Databehandleraftale

Mellem

Den dataansvarlige:

CVR:

og

Databehandleren:

ReindexKnowledge ApS

CVR 34472300

Fruebjergvej 3

2100 København Ø

Danmark

Den dataansvarlige og databehandleren er hver især en "part", og sammen udgør de "parterne".

Parterne har aftalt følgende standardkontraktbestemmelser (Bestemmelserne) med henblik på at overholde databeskyttelsesforordningen og sikre beskyttelse af privatlivets fred og fysiske personers grundlæggende rettigheder og frihedsrettigheder.

1 Baggrund for databehandleraftalen

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

2. Disse bestemmelser er udformet med henblik på parternes efterlevelse af artikel 28, stk. 3, i Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (databeskyttelsesforordningen).

3. I forbindelse med leveringen af Reindex bibliotekstjenester behandler databehandleren personoplysninger på vegne af den dataansvarlige i overensstemmelse med disse Bestemmelser.

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

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

6. Bilag A indeholder nærmere oplysninger om behandlingen af personoplysninger, herunder om behandlingens formål og karakter, typen af personoplysninger, kategorierne af registrerede og varighed af behandlingen.

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

8. Bilag C indeholder den dataansvarliges instruks for så vidt angår databehandlerens behandling af personoplysninger, en beskrivelse af de sikkerhedsforanstaltninger, som databehandleren som minimum skal gennemføre, og hvordan der føres tilsyn med databehandleren og eventuelle underdatabehandlere.

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

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

2 Den dataansvarliges forpligtelser og rettigheder

1. Den dataansvarlige er ansvarlig for at sikre at behandlingen af personoplysninger sker i overensstemmelse med databeskyttelsesforordningen (se forordningens artikel 24), databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser. Henvisninger til "medlemsstat" i disse bestemmelse skal forstås som en henvisning til "EØS medlemsstater".

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

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

3 Databehandleren handler efter instruks

1. Databehandleren må kun behandle personoplysninger efter dokumenteret instruks fra den dataansvarlige, medmindre det kræves i henhold til EU-ret eller medlemsstaternes nationale ret, som databehandleren er underlagt. Denne instruks skal være specificeret i bilag A og C. Efterfølgende instruks kan også gives af den dataansvarlige, mens der sker behandling af personoplysninger, men instruksen skal altid være dokumenteret og opbevares skriftligt, herunder elektronisk, sammen med disse Bestemmelser.

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

4 Fortrolighed

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

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

5 Behandlingssikkerhed

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

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

   a. Pseudonymisering og kryptering af personoplysninger

b. Evne til at sikre vedvarende fortrolighed, integritet, tilgængelighed og robusthed af behandlingssystemer og -tjenester

c. Evne til rettidigt at genoprette tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse

d. En procedure for regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske foranstaltninger til sikring af behandlingssikkerhed.

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

3. Derudover skal databehandleren bistå den dataansvarlige med vedkommendes overholdelse af den dataansvarliges forpligtelse efter forordningens artikel 32, ved bl.a. at stille den nødvendige information til rådighed for den dataansvarlige vedrørende de tekniske og organisatoriske sikkerhedsforanstaltninger, som databehandleren allerede har gennemført i henhold til forordningens artikel 32, og al anden information, der er nødvendig for den dataansvarliges overholdelse af sin forpligtelse efter forordningens artikel 32.

   Hvis imødegåelse af de identificerede risici – efter den dataansvarliges vurdering – kræver gennemførelse af yderligere foranstaltninger end de foranstaltninger, som databehandleren allerede har gennemført, skal den dataansvarlige angive de yderligere foranstaltninger, der skal gennemføres, i bilag C.

6 Anvendelse af underdatabehandlere

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

2. Databehandleren må således ikke gøre brug af en underdatabehandler til opfyldelse af disse Bestemmelser uden forudgående godkendelse fra den dataansvarlige. Godkendelse sker ved indgåelse af denne aftale og ved instruks fra dataansvarlig til databehandler vedrørende brug af konkrete funktioner der involverer underdatabehandlere i den daglige biblioteksforretning.

