPF-fallback), vedligeholder jeg en dokumenteret Transfer Impact Assessment (TIA) udført i overensstemmelse med EDPB-anbefalinger 01/2020 om supplerende foranstaltninger (endelig version, juni 2021)[6] og SKB Punkt 14. TIA'en

[6] EDPB-anbefalinger 01/2020 om foranstaltninger, der supplerer overførselsværktøjer for at sikre overholdelse af EU's databeskyttelsesniveau, endelig version vedtaget 18.

vurderer, om lovgivningen og praksis i destinationslandet forhindrer underdatabehandleren i at opfylde SKB. Jeg gør den aktuelle TIA tilgængelig for dig på skriftlig anmodning inden for **10 arbejdsdage** eller inden for **5 arbejdsdage**, hvis du angiver en regulatorisk frist i anmodningen. Jeg gennemgår hver TIA årligt og umiddelbart efter en væsentlig ændring i overførselskonteksten eller i lovgivningen i destinationslandet (herunder enhver DPF-ugyldighedserklæring).[7]

Aktuel TIA-konklusion (pr. DBA'ens ikrafttrædelsesdato): For overførsler til HubSpot (USA) og Microsoft (USA) under SKB Modul 3 med EU-US DPF som co-gældende, har jeg vurderet det amerikanske retsmiljø efter EDPB's seks-trins-ramme og konkluderet, at underdatabehandlerne, med de supplerende foranstaltninger på plads (EU-datacenter eller EU-datagrænse som primær behandlingslokation; kontraktuelle forbud mod amerikansk myndighedsadgang ud over det lovmæssigt krævede; TLS 1.2+ under transport; AES-256 i hvile), kan opfylde SKB, og at et i det væsentlige tilsvarende beskyttelsesniveau eksisterer for disse specifikke overførsler. For Microsoft betyder EU-datagrænsen for M365, at data for EU-baserede kunder opbevares og behandles inden for EØS som et primært anliggende; US-side-adgang til support og engineering er underlagt SKB Modul 3 og DPF som en parallel mekanisme. Det PCLOB-kvorum-spørgsmål, der er nævnt i Fodnote [8], er vurderet og ændrer i øjeblikket ikke denne konklusion, da SKB forbliver den operative uafhængige mekanisme. Hvis denne vurdering ændrer sig, underretter jeg dig inden for 10 arbejdsdage.

9.5 Alle aktuelle underdatabehandlere er etableret enten i EØS eller i USA (sidstnævnte under EU-US DPF + SKB). Jeg engagerer ikke databehandlere i tredjelande uden en tilstrækkelighedsafgørelse. Hvis dette ændrer sig under et engagement, underretter jeg

---

juni 2021. Den seks-trins-ramme for Transfer Impact Assessments er fastsat i Sektion II i disse Anbefalinger. Tilgængelig: https://www.edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_en

[7] SKB 2021/914, Punkt 14 kræver, at parterne indestår for, at de ikke har grund til at antage, at lovgivningen og praksis i destinationslandet hindrer importøren i at opfylde SKB. Det er en løbende forpligtelse, ikke en engangskontrol ved underskrivelse. Databehandlerens TIA-forpligtelse i Punkt 9.4 er den kontraktuelle mekanisme, der operationaliserer denne forpligtelse og gør den tilgængelig for den dataansvarliges tilsyn.

[8] Kommissionens gennemførelsesafgørelse (EU) 2023/1795 af 10. juli 2023, EU-US Data Privacy Framework-tilstrækkelighedsafgørelsen. Pr. april 2026 forbliver DPF i kraft: EU's Ret afviste Latombe-udfordringen 3. september 2025; Latombe indgav appel til EU-Domstolen i oktober 2025, som er under behandling. PCLOB mistede sit beslutningsdygtige medlemstal i januar 2025 efter politisk motiverede bestyrelsesfjernelser, hvilket rejser bekymringer om det tilsynsorgan, EU-Domstolen tidligere stolede på i Schrems II. Parallel SKB-dækning opretholdes efter Punkt 9. Se https://www.dataprivacyframework.gov. EDPB DPF FAQ opdateret 15. januar 2026.

dig efter Punkt 7.5 (varsel om ændring af underdatabehandler) og indhenter eller dokumenterer den relevante overførselsmekanisme (yderligere SKB, undtagelser efter GDPR Art. 49 eller andre gældende sikringer), før personoplysninger overføres.

9.6 Overførsler til Storbritannien. Hvor du er omfattet af UK GDPR (dvs. du er etableret i Storbritannien, eller personoplysninger om personer bosiddende i Storbritannien behandles under denne DBA), gælder UK GDPR's overførselsbestemmelser uafhængigt af EU GDPR. For enhver overførsel af britiske personoplysninger til USA-baserede underdatabehandlere anført i Bilag 2 er den gældende britiske overførselsmekanisme fastsat i Bilag 5 (UK IDTA / UK Addendum). Bilag 5 udløses automatisk, når en af parterne identificerer, at britiske personoplysninger er omfattet; ingen yderligere instruks er påkrævet.

9.7 Opdateringer af SKB og tilstrækkelighedsafgørelser. Hvor Europa-Kommissionen udsteder nye eller opdaterede Standardkontraktbestemmelser eller ændrer Kommissionens afgørelse (EU) 2021/914, opdateres denne DBA automatisk for at indarbejde de nye bestemmelser fra den dato, de nye bestemmelser har virkning, svarende til auto-opdateringsmekanismen i Bilag 5 §A5.1.2 for UK Addendum. Hvor Kommissionen udsteder nye eller ændrede tilstrækkelighedsafgørelser, der berører en underdatabehandler, underretter jeg dig efter Punkt 7.5 inden for **10 arbejdsdage**.

---

10. NIS2-leverandørkædesikkerhed

10.1 Forpligtelserne i dette Punkt 10 gælder automatisk, hvor du er en væsentlig enhed eller vigtig enhed i medfør af NIS2-loven (Lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau, i kraft 1. juli 2025). Du indestår ved underskrivelsen for, om du er en omfattet enhed. Parterne skal ikke foretage yderligere skridt for at aktivere disse forpligtelser; dog gælder de ikke, hvis du ikke er en NIS2-omfattet enhed.[9]

10.2 NIS2 Art. 21(2)(d) kræver, at væsentlige og vigtige enheder sikrer, at deres direkte leverandører og tjenesteudbydere opfylder tilstrækkelige cybersikkerhedsstandarder. De forpligtelser, jeg påtager mig i dette Punkt 10, er kontraktuelle tilsagn, jeg afgiver for at understøtte din overholdelse af den forpligtelse; de er ikke forpligtelser, NIS2 pålægger mig direkte som din leverandør. Hvor dette Punkt 10 finder anvendelse, forpligter jeg mig til:

[9] NIS2-direktivet (EU) 2022/2555, Art. 21(2)(d): væsentlige og vigtige enheder skal implementere "leverandørkædesikkerhed, herunder sikkerhedsrelaterede aspekter vedrørende relationerne mellem hver enhed og dens direkte leverandører eller tjenesteudbydere." Gennemført i Danmark via NIS2-loven (Lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau), i kraft 1. juli 2025. Ved at placere disse forpligtelser i hovedteksten med en betingelsesundtagelse sikrer DBA-strukturen, at en NIS2-omfattet dataansvarlig ikke skal anmode om aktivering, forpligtelserne er forhåndsindbygget, hvilket opfylder Art. 21(2)(d)-indkøbskravet.

