Databehandleraftale for Ri's ydelser

1. Indledning, baggrund og anvendelsesområde

1.1. Denne databehandleraftale („aftalen") regulerer Ri Statsautoriseret Revisionspartnerselskabs (Ri eller databehandleren) behandling af personoplysninger på vegne af kunden (den dataansvarlige) i overensstemmelse med Europa-Parlamentets og Rådets forordning (EU) 2016/679 (GDPR) artikel 28.

1.2. Aftalen finder anvendelse på de ydelser, hvor den dataansvarlige overlader personoplysninger til Ri med henblik på behandling efter den dataansvarliges dokumenterede instruks – eksempelvis outsourcing af bogføring, lønadministration, regnskabsmæssig assistance uden erklæring eller hosting af kundens data hos Ri.

1.3. Aftalen finder ikke anvendelse på lovpligtige revisioner og andre erklærings- eller attestationsopgaver, eller hvor Ri i øvrigt udfører ydelser i kraft af selvstændige professionelle pligter (f.eks. efter revisorloven, hvidvaskloven og kvalitetsstyringsstandarderne). Ved sådanne ydelser er Ri selvstændig dataansvarlig for de personoplysninger, der behandles som led i opgaven, og en databehandleraftale er hverken påkrævet eller relevant, uanset at behandlingen måtte omfatte personoplysninger om fysiske personer, herunder CPR-numre.

1.4. I tilfælde af uoverensstemmelse mellem databehandleraftalen og det øvrige aftalegrundlag (aftalebrev og Ri's forretningsbetingelser) har databehandleraftalens bestemmelser om behandling af personoplysninger forrang for den behandling, som aftalen omfatter, jf. punkt 1.2.

1.5. Aftalen frigør ikke databehandleren for forpligtelser, som efter GDPR eller anden lovgivning direkte er pålagt databehandleren.

2. Definitioner

2.1. Ord og udtryk anvendt i aftalen har den betydning, der følger af GDPR artikel 4, herunder personoplysninger, behandling, særlige kategorier af personoplysninger, brud på persondatasikkerheden, dataansvarlig, databehandler og underdatabehandler.

2.2. Ved hovedydelsen forstås de ydelser, som Ri leverer til den dataansvarlige efter aftalebrev og Ri's forretningsbetingelser, og som forudsætter, at Ri behandler personoplysninger på den dataansvarliges vegne, og som udelukkende vedrører de ydelser, hvor Ri handler som databehandler, jf. punkt 1.2.

3. Den dataansvarliges rettigheder og forpligtelser

3.1. Den dataansvarlige er over for omverdenen (herunder de registrerede) ansvarlig for, at behandlingen sker inden for rammerne af GDPR og databeskyttelsesloven.

3.2. Den dataansvarlige har retten og forpligtelsen til at træffe beslutning om, til hvilke formål og med hvilke hjælpemidler behandlingen må foretages, og indestår for, at der foreligger lovligt behandlingsgrundlag, og at de registrerede har modtaget de fornødne oplysninger efter GDPR artikel 13 og 14.

3.3. Den dataansvarlige indestår for, at oplysninger, der overdrages til databehandleren, må videregives og behandles til de aftalte formål.

4. Databehandleren handler efter instruks

4.1. Databehandleren må kun behandle personoplysninger efter dokumenteret instruks fra den dataansvarlige, medmindre EU-retten eller medlemsstaternes nationale ret kræver behandling. I så fald underretter databehandleren den dataansvarlige om dette retlige krav inden behandling, medmindre den pågældende ret forbyder en sådan underretning af hensyn til vigtige samfundsmæssige interesser.

4.2. Den dataansvarliges oprindelige instruks fremgår af bilag A og C. Mindre, ikke-væsentlige ændringer i instruksen kan meddeles skriftligt – herunder pr. e-mail – mellem parternes kontaktpersoner.

4.3. Databehandleren underretter omgående den dataansvarlige, hvis en instruks efter databehandlerens vurdering er i strid med GDPR eller anden gældende databeskyttelsesregulering.

5. Fortrolighed

5.1. Databehandleren sikrer, at kun personer, der aktuelt er autoriseret hertil, har adgang til de personoplysninger, der behandles på vegne af den dataansvarlige. Adgangen lukkes straks ned, hvis autorisationen fratages eller udløber.

5.2. Adgang gives alene til personer, for hvem det er nødvendigt at have adgang for at kunne opfylde databehandlerens forpligtelser over for den dataansvarlige (need-to-know-princippet).

5.3. Databehandleren sikrer, at autoriserede personer har påtaget sig fortrolighedsforpligtelse eller er underlagt en passende lovbestemt tavshedspligt. Ri's partnere og medarbejdere er underlagt revisorlovens skærpede tavshedspligt.