3. Databehandleren har den dataansvarliges generelle godkendelse til brug af underdatabehandlere. Databehandleren skal skriftligt underrette den dataansvarlige om eventuelle planlagte ændringer vedrørende tilføjelse eller udskiftning af underdatabehandlere med mindst 30 dages varsel og derved give den dataansvarlige mulighed for at gøre indsigelse mod sådanne ændringer inden brugen af de(n) omhandlede underdatabehandler(e). Længere varsel for underretning i forbindelse med specifikke behandlingsaktiviteter kan angives i bilag B. Listen over underdatabehandlere som den dataansvarlige allerede har godkendt, fremgår af bilag B.

4. Når databehandleren gør brug af en underdatabehandler i forbindelse med udførelse af specifikke behandlingsaktiviteter på vegne af den dataansvarlige, skal databehandleren, gennem en kontrakt eller andet retligt dokument i henhold til EU-retten eller medlemsstaternes nationale ret, pålægge

underdatabehandleren de samme databeskyttelsesforpligtelser som dem, der fremgår af disse Bestemmelser, hvorved der navnlig stilles de fornødne garantier for, at underdatabehandleren vil gennemføre de tekniske og organisatoriske foranstaltninger på en sådan måde, at behandlingen overholder kravene i disse Bestemmelser og databeskyttelsesforordningen.

Databehandleren er derfor ansvarlig for at kræve, at underdatabehandleren som minimum overholder databehandlerens forpligtelser efter disse Bestemmelser og databeskyttelsesforordningen.

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

6. Databehandleren skal sikre at den dataansvarlige kan få udleveret og slettet alle data, herunder også fra underdatabehandlere, i tilfælde af databehandlerens konkurs.

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

7 Overførsel af oplysninger til tredjelande

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

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

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

    a. overføre personoplysninger til en dataansvarlig eller databehandler i et tredjeland eller en international organisation

    b. overlade behandling af personoplysninger til en underdatabehandler i et tredjeland

    c. behandle personoplysningerne i et tredjeland

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

5. Disse Bestemmelser skal ikke forveksles med standardkontraktsbestemmelser som omhandlet i databeskyttelsesforordningens artikel 46, stk. 2, litra c og d, og disse Bestemmelser kan ikke udgøre et grundlag for overførsel af personoplysninger som omhandlet i databeskyttelsesforordningens kapitel V.

8 Bistand til den dataansvarlige

1. Databehandleren bistår, under hensyntagen til behandlingens karakter, så vidt muligt den dataansvarlige ved hjælp af passende tekniske og organisatoriske foranstaltninger med opfyldelse af den dataansvarliges forpligtelse til at besvare anmodninger om udøvelsen af de registreredes rettigheder som fastlagt i databeskyttelsesforordningens kapitel III.

   Dette indebærer, at databehandleren så vidt muligt skal bistå den dataansvarlige i forbindelse med, at den dataansvarlige skal sikre overholdelsen af:

   a. oplysningspligten ved indsamling af personoplysninger hos den registrerede

   b. oplysningspligten, hvis personoplysninger ikke er indsamlet hos den registrerede

   c. indsigtsretten

   d. retten til berigtigelse

   e. retten til sletning ("retten til at blive glemt")

   f. retten til begrænsning af behandling

   g. underretningspligten i forbindelse med berigtigelse eller sletning af personoplysninger eller begrænsning af behandling

   h. retten til dataportabilitet

   i. retten til indsigelse

   j. retten til ikke at være genstand for en afgørelse, der alene er baseret på automatisk behandling, herunder profilering

2. I tillæg til databehandlerens forpligtelse til at bistå den dataansvarlige i henhold til Bestemmelse 5.3., bistår databehandleren endvidere, under hensyntagen til behandlingens karakter og de oplysninger, der er tilgængelige for databehandleren, den dataansvarlige med:

   a. den dataansvarliges forpligtelse til uden unødig forsinkelse og om muligt senest 48 timer, efter at denne er blevet bekendt med det, at anmelde brud på persondatasikkerheden til den kompetente tilsynsmyndighed, Datatilsynet, medmindre at det er usandsynligt, at bruddet på persondatasikkerheden indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder.