(a) At opretholde sikkerhedsforanstaltningerne i Bilag 3 på et niveau, der risikoproportionalt dækker hændelseshåndtering, adgangskontrol, leverandørkæde og kryptering, og dermed understøtter din mulighed for at dokumentere leverandørsidens egnethed i henhold til NIS2 Art. 21(2)(d);

(b) At samarbejde om enhver NIS2-pålagt sikkerhedsaudit eller -vurdering, som du er forpligtet til at gennemføre af dine tjenesteudbydere, og at gøre det inden for auditrammen i Punkt 12;

(c) At underrette dig inden for **24 timer** efter, jeg er blevet bekendt med en cybersikkerhedshændelse på systemer, jeg anvender til at levere dit engagement, som du måske skal vurdere mod din egen NIS2 Art. 23-anmeldelsesforpligtelse. Din Art. 23-forpligtelse påhviler dig som væsentlig eller vigtig enhed; jeg kan ikke opfylde den på dine vegne. 24-timers-anmeldelsen giver dig arbejdstid til at vurdere og rapportere. Trusselsoplysninger, jeg støder på under engagementet, og som ikke når tærsklen for væsentlig hændelse, deles rettidigt som led i den almindelige engagementskommunikation, ikke under 24-timers-uret. For alle andre dataansvarlige (ikke omfattet af NIS2) underretter jeg dig inden for **48 timer** efter, jeg er blevet bekendt med et brud på persondatasikkerheden, som fastsat i Punkt 11;

(d) At pålægge tilsvarende NIS2-leverandørkædeforpligtelser på enhver underdatabehandler, hvis tjenester jeg anvender til at levere dit engagement, ved skriftlig kontrakt;

(e) På anmodning at oplyse følgende information til støtte for din kritikalitetsklassificering af mig som leverandør: min forretningskontinuitetsstatus (herunder RTO, RPO, backupstrategi og kontinuitetskontakt som beskrevet i Punkt 7.4), mit afhængighedskort over væsentlige fjerdepartsunderdatabehandlere (dvs. underdatabehandlere af mine underdatabehandlere, som er relevante for dit engagement), og min nuværende tilgang til sårbarhedshåndtering og afhjælpningstidsfrister; og

(f) At yde exit- og overgangsbistand som beskrevet i Punkt 14.4 for at understøtte en velordnet overdragelse, hvis engagementet ophører af enhver grund.

10.3 Intet i dette Punkt 10 begrænser forpligtelserne i den øvrige DBA, som gælder for alle dataansvarlige uanset NIS2-status.

10.4 Ændring af NIS2-status. Hvis en af parterne bliver bekendt med, at din NIS2-klassificering har ændret sig efter datoen for underskrivelse af denne DBA, f.eks. fordi din sektor eller delsektor bliver omfattet af NIS2-loven, eller fordi du når antals- eller omsætningstærsklen for status som væsentlig eller vigtig enhed, vil hver part:

(a) Underrette den anden skriftligt inden for **30 dage** efter at være blevet bekendt med ændringen;

(b) I fællesskab revurdere de leverandørkædeforpligtelser, der gælder efter NIS2 Art. 21(2)(d), inden for **60 dage** efter denne underretning; og

(c) Opdatere Hovedaftalen og denne DBA i overensstemmelse hermed for at afspejle eventuelle ændringer i de gældende forpligtelser.

Dette er en gensidig forpligtelse. Ingen part bærer revurderingsbyrden alene. Hvis jeg bliver bekendt med en ændring af din NIS2-status (f.eks. via sektorspecifikke regulatoriske offentliggørelser eller offentlige meddelelser), før du underretter mig, rejser jeg det med dig uden unødigt ophold.

---

11. Procedure for brud på persondatasikkerheden

11.1 Definition. Et brud på persondatasikkerheden er enhver hændelse, der opfylder definitionen i Punkt 2 i denne DBA. Jeg anvender definitionen bredt: den omfatter mistænkte brud, hvor jeg ikke umiddelbart kan bekræfte, om personoplysninger faktisk var berørt.

11.2 Tidsfrister. Anmeldelsesuret begynder at løbe, når jeg bliver bekendt med et bekræftet eller mistænkt brud. Når jeg bliver bekendt:

Trin 1, Inddæmning (inden for 4 timer): Isoler berørte systemer eller dataadgang; forhindr yderligere eksponering, hvor det er teknisk muligt.

Trin 2, Anmeldelse (inden for 24 timer for NIS2-omfattede dataansvarlige; inden for 48 timer for alle andre dataansvarlige): Send skriftlig anmeldelse til dig. Min anmeldelsesforpligtelse over for dig bygger på GDPR Art. 33(2). 24-timers- og 48-timers-fristerne er strengere kontraktuelle standarder end den lovbestemte baseline "uden unødigt ophold." For NIS2-omfattede dataansvarlige giver 24-timers-fristen dig arbejdstid til at vurdere situationen, inden din egen Art. 23(4)(a)-tidlig-varslingsforpligtelse til den nationale CSIRT forfalder; den forpligtelse påhviler dig som væsentlig eller vigtig enhed, og jeg kan ikke opfylde den på dine vegne. For alle andre dataansvarlige giver 48-timers-fristen dig tid til at vurdere og anmelde til Datatilsynet inden for GDPR Art. 33(1)'s 72-timers-vindue.[10]

---

[10] GDPR Art. 33(2) fastsætter den lovbestemte standard: "Hvor bruddet på persondatasikkerheden involverer en databehandler, skal denne databehandler underrette den dataansvarlige uden unødigt ophold, efter at databehandleren er blevet bekendt med bruddet på persondatasikkerheden." 24-timers- og 48-timers-fristerne i denne DBA er strengere kontraktuelle standarder end Art. 33(2)'s "uden unødigt ophold"-baseline. De er medtaget for at give praktisk virkning til den dataansvarliges egne nedstrøms-forpligtelser: 24-timers-fristen for NIS2-omfattede dataansvarlige sikrer tid til at indgive NIS2-loven Art. 23-tidlig-varsling til den nationale CSIRT; 48-timers-fristen for alle andre dataansvarlige sikrer tid til at vurdere, før GDPR Art. 33(1)'s 72-timers controller-til-myndighed-ur udløber. Se også Datatilsynets vejledning

Trin 3, Tilvejebring oplysninger om bruddet. Anmeldelsen vil i det omfang, det er kendt, indeholde:

(a) En beskrivelse af bruddets karakter, herunder kategorierne og det omtrentlige antal berørte registrerede og kategorierne og det omtrentlige antal berørte personoplysningsposter;

(b) Mit navn og kontaktoplysninger (Behzad Motaghi, info@accelcomply.com);

(c) En beskrivelse af bruddets sandsynlige konsekvenser;

(d) En beskrivelse af de foranstaltninger, der er truffet eller foreslået for at afhjælpe bruddet og afbøde dets eventuelle skadelige virkninger.

Hvis ikke alle oplysninger er tilgængelige på anmeldelsestidspunktet, leverer jeg det, der er kendt, og leverer suppleringer hurtigst muligt uden at vente, indtil et fuldstændigt billede foreligger.

11.3 Undersøgelse og samarbejde. Jeg samarbejder fuldt ud med din undersøgelse og, på din anmodning, med Datatilsynet eller enhver kompetent myndighed. Jeg kommunikerer ikke med registrerede om bruddet, medmindre du skriftligt instruerer det.

11.4 Dokumentation. Jeg dokumenterer alle brud på persondatasikkerheden, herunder de brud, der ikke skal anmeldes til en tilsynsmyndighed, og gør dokumentationen tilgængelig for dig på anmodning.