6. Behandlingssikkerhed

6.1. Databehandleren gennemfører passende tekniske og organisatoriske foranstaltninger som krævet af GDPR artikel 32, så behandlingen opfylder kravene i forordningen og beskytter de registreredes rettigheder.

6.2. En overordnet beskrivelse af de implementerede foranstaltninger fremgår af bilag C, punkt C.2. Foranstaltningernes konkrete udmøntning er beskrevet i databehandlerens interne IT- og informationssikkerhedspolitik, der ikke udleveres som en del af aftalen.

6.3. Hvis behandlingen kræver yderligere foranstaltninger end dem, der er beskrevet i bilag C, aftales dette skriftligt mellem parterne, herunder eventuelt vederlag herfor.

7. Anvendelse af underdatabehandlere

7.1. Databehandleren har den dataansvarliges generelle godkendelse til at gøre brug af underdatabehandlere, jf. listen i bilag B. Databehandleren skal opfylde betingelserne i GDPR artikel 28, stk. 2 og stk. 4, herunder pålægge underdatabehandleren databeskyttelsesforpligtelser, der ikke er mindre byrdefulde end aftalens.

7.2. Databehandleren underretter skriftligt den dataansvarlige om planlagte ændringer (tilføjelse eller udskiftning) af underdatabehandlere mindst 30 kalenderdage forud for ændringen, så den dataansvarlige har mulighed for at gøre indsigelse. Indsigelse skal være saglig og begrundet i databeskyttelsesretlige forhold og fremsættes inden 14 kalenderdage. Underretning kan ske via e-mail og/eller offentliggørelse på www.ri.dk.

7.3. Hvis parterne ikke kan blive enige om en løsning, kan hver part opsige aftalen og den berørte Hovedydelse med rimeligt varsel, dog ikke længere end 60 kalenderdage.

7.4. Hvis underdatabehandleren ikke opfylder sine databeskyttelsesforpligtelser, forbliver databehandleren fuldt ansvarlig over for den dataansvarlige for opfyldelsen af underdatabehandlerens forpligtelser.

8. Overførsel til tredjelande

8.1. Databehandleren overfører ikke personoplysninger til tredjelande eller internationale organisationer uden dokumenteret instruks fra den dataansvarlige. Som udgangspunkt sker behandlingen udelukkende inden for EU/EØS, jf. bilag B.

8.2. Hvis instruks om overførsel gives, sker overførslen kun på et lovligt grundlag efter GDPR kapitel V (eksempelvis tilstrækkelighedsafgørelse efter artikel 45 eller standardkontraktbestemmelser efter artikel 46) suppleret med eventuelle nødvendige supplerende foranstaltninger.

8.3. Aftalen udgør ikke standardkontraktbestemmelser efter GDPR artikel 46, stk. 2, litra c og d, og kan ikke i sig selv danne grundlag for overførsel til tredjelande.

9. Bistand til den dataansvarlige

9.1. Databehandleren bistår – i det omfang det er relevant for den konkrete behandling – den dataansvarlige med at opfylde den dataansvarliges forpligtelser efter GDPR, herunder:

- besvarelse af anmodninger om udøvelse af de registreredes rettigheder efter GDPR kapitel III,
- anmeldelse af brud på persondatasikkerheden til Datatilsynet og underretning af registrerede, jf. GDPR artikel 33-34,
- udarbejdelse af konsekvensanalyser (DPIA) og forudgående høring efter GDPR artikel 35-36, hvor det er relevant for behandlingen.

9.2. Bistanden honoreres efter Ri's til enhver tid gældende timesatser, medmindre andet aftales eller medmindre bistanden er nødvendiggjort af forhold, som databehandleren bærer ansvaret for.

10. Underretning om brud på persondatasikkerheden

10.1. Databehandleren underretter uden unødig forsinkelse den dataansvarlige efter at være blevet opmærksom på, at der er sket et brud på persondatasikkerheden hos databehandleren eller en underdatabehandler, så den dataansvarlige har mulighed for at efterleve sin forpligtelse til at anmelde bruddet til Datatilsynet inden for 72 timer.

10.2. Underretningen skal i det omfang, det er muligt, indeholde beskrivelse af bruddet (herunder kategorier og omtrentligt antal berørte registrerede og berørte registreringer), kontaktoplysninger på en kontaktperson, sandsynlige konsekvenser samt trufne eller foreslåede foranstaltninger. Hvor det ikke er muligt at give alle oplysninger samlet, kan oplysningerne meddeles trinvist uden unødig yderligere forsinkelse.

11. Sletning og tilbagelevering ved aftalens ophør

11.1. Ved ophør af de tjenester, aftalen omfatter, sletter eller tilbageleverer databehandleren – efter den dataansvarliges valg – alle personoplysninger til den dataansvarlige og sletter herefter eksisterende kopier, medmindre EU-retten eller national ret kræver fortsat opbevaring.