b. den dataansvarliges forpligtelse til uden unødig forsinkelse at underrette den registrerede om brud på persondatasikkerheden, når bruddet sandsynligvis vil medføre en høj risiko for fysiske personers rettigheder og frihedsrettigheder.

c. den dataansvarliges forpligtelse til forud for behandlingen at foretage en analyse af de påtænkte behandlingsaktiviteters konsekvenser for beskyttelse af personoplysninger (en konsekvensanalyse)

d. den dataansvarliges forpligtelse til at høre den kompetente tilsynsmyndighed, Datatilsynet, inden behandling, såfremt en konsekvensanalyse vedrørende databeskyttelse viser, at behandlingen vil føre til høj risiko i mangel af foranstaltninger truffet af den dataansvarlige for at begrænse risikoen.

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

9 Underretning om brud på persondatasikkerheden

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

2. Databehandlerens underretning til den dataansvarlige skal om muligt ske senest 48 timer efter, at denne er blevet bekendt med bruddet, sådan at den dataansvarlige kan overholde sin forpligtelse til at anmelde bruddet på persondatasikkerheden til den kompetente tilsynsmyndighed, jf. databeskyttelsesforordningens artikel 33.

3. I overensstemmelse med Bestemmelse 8.2.a skal databehandleren bistå den dataansvarlige med at foretage anmeldelse af bruddet til den kompetente tilsynsmyndighed. Det betyder, at databehandleren skal bistå med at tilvejebringe nedenstående information, som ifølge artikel 33, stk. 3, skal fremgå af den dataansvarliges anmeldelse af bruddet til den kompetente tilsynsmyndighed:

    a. karakteren af bruddet på persondatasikkerheden, herunder, hvis det er muligt, kategorierne og det omtrentlige antal berørte registrerede samt kategorierne og det omtrentlige antal berørte registreringer af personoplysninger

    b. de sandsynlige konsekvenser af bruddet på persondatasikkerheden

    c. de foranstaltninger, som den dataansvarlige har truffet eller foreslår truffet for at håndtere bruddet på persondatasikkerheden, herunder, hvis det er relevant, foranstaltninger for at begrænse dets mulige skadevirkninger.

4. Parterne skal i bilag C angive den information, som databehandleren skal tilvejebringe i forbindelse med sin bistand til den dataansvarlige i dennes forpligtelse til at anmelde brud på persondatasikkerheden til den kompetente tilsynsmyndighed.

10 Sletning og tilbagelevering af oplysninger

1. Ved ophør af tjenesterne vedrørende behandling af personoplysninger er databehandleren forpligtet til at udlevere en kopi af alle personoplysninger til den dataansvarlige og umiddelbart herefter slette alle personoplysninger, medmindre EU-retten eller medlemsstaternes nationale ret foreskriver opbevaring af personoplysningerne.

2. Databehandleren forpligter sig til alene at behandle personoplysningerne til de(t) formål, i den periode og under de betingelser, som disse regler foreskriver.

11 Tilsyn og revision

1. Databehandleren stiller alle oplysninger, der er nødvendige for at påvise overholdelsen af databeskyttelsesforordningens artikel 28 og disse Bestemmelser, til rådighed for den dataansvarlige og giver mulighed for og bidrager til revisioner, herunder inspektioner, der foretages af den dataansvarlige eller en anden revisor, som er bemyndiget af den dataansvarlige.

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

3. Databehandleren er forpligtet til at give tilsynsmyndigheder, som efter gældende lovgivningen har adgang til den dataansvarliges eller databehandlerens faciliteter, eller repræsentanter, der optræder på tilsynsmyndighedens vegne, adgang til databehandlerens fysiske faciliteter mod behørig legitimation.

12 Parternes aftaler om andre forhold

1. Parterne kan aftale andre bestemmelser vedrørende tjenesten vedrørende behandling af personoplysninger om f.eks. erstatningsansvar, så længe disse andre bestemmelser ikke direkte eller indirekte strider imod Bestemmelserne eller forringer den registreredes grundlæggende rettigheder og frihedsrettigheder, som følger af databeskyttelsesforordningen.

13 Ikrafttræden og ophør

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

2. Begge parter kan kræve Bestemmelserne genforhandlet, hvis lovændringer eller uhensigts-mæssigheder i Bestemmelserne giver anledning hertil.