11.5 Anmeldelse er ikke en erkendelse af ansvar. Anmeldelse af et brud udgør ikke en erkendelse af ansvar fra min side.

---

12. Auditrettigheder

12.1 Årlig egenattestering. Én gang pr. kalenderår, uden ekstra omkostninger, leverer jeg til dig:

(a) En skriftlig bekræftelse af, at TOF i Bilag 3 fortsat er på plads og er gennemgået inden for de seneste 12 måneder; og

(b) En oversigt over eventuelle sikkerhedshændelser (herunder nær-hændelser) og afhjælpende foranstaltninger truffet i perioden.

12.2 Levering af dokumenter. Du kan til enhver tid anmode om relevant dokumentation (politikker, fortegnelser, underdatabehandleraftaler, TIA-resuméer, Art.

---

om brud-anmeldelse på https://www.datatilsynet.dk/english/data-security/personal-data-breach-notifications

30(2)-fortegnelser), ikke begrænset til én gang om året. Jeg leverer den ønskede dokumentation inden for 10 arbejdsdage.

12.3 Tredjepartsaudit på anmodning. Du kan, højst én gang pr. kalenderår (eller to gange pr. kalenderår i de 12 måneder, der følger efter et brud på persondatasikkerheden), bestille en tredjepartsaudit af min overholdelse af denne DBA. Du:

(a) Giver mig mindst **30 dages forudgående skriftlig varsel**;

(b) Bærer omkostningen til tredjepartsauditøren;

(c) Sikrer, at auditøren er underlagt en fortrolighedsforpligtelse, som mindst svarer til denne DBA;

(d) Begrænser auditens omfang til de behandlingsaktiviteter, der er omfattet af denne DBA.

12.4 Tredjepartscertificering som alternativ. Hvis jeg har en gyldig, tredjepartsbekræftet certificering, der er relevant for auditomfanget (f.eks. ISO 27001 eller SOC 2 Type II), kan jeg tilbyde den certificering og tilhørende bevis som alternativ til eller supplement til en fysisk audit, med dit samtykke. **Pr. denne DBA's ikrafttrædelsesdato har jeg ikke ISO 27001- eller SOC 2-certificering. Denne bestemmelse aktiveres kun, hvis og når en sådan certificering opnås og forbliver gyldig. Jeg underretter dig efter Punkt 7.5 inden for 10 arbejdsdage, når jeg opnår eller mister en sådan certificering.**

12.5 Samarbejde. Jeg samarbejder fuldt ud om audits og inspektioner, der gennemføres efter denne bestemmelse, herunder ved at give adgang til relevant dokumentation og systemer. Jeg kan med rimelighed begrænse fysisk adgang til lokaliteter, hvor andre kunders data behandles, forudsat at jeg gør tilsvarende dokumentbevis tilgængeligt.

12.6 Tilsynsmyndighedens audits. Auditrettighederne i denne bestemmelse begrænser ikke Datatilsynets lovbestemte kontrolbeføjelser efter GDPR Art. 58.

---

13. Ansvar

13.1 Mit samlede aggregerede ansvar over for dig under denne DBA, hvad enten det er i kontrakt, erstatning uden for kontrakt eller på anden måde, er begrænset til det **højeste af (a) 24 måneders honorarer betalt eller forfaldne under den relevante Hovedaftale i de 24 måneder, der ligger forud for den begivenhed, der giver anledning til kravet, eller (b) DKK 500.000** ("DBA-loftet"). Dette loft er et selvstændigt DBA-niveauloft og gælder uanset et eventuelt afvigende loft aftalt i Hovedaftalen.

13.2 Undtagelser. DBA-loftet finder ikke anvendelse på:

(a) Brud på fortrolighedsforpligtelsen i Punkt 7.2;

(b) Forsætlig misligholdelse eller grov uagtsomhed fra min side; eller

(c) Ansvar, der ikke kan begrænses efter ufravigelig dansk eller EU-lovgivning.

13.3 Bidrag til Datatilsynets bøder. Hvor du betaler en regulatorisk bøde eller sanktion pålagt af Datatilsynet, som helt eller delvist er forårsaget af min misligholdelse af denne DBA, og forudsat at du har overholdt dine egne GDPR-forpligtelser og har truffet rimelige skridt for at afbøde tabet, vil jeg bidrage til bøden i forhold til den andel af skylden, der kan tilskrives mig, op til DBA-loftet. Parterne fastlægger andelen af skylden ved en god-tro-fordeling, der afspejler Datatilsynets afgørelse; ved manglende enighed inden for **60 dage** efter, at bøden er pålagt, henvises sagen til tvistløsningsmekanismen i Punkt 17.2.

13.4 Underdatabehandlerens fejl. Jeg er ansvarlig over for dig for underdatabehandleres handlinger og undladelser i samme omfang, som hvis jeg selv havde udført behandlingen, dog underlagt DBA-loftet og undtagelserne i denne bestemmelse.

13.5 Bidragsret efter Art. 82. Hvor du betaler erstatning til en registreret efter GDPR Art. 82, og denne erstatning helt eller delvist kan tilskrives min misligholdelse af denne DBA, refunderer jeg dig den andel, der kan tilskrives min misligholdelse. Denne refunderingsforpligtelse er **ikke underlagt DBA-loftet**: bidragsretten efter Art. 82(5) er en mekanisme, der beskytter den registreredes effektive retsmiddel og kan ikke underlægges et kontraktuelt loft mellem parterne uden potentielt at fratage den registrerede fuld erstatning. Mit ansvar for min egen misligholdelse, som fastslået af den kompetente domstol eller tilsynsmyndighed, afgør det beløb, jeg skylder dig efter denne bestemmelse. Jeg samarbejder fuldt ud om ethvert Art. 82-krav, herunder ved at dele dokumenter, deltage i møder og levere oplysninger på vilkår, der aftales mellem os, uden vederlag til dig i første omgang.

13.6 Intet i denne DBA begrænser nogen af parternes ansvar over for registrerede eller over for Datatilsynet.

---

14. Aftalens ophør og opsigelse

14.1 Denne DBA ophører, når Hovedaftalen ophører.

14.2 Hver part kan opsige denne DBA med øjeblikkelig virkning ved skriftlig meddelelse, hvis:

(a) Den anden part begår en væsentlig misligholdelse af denne DBA og ikke afhjælper misligholdelsen inden for **14 dage** efter skriftlig meddelelse, der identificerer misligholdelsen;

(b) Den anden part ikke kan betale sine forpligtelser, indleder konkursbehandling eller likvidation eller ophører med at drive virksomhed; eller

(c) Fortsat behandling ville være i strid med GDPR eller anden gældende lovgivning.

14.3 Opsigelse af denne DBA fritager ikke nogen af parterne fra forpligtelser, der er opstået før opsigelsen.

14.4 Exit-bistand. Ved opsigelse eller udløb af Hovedaftalen af enhver grund og i en periode på **30 dage** efter opsigelsen vil jeg:

(a) Fortsat stille alle leverancer fra engagementet og arbejdsdokumenter til rådighed i et standard maskinlæsbart format (CSV, JSON eller som ellers aftalt);

(b) Yde rimelig vidensoverdragelsesbistand for at gøre dig eller din efterfølgende leverandør i stand til at fortsætte uden afbrydelse;

(c) Slette eller tilbagelevere alle personoplysninger efter Punkt 15.

(d) Med henblik på dette Punkt og Punkt 15 betyder "leverancer fra engagementet" alle rapporter, vurderinger, planer, anbefalinger, arbejdsdokumenter, dataeksporter, konfigurationsbeviser, skærmbilleder og andre dokumenter, jeg har frembragt under udførelsen af Hovedaftalen, i deres endelige eller aktuelle udkastform, i maskinlæsbart format hvor det er anvendeligt.

Hvis du er en NIS2-omfattet enhed, og engagementet understøtter en kritisk funktion, forlænges exit-bistandsperioden til **60 dage** på skriftlig anmodning.