11.2. Ri kan være forpligtet til at opbevare oplysninger ud over aftalens ophør i medfør af bogføringsloven, hvidvaskloven, revisorloven samt skatte- og afgiftslovgivningen. I så fald opbevares oplysningerne alene til de(t) lovbestemte formål og i den lovbestemte periode.

11.3. Sletning eller tilbagelevering sker uden unødig forsinkelse og senest 60 kalenderdage efter den dataansvarliges anmodning. Databehandleren bekræfter sletningen skriftligt over for den dataansvarlige.

12. Tilsyn

12.1. Den dataansvarlige har ret til – efter rimeligt skriftligt varsel – at modtage dokumentation for databehandlerens efterlevelse af aftalen og GDPR. Dokumentationen kan eksempelvis bestå af generelle auditrapporter, sikkerhedsbeskrivelser eller besvarelse af et leverandør-spørgeskema.

12.2. Den dataansvarlige eller en bemyndiget repræsentant kan – efter skriftligt varsel på mindst 30 kalenderdage og maksimalt én gang årligt – foretage et rimeligt fysisk tilsyn hos databehandleren. Tilsynet skal gennemføres uden gene for databehandlerens øvrige drift, og den dataansvarliges dokumenterede omkostninger samt databehandlerens tidsforbrug afregnes efter Ri's til enhver tid gældende timesatser, medmindre væsentlige misligholdelsesforhold konstateres.

12.3. Databehandleren er forpligtet til at give offentlige myndigheder, der efter lovgivningen har adgang, fornøden adgang mod behørig legitimation.

13. Aftalens ophør og lovvalg

13.1. Aftalen træder i kraft ved parternes underskrift og er gældende, så længe databehandleren behandler personoplysninger på den dataansvarliges vegne. Aftalen kan opsiges af begge parter med rimeligt varsel, dog således at aftalen forbliver i kraft frem til behandlingens ophør og oplysningernes sletning eller tilbagelevering, jf. punkt 11.

13.2. Ændringer i aftalen aftales skriftligt mellem parterne. Begge parter kan kræve aftalen genforhandlet, hvis lovændringer eller forhold i øvrigt giver anledning hertil.

13.3. Aftalen er undergivet dansk ret, og enhver tvist afgøres ved de danske domstole med Ri's hjemsted som værneting.

Bilag A – Behandlingens karakter, formål og kategorier

A.1 Formål og karakter

Databehandleren behandler personoplysninger på vegne af den dataansvarlige med henblik på at levere de aftalte ydelser i henhold til aftalebrev og Ri's forretningsbetingelser, jf. aftalens punkt 1.2. Behandlingen kan – afhængigt af den konkrete ydelse – omfatte indsamling, registrering, organisering, opbevaring, søgning, tilpasning, brug, sammenstilling, videregivelse, sletning og tilintetgørelse.

A.2 Kategorier af registrerede

Behandlingen kan – afhængigt af ydelsen – omfatte oplysninger om:

- Den dataansvarliges medarbejdere, herunder tidligere medarbejdere.
- Den dataansvarliges medlemmer, kontingentbetalere, frivillige, beboere eller andre tilknyttede fysiske personer (relevant for f.eks. fagforeninger, foreninger, fonde, partier, almene boligorganisationer, andelsbolig- og ejerforeninger).
- Den dataansvarliges kunder, debitorer, kreditorer, leverandører og samarbejdspartnere samt disses kontaktpersoner.
- Den dataansvarliges bestyrelsesmedlemmer, ledelse, ejere og reelle ejere.
- Andre fysiske personer, der måtte fremgå af det materiale, som den dataansvarlige overlader til databehandleren med henblik på Hovedydelsen.

A.3 Typer af personoplysninger

Behandlingen kan – afhængigt af ydelsen – omfatte:

- Almindelige personoplysninger (GDPR artikel 6), herunder identifikations-, kontakt-, ansættelses-, løn-, betalings- og medlemsoplysninger.
- Personnummer (CPR), hvor dette er nødvendigt af hensyn til lønadministration, skatteindberetning eller anden lovbestemt behandling, jf. databeskyttelseslovens § 11.
- I begrænset omfang særlige kategorier af personoplysninger (GDPR artikel 9) og oplysninger om strafbare forhold (GDPR artikel 10), hvor dette er nødvendigt og lovligt for ydelsen.

A.4 Behandlingens varighed

Behandlingen er ikke tidsbegrænset og varer, indtil aftalen om Hovedydelsen ophører, og oplysningerne herefter er slettet eller tilbageleveret i overensstemmelse med aftalens punkt 11.