3. Bestemmelserne er gældende, så længe tjenesten vedrørende behandling af personoplysninger varer. I denne periode kan Bestemmelserne ikke opsiges, medmindre andre bestemmelser, der regulerer levering af tjenesten vedrørende behandling af personoplysninger, aftales mellem parterne.

4. Hvis levering af tjenesterne vedrørende behandling af personoplysninger ophører, og personoplysningerne er slettet eller returneret til den dataansvarlige i overensstemmelse med Bestemmelse 11.1 og Bilag C, er Bestemmelserne at betragte som opsagte.

5. Underskrift (Ved brug af digital signatur: Se signatur og godkendelseslog i afslutningen af dokumentet)

På vegne af databehandleren

Navn	Martin W. Hultén
Stilling	Adm.dir.
Telefonnummer	+45 8880 8220
E-mail	mh@reindexknowledge.dk
Underskrift	

På vegne af den dataansvarlige

Navn	
Stilling	
Telefonnummer	
E-mail	
Underskrift	

14 Kontaktpersoner hos den dataansvarlige og databehandleren

1. Ovenstående underskriver pva. af databehandleren (13.5) er at betragte som kontaktperson.
2. Kontaktperson(er) for den dataansvarlige er virksomhedens, organisationens eller institutionens biblioteksmedarbejder(e), som om nødvendigt kan videreformidle informationer til den relevante kontaktperson hos den dataansvarlige.

Bilag A Oplysninger om behandlingen

Formålet med databehandlerens behandling af personoplysninger på vegne af den dataansvarlige er:

At den dataansvarlige kan anvende Reindex til biblioteksadministration og biblioteksbetjening af slutbrugere.

Behandlingen kan omfatte følgende typer af personoplysninger om de registrerede:

- Unik brugerkode
- Navn
- Evt. cpr.nr.
- Evt. mailadresse
- Evt. adresse
- Evt. mobilnummer
- Evt. hold-, klasse-, afdelings-, eller kontorbetegnelse
- Evt. oplysninger om bøder, gebyrer og erstatning for tabt materiale.

Oplysninger om aktuelle lån og brug af andre bibliotekstilbud såsom abonnement på nyhedslister, tidsskrifter mv. vil være knyttet til brugerens konto.

Den dataansvarlige vil ikke registrere, og databehandleren vil ikke på vegne af den dataansvarlige behandle, personoplysninger omfattet af databeskyttelsesforordningens artikel 9 om "særlige kategorier af personoplysninger".

Lånehistorik slettes som hovedregel i det øjeblik materialet afleveres. Historik omkring brug af andre tilbud og tjenester slettes også øjeblikkeligt ved ophør af brug. Der er to undtagelser fra denne regel:

1) Lånehistorik kan opbevares i maksimalt tredive (30) dage efter aflevering, hvis den dataansvarlige har truffet beslutning om dette efter samråd med databehandleren.

2) Lånehistorik gemmes om konkrete titler knyttet til låneren i de tilfælde, hvor der påløber gebyrer i forbindelse med lånet. Denne historik slettes når gebyr er afregnet eller fjernet fra lånerens konto.

Behandlingen kan omfatte følgende kategorier af registrerede:

- Ansatte i biblioteket eller informationsafdelingen (bibliotekarer og bibliotekspersonale).
- Medarbejdere i den organisation eller institution biblioteket eventuelt er en del af.

- Elever og studerende i den institution biblioteket eventuelt er en del af.
- Udefrakommende lånere og brugere af bibliotekets tjenester, herunder eventuelt andre biblioteker og deres kontaktpersoner.

Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige kan påbegyndes efter denne aftales ikrafttræden. Behandlingen har følgende varighed:

Behandlingen er ikke tidsbegrænset og varer indtil aftalen opsiges eller ophæves af en af parterne.

Bilag B Betingelser for databehandlerens brug af underdatabehandlere og liste over godkendte underdatabehandlere

Betingelser for databehandlerens brug af eventuelle underdatabehandlere
Databehandleren benytter underdatabehandlere til følgende ydelser: hosting og udsendelse af beskeder til slutbrugere via SMS og email.