---

15. Sletning og tilbagelevering af personoplysninger

15.1 Ved opsigelse eller udløb af Hovedaftalen eller tidligere efter din skriftlige anmodning vil jeg inden for **30 dage**:

(a) Sikkert slette eller tilbagelevere alle personoplysninger, der behandles på dine vegne (du kan angive din præference);

(b) Slette eller tilbagelevere alle kopier, herunder i backups og underdatabehandleres systemer, i det omfang jeg har bemyndigelse hertil.

15.2 Hvor du anmoder om tilbagelevering, leverer jeg dataene i et standard maskinlæsbart format (CSV, JSON eller som ellers aftalt).

15.3 På din skriftlige anmodning leverer jeg en skriftlig sletteattest inden for **10 arbejdsdage** efter, at sletningen er gennemført, med angivelse af de slettede datakategorier og den anvendte metode (f.eks. sikker overskrivning, kryptografisk sletning).

15.4 Jeg kan opbevare personoplysninger ud over 30 dage alene i det omfang, det er påkrævet efter EU-ret eller dansk ret (f.eks. regnskabsmateriale efter bogføringsloven). I så fald underretter jeg dig om opbevaringsgrundlaget og varigheden og behandler ikke dataene yderligere til andet formål.

---

16. Forsikring

16.1 Jeg har en professionsansvarsforsikring, der dækker krav, der opstår som følge af fejl og forsømmelser i professionelle rådgivningsydelser. Standarddækningen for engagementer omfattet af denne DBA er **DKK 5.000.000 pr. krav**, med forsikringsselskabets navn og policenummer angivet i Hovedaftalen. På skriftlig anmodning før underskrivelse af Hovedaftalen kan dækningen forhøjes (forudsat bekræftelse fra mit forsikringsselskab og en tilsvarende justering af engagementshonoraret for at afspejle den øgede præmie og selvrisiko); en højere dækning gælder kun, når den udtrykkeligt er anført i det underskrevne Hovedaftale. Bevis for bunden dækning på det aftalte niveau leveres efter Punkt 16.3, før behandlingen påbegyndes. Du kan betinge engagement under enhver ny kontrakt af skriftligt bevis for bunden dækning på det niveau, du kræver.[11]

16.2 Jeg underretter dig inden for **10 arbejdsdage**, hvis min professionsansvarsdækning bortfalder eller bliver væsentligt nedsat under det niveau, der er beskrevet i Punkt 16.1.

16.3 Bevis for aktuel dækning (forsikringscertifikat eller tilsvarende) er tilgængeligt på skriftlig anmodning inden for 5 arbejdsdage.

---

17. Lovvalg og værneting

17.1 Denne DBA er underlagt dansk ret, herunder GDPR som inkorporeret i dansk ret og databeskyttelsesloven.

17.2 Enhver tvist, der opstår som følge af eller i forbindelse med denne DBA, er underlagt de danske domstoles enekompetence. Den primære første instans for handelstvister mellem virksomheder er **Sø- og Handelsretten i København** (for tvister

[11] Datatilsynets fokusområder for tilsynsaktiviteter i 2026 omfatter undersøgelse af store databehandlere og deres tilsyn med underdatabehandlere, auditmekanismer og sikkerhedsforanstaltninger. Selvom Datatilsynet ikke pålægger PI-forsikring i GDPR-rammen, kræver indkøbsstandarder for danske industri- og offentlige sektorklienter ofte minimum DKK 10.000.000 i professionsansvarsdækning for IT-tjenesteudbydere, der behandler personoplysninger. Forsikringserklæringen i denne bestemmelse opfylder det indkøbskrav uden at udgøre en regulatorisk forpligtelse. Se https://www.datatilsynet.dk/afgoerelser/generelt-om-tilsyn/saerlige-fokusomraader-for-datatilsynets-tilsynsaktiviteter-i-2026

over DKK 500.000 eller mellem parter, der er enige om denne ret efter denne bestemmelse). For mindre krav har Retten i Vejle kompetence, medmindre parterne aftaler andet skriftligt.

17.3 Hver part kan eskalere sagen til Datatilsynet efter GDPR Art. 77 før eller i stedet for at indlede retssag.

---

18. DORA-tillægsmeddelelse (kunder i finanssektoren)

Hvor du er en finansiel enhed omfattet af DORA, henvises til Bilag 4 (DORA-tillæg), som udgør en del af denne DBA. Bilag 4 behandler de yderligere kontraktkrav efter DORA Art. 28-30 og er gældende fra datoen for underskrivelse af denne DBA.

---

19. Underskrifter

Denne DBA indgås på den dato, der senest er underskrevet nedenfor. Elektronisk underskrift (DocuSign, Adobe Sign eller tilsvarende) accepteres udtrykkeligt af begge parter.

For den Dataansvarlige:

Navn: _____

Titel: _____

Organisation: _____

Dato: _____

Underskrift: _____

For Databehandleren (Accel Comply / Behzad Motaghi):

Navn: Behzad Motaghi

Titel: Stifter, Accel Comply

Dato: _____

Underskrift: _____

Del B: Bilag

Bilag 1: Beskrivelse af behandlingen (GDPR Art. 28(3))

Bilag 1 udfyldes ved engagementets start som en del af Hovedaftalen og udgør en del af denne DBA. Den version af Bilag 1, der er gældende på et givent tidspunkt, er den version, der senest er underskrevet af begge parter eller vedhæftet den seneste ændring af Hovedaftalen.

Dette Bilag skal udfyldes eller bekræftes for hvert engagement. Det kan vedhæftes som en separat tilføjelse til Hovedaftalen.

Felt	Detaljer
Behandlingens genstand	Levering af [tjenestetype, f.eks. NIS2-parathedsanalyse] som beskrevet i Hovedaftalen
Behandlingens varighed	Slutter, når Hovedaftalen ophører; jf. Punkt 4
Behandlingens karakter	Tilgang til, gennemgang, analyse og rapportering om kundens datasystemer og processer; intet salg eller videregivelse til tredjepart; ingen automatiseret beslutningstagning med retsvirkning for de registrerede
Behandlingens formål	[Indsættes pr. engagement, f.eks. “At vurdere den Dataansvarliges nuværende cybersikkerhedsstilling og parathed i forhold til NIS2-krav, herunder gennemgang af IAM-konfigurationer, hændelseshåndteringsprocedurer og tredjepartsrisikohåndtering”]
Kategorier af personoplysninger	Som anført i Punkt 5.1; specificeres yderligere pr. engagement. Typisk: medarbejdernavne, arbejds-e-mailadresser, jobtitler, adgangsrettighedsloger, systembrugernavne, IP-adresser i logfiler, leverandørkontaktnavne og -e-mailadresser
Kategorier af registrerede	Som anført i Punkt 6; typisk: den Dataansvarliges medarbejdere; den Dataansvarliges leverandørkontakter; den Dataansvarliges kunder (kun hvor de er omfattet)
Følsomme personoplysninger	Ingen, medmindre udtrykkeligt aftalt i

Felt	Detaljer
	Hovedaftalen, jf. Punkt 5.2
Automatiseret beslutningstagning	Ingen, jeg foretager ikke automatiseret beslutningstagning eller profilering med retsvirkning eller tilsvarende væsentlig virkning for registrerede

Udfyldning og underskrift af Bilag 1

Dette Bilag 1 er udfyldt pr. [DATO] og udgør en del af DBA'en mellem [KUNDENS JURIDISKE NAVN] og Accel Comply (Behzad Motaghi), gældende fra [DATO].