Bilag B – Godkendte underdatabehandlere

Den dataansvarlige godkender ved aftalens ikrafttræden, at databehandleren anvender følgende kategorier af underdatabehandlere til de behandlingsaktiviteter, aftalen omfatter:

Underdatabehandler	Ydelse	Lokation
Microsoft	Cloud-drift, e-mail, fildeling og identitetsstyring	EU/EØS
IT-driftspartner	Drift, overvågning og support af Ri's IT-infrastruktur	EU/EØS
Dokumenthåndteringsleverandør	Sags- og dokumenthåndteringssystem	EU/EØS
Lønsystem-leverandør	Lønadministration (kun ved aftalt lønbehandling)	EU/EØS
Underskriftsleverandør	Elektronisk underskrift af dokumenter	EU/EØS
Mailsikkerheds- og arkiveringsleverandør	Sikker e-mail, kryptering og lovpligtig arkivering	EU/EØS
AI-værktøjer	Sprogmodel-baserede hjælpeværktøjer til tekstudarbejdelse, opsummering og analyse	EU/EØS

Ri har indgået gyldige underdatabehandleraftaler med ovenstående underdatabehandlere i overensstemmelse med GDPR artikel 28. En aktuel og navngiven oversigt over de konkrete underdatabehandlere kan rekvireres ved henvendelse til support@ri.dk.

Ingen yderligere underdatabehandlere benyttes uden forudgående underretning, jf. aftalens punkt 7.2.

Bilag C – Instruks og sikkerhedsforanstaltninger

C.1 Instruks

Databehandlerens behandling sker som beskrevet i bilag A med henblik på levering af hovedydelsen i overensstemmelse med aftalebrev og Ri's forretningsbetingelser. Den oprindelige instruks omfatter:

- indsamling og modtagelse af personoplysninger fra den dataansvarlige,
- opbevaring og behandling i databehandlerens systemer og hos de godkendte underdatabehandlere,
- videregivelse til myndigheder eller tredjeparter efter den dataansvarliges instruks eller efter lovkrav,
- tilbagelevering eller sletning ved aftalens ophør, jf. punkt C.3.

C.2 Tekniske og organisatoriske foranstaltninger

Databehandleren vedligeholder et informationssikkerhedsniveau i overensstemmelse med GDPR artikel 32. De implementerede foranstaltninger omfatter blandt andet:

- Organisatoriske rammer: ledelsessystem for informationssikkerhed med formelle ansvarsområder, fortrolighedsforpligtelse for medarbejdere samt awareness-træning ved ansættelse og løbende.
- Adgangsstyring: rollebaserede adgangsrettigheder efter need-to-know, autorisation efter arbejdsbehov samt straks-lukning af adgang ved fratrædelse.
- Datasikkerhed: kryptering af følsomme data under overførsel og hvile, hvor det er relevant, samt klassifikation og fortrolig behandling af kundedata.
- Netværks- og endpoint-sikkerhed: firewalls, antivirus, patch-management, begrænsede lokale administratorrettigheder (application control) samt logning af relevante systemhændelser.
- Backup og driftskontinuitet: regelmæssig backup, beredskabsprocedurer og testede gendannelsesrutiner.
- Hændelseshåndtering: procedurer for håndtering, vurdering og rapportering af brud på persondatasikkerheden, jf. aftalens punkt 10.
- Anvendelse af AI-værktøjer: Kundedata behandles ikke i uautoriserede AI-tjenester. Eventuel anvendelse af AI sker under databehandlerens fulde kontrol og i overensstemmelse med gældende databeskyttelsesregler.

Den konkrete udmøntning af foranstaltningerne fremgår af Ri's interne IT-sikkerhedspolitik. Denne udleveres ikke som en del af aftalen, men en overordnet redegørelse kan rekvireres efter rimeligt varsel, jf. aftalens punkt 12.

C.3 Sletning og tilbagelevering ved ophør

Ved ophør af tjenesterne sletter eller tilbageleverer databehandleren personoplysningerne efter den dataansvarliges valg, jf. aftalens punkt 11. Bekræftelse af sletning sker skriftligt over for den dataansvarlige inden for 30 kalenderdage efter, at sletningen er gennemført. Lovbestemte opbevaringsperioder, jf. punkt 11.2, respekteres.

C.4 Lokation

Behandlingen sker på Ri's kontorer i Danmark og hos de godkendte underdatabehandleres lokationer i EU/EØS, jf. bilag B. Hjemmearbejde for Ri's medarbejdere kan ske på vilkår fastsat i Ri's interne IT-sikkerhedspolitik.

C.5 Tredjelandsoverførsler

Der overføres ikke personoplysninger til tredjelande uden dokumenteret instruks fra den dataansvarlige, jf. aftalens punkt 8. Manglende instruks udgør et forbud mod overførsel.