Ikke alle dataansvarlige gør brug af SMS- og mailtjenester. For så vidt der gøres brug af disse tjenester og dermed disse underdatabehandlere sker det efter skriftlig instruks fra den dataansvarlige til databehandleren.

Den dataansvarlige har ved databehandleraftalens ikrafttræden godkendt anvendelsen af de herunder nævnte underdatabehandlere til den behandling, som er beskrevet, såfremt databehandleren gør brug af de funktioner der er tale om.

Den dataansvarlige godkender endvidere ved indgåelse af denne aftale at databehandleren uden den dataansvarliges specifikke og skriftlige godkendelse kan lade en anden underdatabehandler bistå databehandleren med hosting eller leverance af SMS og/eller mailtjenester.

Databehandleren skal underrette den dataansvarlige om eventuelt skift af underdatabehandler, jvf. denne aftales afsnit 6.3.

Anvendelse af anden underdatabehandler kan kun ske, hvis underdatabehandleren lever op til de samme krav til databehandling som de her beskrevne underdatabehandlere:

- Der skal være tale om samme afgrænsede og specifikke ydelser og tjenester.
- Levering af ydelserne og tjenesterne skal ske på det samme aftalegrundlag.
- Levering af ydelserne skal være omfattet af de samme garanterede sikkerhedspolitikker.

Den dataansvarlige kan gøre indsigelse mod skift af underdatabehandler. Hvis den dataansvarlige modsætter sig brugen af den nye underdatabehandler, deaktiverer databehandleren efter anmodning herom brugen af SMS- og/eller mailtjenester med den virkning at underdatabehandlere ikke efterfølgende behandler personoplysninger for den dataansvarlige.

Godkendte underdatabehandlere
Ved Bestemmelsernes ikrafttræden har den dataansvarlige godkendt brugen af nedenstående underdatabehandlere for den beskrevne behandlingsaktivitet. Databehandleren må ikke – uden den dataansvarliges skriftlige godkendelse – gøre brug af en underdatabehandler til en anden behandlingsaktivitet end den beskrevne og aftalte.

1) **Hetzner Online GmbH, Industriestr. 25. 91710 Gunzenhausen, Tyskland**

Databehandleren køber serverplads hos Hetzner, som således er hostingcenter. Databaseservere og applikationsservere hostes på root-servere. Dette indebærer at det kun er Reindex' ansatte, som har adgang til serverne i deres helhed.

I juridisk forstand fungerer Hetzner som underdatabehandler.

Der er indgået en Data Processing Agreement med Hetzner Online GmbH.

Hetzner Online GmbH er et 100% tysk ejet selskab, beliggende i Tyskland. Firmaet administrerer egne serverparker fysisk beliggende i Tyskland og Finland.

2) **Compaya A/S, CVR nr. 3137 5428, Palægade 4, 2. tv., 1261 Kbh. K**

Compaya benyttes til udsendelse af beskeder til slutbrugere via SMS. Dog kun i biblioteker som anvender denne kommunikationsmetode overfor slutbrugere.

Tjenesten indeholder en log med følgende personoplysninger:

- Brugerens arbejdsplads, organisation eller institution
- Brugerens navn
- Brugerens mobilnummer
- Tekstbesked som kan indeholde en titel på lånt biblioteksmateriale eller oplysning om antal lån

Disse oplysninger opbevares i en log, som er tilgængelig for databehandleren i 30 dage. Herefter slettes de.

Der er indgået en underdatabehandleraftale mellem ReindexKnowledge ApS og Compaya A/S.

Compaya A/S er et 100% dansk ejet selskab, beliggende i Danmark.

Compaya benytter et hostingmiljø fysisk placeret i Skanderborg og ejet af Zitcom/team.blue. Dette selskab er registreret i Danmark og ejet af et belgisk selskab, hvis ejerstruktur i sidste ende leder til et moderselskab registreret i Luxembourg.

Tilsyn med Zitcom/team-blue er underlagt ISO 27001 certificering.

CPSMS, som er den tjeneste vi konkret benytter fra Compaya, bliver årligt revideret og får tildelt ISAE-erklæring fra et eksternt revisionsfirma.