For den Dataansvarlige: _____ Dato: _____

For Databehandleren: _____ Dato: _____

Bilag 2: Aktuelle underdatabehandlere

Denne liste er aktuel pr. DBA'ens ikrafttrædelsesdato. Ændringer varsles efter Punkt 7.5.

Alle overførsler fra mig (som Databehandler) til disse underdatabehandlere anvender **SKB Modul 3 (Databehandler til underdatabehandler)** efter Kommissionens afgørelse (EU) 2021/914. Hvor en underdatabehandler også har DPF-certificering, gælder begge mekanismer parallelt.

Underdatabehandler	Land / Jurisdiktion	Tjeneste / Rolle	Datakategorier	Overførselsmekanisme
HubSpot, Inc.	USA (EU-datacenter tilgængeligt)	CRM, marketingautomatisering, kontaktformularer og HubSpot Meetings (booking af kunde- og prospektmøde	Kundekontaktnavne, forretnings-e-mailadresser, telefonnumre, mødetidspunkter	EU-US DPF + SKB (EU 2021/914, **Modul 3**). HubSpot DPA, senest ændret 14. april 2026.[12]

[12] HubSpot Data Processing Agreement, senest ændret 14. april 2026, der inkorporerer EU-Kommissionens SKB 2021/914 Modul 3 og DPF-certificering. https://legal.hubspot.com/dpa

Underdatabehandler	Land / Jurisdiktion	Tjeneste / Rolle	Datakategorier	Overførselsmekanisme
		r); opbevarer kundekontaktoplysninger, engagementsnotater og mødemetadata		
Microsoft Corporation	USA (EU-datagrænse for M365)	Microsoft 365 — e-mail (Exchange Online), kalender, dokumentopbevaring (OneDrive, SharePoint), Microsoft Teams-møder	Personoplysninger i e-mails, dokumenter, kalenderinvitationer eller Teams-mødenoter relateret til et engagement	EU-US DPF + SKB (EU 2021/914, Modul 3). Microsoft M365 DBA april 2025.[13]

Bemærkninger: 1. Hvor en underdatabehandler tilbyder EU-baseret datacenter eller primær EU-behandling, og jeg har valgt EU-hosting, gælder SKB- og DPF-kolonnerne kun for resterende US-side-adgang (support, engineering). EU-behandling er primær for HubSpot (EU-datacenter valgt) og Microsoft 365 (EU-datagrænse). 2. Listen ovenfor er aktuel pr. underskrivelsesdatoen. Notion er ikke en underdatabehandler og er ikke i brug. Cal.com bruges ikke; PE-booking sker via HubSpot Meetings. Vercel (webhosting), Google Analytics, Google Ads og LinkedIn (annoncering / webanalyse) er besøgsdatabehandlere, der håndterer besøgstrafikdata, ikke engagement-personoplysninger, og er derfor oplyst i Privatlivspolitikken på `/privacy` snarere end i dette Bilag. Hvis en ny underdatabehandler engageres, tilføjes den under processen for ændringsvarsel i Punkt 7.5, før kundepersonoplysninger overføres. 3. Jeg anvender ingen underdatabehandler med henblik på salg, aggregering eller re-identifikation af personoplysninger. 4. **Status for fravalg af AI/ML-træning (jf. Punkt 7.11(b)):** HubSpot: jeg har fravalgt enhver AI-træning, der ville anvende kundeindhold; HubSpot's AI-funktioner behandler kundeindhold under kontraktuel fortrolighed. Microsoft: under Microsoft Online Services Terms og M365 DPA anvendes kundedata ikke til at træne AI/ML-modeller til Microsofts eget brug; jeg har fravalgt valgfri AI-funktioner, der ville behandle kundeindhold. Jeg genbekræfter disse fravalgsstatusser årligt som led i min

[13] Microsoft Online Services Data Protection Addendum (DPA), version april 2025. Tilgængelig på https://www.microsoft.com/licensing/docs. Dækker Exchange Online, OneDrive, SharePoint og Teams under SKB 2021/914 Modul 3 og EU-US DPF. Inkluderer EU-datagrænse-tilsagnet for M365-kunder med EU-baserede faktureringsadresser.

Bilag 3 §4.4-gennemgang. 5. **Værktøjer der ikke er underdatabehandlere.** Jeg anvender Apple Passwords (iCloud Keychain) til opbevaring af mine egne tjeneste-credentials; ingen kundepersonoplysninger behandles gennem dette værktøj. Jeg er aktivt i gang med at migrere credentials til passkey-baseret autentifikation, hvor det understøttes. Intet tredjepartsværktøj uden for de underdatabehandlere, der er anført ovenfor, behandler kundepersonoplysninger på mine vegne.

Bilag 3: Tekniske og Organisatoriske Foranstaltninger (TOF) efter GDPR Art. 32

Disse foranstaltninger udgør mit aktuelle, faktiske sikkerhedsgrundlag. De gennemgås mindst én gang årligt og opdateres efter et brud på persondatasikkerheden eller en væsentlig ændring.

1. Adgangskontrol

1.1 Multifaktor-autentifikation (MFA): Phishing-resistent MFA håndhæves på alle konti, der kan tilgå kundedata, ved brug af FIDO2-sikkerhedsnøgler eller platform-passkeys (kryptografiske adgangsnøgler bundet til min enhed, fx Apple Touch ID / Face ID, Windows Hello) som primær faktor, hvor det understøttes af tjenesten. Hvor en tjeneste endnu ikke understøtter phishing-resistente faktorer, anvendes time-based one-time passcodes (TOTP) som midlertidig foranstaltning med en dokumenteret migrationsplan. SMS-baseret og stemme-baseret MFA anvendes ikke. Specifikke konfigurationer:

- Microsoft 365 (Entra ID): passkey eller FIDO2-hardwarenøgle;
- HubSpot: TOTP via authenticator-app (midlertidigt, med passkey-migration sporet);
- Enhver cloud-konsol (AWS, Azure, GCP) tilgået under et engagement: phishing-resistent MFA hvor det understøttes, ellers TOTP.

MFA-omgåelsesmetoder (per-app-adgangskoder til ældre protokoller, gendannelseskoder der omgår MFA) er deaktiveret.

1.2 Håndtering af adgangsoplysninger: Alle mine adgangsoplysninger til tjenester (loginoplysninger og tilhørende hemmeligheder) opbevares i **Apple Passwords (iCloud Keychain)**, end-to-end-krypteret med Apples zero-knowledge-arkitektur. Ingen adgangskoder genbruges på tværs af tjenester. Genererede adgangskoder er minimum 20 tilfældige tegn. Jeg er aktivt i gang med at migrere mine adgangsoplysninger til **passkey-baseret autentifikation** (passwordless, phishing-resistent, kryptografisk adgangsnøgle bundet til min enhed), hvor tjenesteudbyderne understøtter det; det reducerer angrebsfladen for opbevaring af adgangsoplysninger over tid. Kundepersonoplysninger opbevares ikke i adgangsoplysningsmanageren, kun mine egne adgangsoplysninger til tjenester.

1.3 Mindste privilegium: Kundesystemer tilgås med de minimumsrettigheder, der kræves for den specifikke opgave. Privilegeret adgang (global admin, root) anvendes kun, hvor det er uundgåeligt, og sessionen dokumenteres i engagementsloggen.

1.4 Sessionshåndtering: Admin-sessioner afsluttes straks efter brug. Ingen vedvarende privilegerede sessioner opretholdes på tværs af engagementsopgaver.

2. Kryptering

2.1 Kryptering under transport: Al kommunikation mellem mig og kundesystemer anvender TLS 1.2 eller højere. Forbindelser, der ikke understøtter TLS 1.2+, anvendes ikke til overførsel af personoplysninger.

2.2 Kryptering i hvile, endpoint: Min primære arbejdsenhed er en Apple MacBook med **FileVault fuld diskkryptering (AES-256)** aktiveret. Enheden låses, når den er uden opsyn (auto-lås under 5 min), og kræver biometrisk (Touch ID) eller adgangskode-oplåsning. Ingen kundepersonoplysninger opbevares på bærbare flytbare medier (USB-drev, SD-kort) uden tilsvarende kryptering.

2.3 Kryptering i hvile, cloud-opbevaring: Dokumenter og filer med kundepersonoplysninger, der opbevares i cloud-tjenester, beskyttes af leverandørens kryptering i hvile (AES-256 eller tilsvarende), som dokumenteret i underdatabehandlerens DPA. Cloud-opbevaringens primære regioner er konfigureret til EU-regioner: HubSpot EU-datacenter; Microsoft 365 EU-datagrænse. Hvor en underdatabehandlers resterende funktioner (support, engineering, produkttelemetri) involverer US-side-adgang, er disse strømme dækket af overførselsmekanismerne i Punkt 9. Jeg opbevarer ikke primære kopier af dine personoplysninger uden for EØS uden dit forudgående skriftlige samtykke og en dokumenteret Transfer Impact Assessment efter Punkt 9.4.

2.4 E-mail: Kundepersonoplysninger overføres ikke via ukrypteret e-mail, hvor det kan undgås. Til overførsel af følsomme data (f.eks. eksporter fra adgangsgennemgange) anvender jeg adgangskodebeskyttede arkiver, sikre fildelingslinks (HubSpot file portal, Microsoft 365 / SharePoint / OneDrive eller tilsvarende) eller krypterede overførselsmetoder, alt efter omstændighederne.

3. Enhedssikkerhed

3.1 Administreret endpoint: Kun min egen administrerede enhed anvendes til engagementsarbejde. Kundedata behandles ikke på delte, personlige (ikke-arbejds-) eller uadministrerede enheder.

3.2 Automatisk skærmlås: Enheden låses automatisk efter 5 minutters inaktivitet.

3.3 Ingen kundedata på personlige enheder: Kundepersonoplysninger downloades ikke til eller opbevares på nogen personlig mobilenhed (telefon, personlig tablet). Det er et forbud, kryptering af en personlig enhed gør den ikke til et acceptabelt opbevaringssted for engagementsdata.

3.4 Fjernsletningsmulighed: Jeg opretholder mulighed for fjernsletning af den primære arbejdsenhed via Apple Find My eller tilsvarende MDM, så data kan slettes, hvis enheden mistes eller stjæles.

3.5 Operativsystem- og softwareopdateringer: Sikkerhedspatches anvendes inden for 14 dage efter udgivelsen for operativsystemet og primære arbejdsapplikationer.

4. Sikkerhedsovervågning og hændelsesdetektion

4.1 Sikkerhedslogning: Jeg opbevarer adgangslogs for cloud-tjenester (Microsoft 365 sign-in-logs, HubSpot aktivitetslogs) og gennemgår dem for unormal aktivitet. For engagementer klassificeret som høj-risiko i Bilag 1 (herunder alle NIS2-omfattede dataansvarlige og alle engagementer, der involverer mere end 500 registrerede), gennemføres logging-gennemgang mindst **dagligt**. For standard engagementer gennemføres logging-gennemgang mindst **ugentligt**.

4.2 Brud-bevidsthed: Jeg overvåger threat-intelligence-kilder relevante for de underdatabehandlere, der er anført i Bilag 2 (f.eks. HaveIBeenPwned for credentials-eksponering, leverandør-sikkerhedsbulletiner).

4.3 Hændelseshåndtering: Ved opdagelse af en mistænkt hændelse følger jeg processen i Punkt 11.2 (Inddæm; Anmeld inden for 24 timer for NIS2-dataansvarlige eller 48 timer for alle andre; Tilvejebring oplysninger; Dokumentér og samarbejd). En hændelseslog vedligeholdes internt.

4.4 Årlig sikkerhedsgennemgang: Jeg gennemfører en årlig gennemgang af disse TOF, hvor eventuelle ændringer og deres begrundelse dokumenteres. Gennemgangsdato og opsummerende fund er tilgængelige for dig på anmodning.

5. Dataminimering og opbevaring

5.1 Minimering ved indsamling: Jeg anmoder kun om de personoplysninger, der er strengt nødvendige for den aktuelle engagementsopgave. Dataeksporter fra kundesystemer afgrænses til de nødvendige felter.

5.2 Arbejdskopier: Arbejdskopier af kundedata (regneark, skærmbilleder, log-uddrag) opbevares kun i mit udpegede arbejdsmiljø (HubSpot / Microsoft 365 / cloud-opbevaring) og slettes eller tilbageleveres efter Punkt 15 ved engagementets afslutning.

5.3 Ingen skyggekopier: Jeg opretter ikke backup-kopier af kundepersonoplysninger i personlig e-mail, personlig cloud-opbevaring eller noget sted uden for det primære arbejdsmiljø.

6. Fysisk sikkerhed

6.1 Engagementsarbejde udføres fra mit registrerede kontor eller arbejdssted. Min primære arbejdsenhed efterlades ikke uden opsyn i offentlige rum med kundedata synlige på skærmen.

6.2 Fysiske dokumenter med kundepersonoplysninger (udskrifter, noter) opbevares sikkert og makuleres (krydsmakulering), når de ikke længere er nødvendige.

7. Personale og fortrolighed

7.1 Solo-praksis: Accel Comply er en enkeltmandsvirksomhed. Jeg er den eneste person, der behandler kundepersonoplysninger som led i den almindelige drift. Der er ingen fastansatte.

7.2 Særlige tilfælde: Hvis en afløser (f.eks. en underleverandør til barsels- eller sygdomsdækning) engageres under omstændigheder, hvor kundeadgang er uundgåelig, skal vedkommende underskrive en skriftlig fortrolighedsforpligtelse og bekræfte disse TOF, før der gives adgang. Du underrettes på forhånd.

7.3 Sikkerhedsbevidsthed: Jeg opretholder bevidsthed om aktuelle phishing-, social engineering- og BEC-trusler (Business Email Compromise) som led i den løbende faglige udvikling.

8. Sikkerhedstilsyn med underdatabehandlere

8.1 Før jeg engagerer en ny underdatabehandler, gennemgår jeg underdatabehandlerens offentligt tilgængelige sikkerhedsdokumentation (DPA, security whitepaper, certificeringer, f.eks. ISO 27001, SOC 2).

8.2 Jeg bekræfter, at hver underdatabehandler i Bilag 2 har enten ISO 27001-certificering, SOC 2 Type II-attestering eller tilsvarende, og at det forbliver gyldigt årligt.

9. Forsikring

9.1 Professionel ansvarsforsikring: DKK 5 mio. som standard. Højere dækningsgrænser kan anmodes om for relevante engagementer, forudsat forsikringsselskabets godkendelse og aftalt scope. Forsikringsselskabets navn, policenummer og dækningsgrænse er angivet i hvert Hovedaftale. Bevis for bunden dækning på det aftalte niveau leveres efter Punkt 16.3, før behandlingen påbegyndes.

Bilag 4: DORA-tillæg (kunder i finanssektoren)

Dette Bilag er gældende, hvor du er en finansiel enhed omfattet af DORA (Forordning (EU) 2022/2554), som trådte i anvendelse den 17. januar 2025. Det udgør en del af denne DBA fra datoen for underskrivelse.

A4.1 Omfang og formål

Dette Tillæg fastlægger de yderligere forpligtelser, jeg påtager mig, hvor du er en DORA-reguleret finansiel enhed, som krævet efter DORA Art. 28-30's kontraktkrav til IKT-tredjepartstjenesteudbydere.[14]

A4.2 Beskrivelse af tjenester og underentreprise

A4.2.1 De leverede IKT-tjenester er beskrevet i Bilag 1 til DBA'en og i Hovedaftalen. Alle ændringer i omfang dokumenteres ved skriftlig ændring af Bilag 1.

A4.2.2 Underentreprise. Jeg sætter ikke funktioner, der direkte understøtter dine kritiske eller vigtige forretningsfunktioner, i underentreprise uden din forudgående skriftlige godkendelse. Underdatabehandlere, der anvendes til operationelle værktøjer (CRM, e-mail, booking, som anført i Bilag 2), er forhåndsgodkendt under den generelle bemyndigelse i Punkt 7.5. Enhver underentreprise af substantielt rådgivningsarbejde kræver en separat skriftlig aftale mellem dig, mig og underleverandøren på vilkår, der mindst svarer til dette Tillæg.

A4.2.3 Jeg vedligeholder og stiller på anmodning til rådighed et register over underleverandører anvendt i forbindelse med dit engagement, med angivelse af funktion, land og gældende kontraktuelle sikringer.

A4.3 Ubegrænsede audit- og inspektionsrettigheder

A4.3.1 Du, enhver tredjepart du udpeger, og enhver kompetent myndighed (herunder Finanstilsynet og de europæiske tilsynsmyndigheder) har ubegrænsede rettigheder til adgang, inspektion og audit af mine forretningslokaler, systemer og dokumentation, der er relevante for de tjenester, der leveres under Hovedaftalen.

A4.3.2 Disse auditrettigheder er ikke underlagt den årlige hyppighedsbegrænsning i Punkt 12.3. Tilsynsmyndigheder kan udøve deres adgangsrettigheder uden forudgående varsel. Du kan udøve dine rettigheder med rimeligt varsel (minimum 5 arbejdsdage, medmindre der er rimelig grund til en tidligere anmodning).

A4.3.3 Jeg samarbejder fuldt ud og uden vederlag om enhver audit eller inspektion gennemført af dig eller en kompetent myndighed efter DORA Art. 30(2)(c).

A4.3.4 Jeg deltager i threat-led penetration testing (TLPT) øvelser, hvis du kræver det efter DORA Art. 26, med rimeligt varsel.

---

[14] Forordning (EU) 2022/2554 (DORA), i anvendelse fra 17. januar 2025. Art. 28-30 fastsætter kontraktkrav for IKT-tredjepartstjenesteudbydere. ESA'erne offentliggjorde de endelige RTS om IKT-tredjepartsrisiko (Forordning 2024/1773) den 17. januar 2025; Europa-Kommissionen afviste udkastet til RTS om underentreprise i januar 2025 på grund af omfangshensyn. Kontraktkravene i dette Tillæg afspejler DORA Art. 28-30 som de gælder; parterne bør følge ESA's tekniske standardudvikling. Se https://www.digital-operational-resilience-act.com/Article_30.html

A4.4 Opsigelse uden varsel ved kritisk misligholdelse

A4.4.1 Uanset Punkt 14.2 i denne DBA (som giver en 14-dages afhjælpningsperiode), kan du opsige Hovedaftalen og denne DBA med øjeblikkelig virkning ved skriftlig meddelelse, uden afhjælpningsperiode, i en af følgende situationer:

(a) Jeg begår en væsentlig misligholdelse af DORA, GDPR eller anden gældende finanssektorregulering, der berører sikkerheden eller integriteten af dine IKT-systemer eller data;

(b) En kompetent myndighed udsteder en bindende afgørelse eller pålæg, der gør fortsat opfyldelse umulig eller ulovlig;

(c) Jeg viser væsentlige svagheder i min IKT-risikohåndtering, som jeg ikke kan afhjælpe inden for en frist, du med rimelighed fastsætter;

(d) Min fortsatte drift som IKT-tredjepartstjenesteudbyder er uforenelig med dine regulatoriske forpligtelser, som fastslået af dig eller en kompetent myndighed.

A4.4.2 Øjeblikkelig opsigelse efter denne bestemmelse berører ikke nogen påløbne rettigheder eller forpligtelserne i Punkt 14.4 og 15.

A4.5 Exit- og overgangsbistand

A4.5.1 Efter opsigelse eller udløb af Hovedaftalen af enhver grund vil jeg yde overgangsbistand i en periode på mindst **60 dage** (kan forlænges efter skriftlig aftale) for at understøtte en velordnet migration af tjenester til dig eller en alternativ leverandør. Overgangsbistand omfatter:

(a) Fortsat tilgængelighed af alle leverancer fra engagementet, arbejdsdokumenter og data i et maskinlæsbart format;

(b) Vidensoverdragelse og dokumentation af metoder, fund og igangværende arbejde;

(c) Rimeligt samarbejde med din alternative leverandør, herunder besvarelse af tekniske spørgsmål;

(d) Tilbagelevering eller sletning af dine personoplysninger som krævet i Punkt 15.

Denne exit- og overgangsbistand ydes efter DORA Art. 30(2)'s kontraktkrav, som kræver, at IKT-tredjepartsudbyderkontrakter indeholder bestemmelser, der understøtter den finansielle enheds exit-forpligtelser efter Art. 28(7) og (8).

A4.5.2 Du bærer omkostningen til overgangsbistand, der strækker sig ud over 60 dage, til en dagsats aftalt i Hovedaftalen. Overgangsbistand inden for de første 60 dage er inkluderet i engagementshonoraret.

A4.6 Datagenoprettelse og kontinuitet

A4.6.1 Jeg implementerer og tester forretningskontinuitetsplaner, der dækker de IKT-tjenester, jeg leverer til dig. På anmodning gør jeg en oversigt over disse planer tilgængelig for dig.

A4.6.2 For ethvert engagement under dette Tillæg skal Hovedaftalen udpege en overdragelseskontakt (en Stedfortræder efter Punkt 7.4(c)). Udpegning af en overdragelseskontakt er en forudsætning for ethvert DORA-reguleret engagement under dette Tillæg. Hvis jeg bliver insolvent, ude af stand til at arbejde eller ophører med at drive virksomhed, opbevares alle data, der behandles på dine vegne under denne DBA, på steder, du kan tilgå uafhængigt, eller stilles til rådighed for dig inden for **24 timer** efter skriftlig anmodning til den udpegede overdragelseskontakt.

A4.6.3 Jeg deltager i dine tests af forretningskontinuitets- og beredskabsplaner med rimeligt varsel, uden ekstra omkostninger.

A4.7 Hændelsesrapportering til finansielle tilsynsmyndigheder

A4.7.1 For DORA-omfattede engagementer vil Accel Comply gøre sit bedste for at underrette kunden om en IKT-relateret hændelse, der påvirker de aftalte ydelser, inden for forretningstider tilpasset hændelsens alvor og det aftalte engagement-scope. Konkrete underretningsvinduer fastlægges per Statement of Work. Formålet er at give dig arbejdstid til at vurdere situationen og, hvor det er påkrævet, indgive din egen Art. 19-hændelsesrapport til Finanstilsynet, inden din regulatoriske frist udløber. Hvor jeg midlertidigt er utilgængelig (søvn, rejse, planlagt fri), sker underretning, så snart jeg er i stand til at rette opmærksomhed mod det. Forretningskontinuitetsbestemmelserne i Punkt 7.4 gælder, hvis jeg er utilgængelig i en længere periode.

A4.7.2 Underretningen efter A4.7.1 vil i det omfang, det er kendt, indeholde: en beskrivelse af hændelsen, berørte systemer, anslået indvirkning og de inddæmningsskridt, der er taget. Suppleringer følger, så snart yderligere oplysninger er tilgængelige.

A4.7.3 Jeg samarbejder med enhver undersøgelse foretaget af Finanstilsynet eller anden kompetent myndighed som følge af en IKT-hændelse, herunder ved at levere dokumentation og adgang på anmodning.

A4.8 Informationssikkerhedsstandarder

A4.8.1 Jeg forpligter mig til at opretholde informationssikkerhedsstandarder i overensstemmelse med DORA Art. 9's IKT-risikohåndteringskrav under ethvert engagement med en DORA-reguleret enhed, proportionalt med tjenesternes karakter, omfang og kompleksitet, herunder kontroller, der dækker fortrolighed, integritet, tilgængelighed og autentifikation.

A4.8.2 Jeg leverer på anmodning bevis for min aktuelle sikkerhedsstilling (f.eks. egenattestering, relevante certificeringer) og underretter dig straks om enhver væsentlig forværring.

A4.9 Register over IKT-tredjepartsarrangementer

Jeg anerkender, at du er forpligtet til at vedligeholde et Informationsregister (RoI) over IKT-tredjepartsarrangementer efter DORA Art. 28(2) og at gøre disse oplysninger tilgængelige for kompetente myndigheder efter Art. 28(3). Jeg leverer de obligatoriske datafelter, der kræves efter Kommissionens delegerede forordning (EU) 2024/1771 (RoI ITS), for din RoI-post vedrørende dette engagement inden for 10 arbejdsdage efter skriftlig anmodning, ved hjælp af arbejdsarket i §A4.10 nedenfor.

A4.10 Informationsregister — per-engagement-arbejdsark

Efter DORA Art. 28(2) og Kommissionens delegerede forordning (EU) 2024/1771 vedligeholder du et Informationsregister over IKT-tredjepartsordninger. Nedenstående tabel indeholder de obligatoriske felter for posten vedrørende dette engagement. Felter markeret [FÆLLES] udfyldes i fællesskab af dig og mig ved engagementets start.

RoI-felt	Obligatorisk efter EU 2024/1771	Værdi for dette engagement
Intern referencenummer	Ja	[TILDELES AF DIG]
Navn på IKT-tredjepartstjenesteudbyder	Ja	Accel Comply / Behzad Motaghi, CVR DK37260312
Etableringsland	Ja	Danmark
LEI-kode (hvis relevant)	Ja	Ikke relevant (enkeltmandsvirksomhed, ingen LEI)
IKT-tjenestekategori (jf. Bilag I, EU 2024/1771)	Ja	[FÆLLES — typisk: IT-rådgivning / sikkerhedskonsultation]
Understøttet funktion (kritisk eller vigtig?)	Ja	[FÆLLES — klassificeres af dig: er NIS2/ISO-rådgivningsfunktionen kritisk eller vigtig for din drift?]
Vurdering af substituerbarhed	Ja	[FÆLLES — enkeltmandsvirksomhed; kan substitueres med moderat indsats; efterfølgermekanisme i Punkt 7.4(c)]

RoI-felt	Obligatorisk efter EU 2024/1771	Værdi for dette engagement
Koncentrationsrisikoindikator	Ja	[FÆLLES — lav (enkeltmandsvirksomhed; ingen systemisk koncentrationseksponering)]
Startdato for aftale	Ja	[DATO FOR HOVEDAFTALEN]
Datafølsomhedsklassificering	Ja	[FÆLLES — typisk: fortrolig / begrænset intern; ingen kritisk infrastrukturdata]
Anvendte underleverandører	Ja	HubSpot (USA), Microsoft (USA/EU-datagrænse), se Bilag 2. Ingen underentreprise af rådgivningsfunktioner uden forudgående godkendelse jf. §A4.2.2.
Dataopbevaringssted	Ja	EU (HubSpot EU-region; Microsoft 365 EU-datagrænse)

Jeg leverer alle yderligere oplysninger, der er nødvendige for at udfylde din RoI-post, inden for 10 arbejdsdage efter skriftlig anmodning, herunder opdaterede underleverandøroplysninger og eventuelle ændringer af ovenstående felter under engagementet.

Bilag 5: UK-overførselstillæg

Dette Bilag er gældende, hvor du er omfattet af UK GDPR, dvs. hvor du er etableret i Storbritannien, eller hvor personoplysninger om personer bosiddende i Storbritannien behandles under denne DBA. Det aktiveres automatisk, når en af parterne identificerer, at britiske personoplysninger er omfattet; ingen yderligere instruks er påkrævet.

A5.1 UK-overførselsmekanisme

A5.1.1 For enhver overførsel af britiske personoplysninger til underdatabehandlere anført i Bilag 2, der er etableret uden for Storbritannien (herunder USA-baserede underdatabehandlere), er den gældende UK-overførselsmekanisme **International Data**

Transfer Addendum to the EU Commission Standard Contractual Clauses udstedt af UK Information Commissioner's Office (ICO) efter s.119A i Data Protection Act 2018 ("UK Addendum").[15]

A5.1.2 UK Addendum inkorporeres hermed ved henvisning i denne DBA. Parterne er enige om, at denne DBA inkorporerer **Part 2: Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of those Mandatory Clauses**. Hvor ICO udsteder et revideret Approved Addendum efter Section 18, opdateres denne DBA automatisk for at inkorporere den revision uden at kræve ændring af parterne. Parterne er endvidere enige om, at:

(a) EU SKB inkorporeret i denne DBA (Punkt 9 og Bilag 2) ændres ved UK Addendum til at dække UK-restricted overførsler;

(b) For så vidt angår Tabel 1 i UK Addendum: Eksportøren er Accel Comply (som Databehandler, der handler efter dine instrukser), og Importøren er den relevante underdatabehandler som anført i Bilag 2;

(c) For så vidt angår Tabel 2: UK Addendum supplerer EU SKB, Kommissionens afgørelse (EU) 2021/914, Modul 3 (Databehandler til underdatabehandler);

(d) For så vidt angår Tabel 3: beskrivelsen af overførsler er som fastsat i Bilag 1 og Bilag 2 til denne DBA;

(e) For så vidt angår Tabel 4: ingen af parterne kan opsige UK Addendum som fastsat i Section 19 i UK Addendum. Dette valg er i overensstemmelse med Punkt 9.7 i denne DBA, som foreskriver automatisk indarbejdelse af opdaterede SKB og tillæg: hvis ICO udsteder et revideret Approved Addendum, og den automatiske opdateringsmekanisme i §A5.1.2 indarbejder det, er der intet grundlag for opsigelse alene af den grund. Begge parter bevarer retten til at opsige Hovedaftalen på de grunde, der er angivet i Punkt 14.2, hvis et revideret tillæg pålægger væsentligt anderledes forpligtelser, som den anden part ikke kan acceptere.

---

[15] International Data Transfer Addendum to the EU Commission Standard Contractual Clauses, udstedt af UK ICO efter s.119A i Data Protection Act 2018, version B.1.0, i kraft 21. marts 2022. Fra 21. marts 2024 skal britiske organisationer anvende enten UK IDTA eller UK Addendum (sammen med EU SKB) for UK-restricted overførsler; overgangsperioden for ældre SKB sluttede på den dato. Part 2 Mandatory Clauses inkorporeres ved henvisning efter ICO's godkendte alternative referenceformulering i A5.1.2 og opdateres automatisk efter Section 18. Se https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/international-transfers/appropriate-safeguards/what-are-standard-data-protection-clauses-the-uk-idta-and-the-addendum/