3) **Flowmailer. Van Nelleweg 1, 3044 BC Rotterdam, Holland. CoC-no.: 62154885**

Flowmailer benyttes til udsendelse af beskeder til slutbrugere via email. Dog kun i biblioteker som anvender denne kommunikation overfor slutbrugere.

Tjenesten indeholder en log med information om metadata for forsendelsen samt indhold i mailbesked. Dette opbevares i tre måneder, hvorefter det slettes automatisk.

Flowmailer er et 100% hollandsk ejet selskab, beliggende i Holland. Firmaet ejer selv den serverinfrastruktur der gøres brug af.

Der er indgået en databehandleraftale (Data Processing Agreement) mellem ReindexKnowledge ApS og Flowmailer.

Tilsyn med Flowmailer er underlagt ISO 27001 certificering.

Bilag C Instruks vedrørende behandling af personoplysninger

Behandlingens genstand/instruks
Databehandleren stiller en tjeneste til rådighed, hvor den dataansvarlige selv foretager registreringen af persondata og selv vælger:

- Hvilke persondata der registreres om den enkelte bruger, jvf. Bilag A
- Hvilke brugere der registreres, jvf. Bilag A
- Loginmetode: Hvordan brugere har adgang til tjenesten via login
- Metoder til kommunikation med registrerede brugere, jvf. Bilag B
- Daglig praksis omkring servicering af brugere f.eks. ved udlån og aflevering af biblioteksmateriale

Hvis der skal registreres brugere systematisk, f.eks. ved automatisk import fra studieadministrationssystemer, medarbejderregistre el.lign., sker dette altid på instruks fra den dataansvarlige til databehandleren.

Behandlingssikkerhed og bistand til den dataansvarlige
Sikkerhedsniveauet afspejler at der ikke er tale om behandling af personoplysninger omfattet af databeskyttelsesforordningens artikel 9 om "særlige kategorier af personoplysninger", jvf. bilag A.

Persondata indgŋr i følgende funktioner og arbejdsrutiner i Reindex :

- Registrering af brugere af tjenesten.
- Login til tjenesten.
- Tildeling af rettigheder til brugere.
- Udlŋn af bøger og andet materiale (artikler, undervisningsmaterialer, hjælpemidler).
- Rykkere for forfaldent materiale via SMS, brev eller mail.
- Advarsel om snarligt udløbet materiale via SMS eller mail.
- Afhentningsbeskeder.
- Regningsudsendelse.
- Regningsinddrivelse, oversendelse til inkasso eller SKAT's inddrivelsessystemer.
- Subskriptionsservices såsom nyheder eller notifikationer til brugere om nyheder indenfor udvalgte temaer.

I alle disse forhold træffer den dataansvarlige valg vedrørende procedure, daglig praksis og politik overfor slutbrugere og i behandling af brugerdata. Databehandleren bistår den dataansvarlige i opsætning og indstillinger af politik og handler således på instruks fra den dataansvarlige i henhold til alle ovenstående forhold.

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

Databehandleren stiller en komplet dokumentation vedrørende sikkerhedsforanstaltninger, opsætning, valg og indstillinger til rådighed for den dataansvarlige i selve tjenesten. Denne dokumentation er specifik for så vidt angår den dataansvarliges valg af f.eks. loginmetode til tjenesten. Dokumentationen er tilgængelig for alle medarbejdere hos den dataansvarlige med en brugerprofil som såkaldt "Admin" i tjenesten. I tjenesten finder man dokumentationen ad denne "sti":

- Hjælp > Data: Sikkerhed

Dokumentationen vedrører de foranstaltninger, som er aftalt med den dataansvarlige. Hertil kommer de nedenstående generelle politikker og praksisser:

Adgangskontrol

Til driftsystemet har kun 1 person hos Reindex til enhver tid adgang via ssh, som er krypteret terminaladgang. Kunder og hostingfirma har ikke adgang til driftsystemet.

Databaseservere og applikationsservere beskyttes af egen firewall der kun tillader adgang til ssh fra kendte IP-numre.

Applikationsservere tillader adgang for http og https samt password beskyttede SIP2 automater fra en række kendte IP-numre og password beskyttet z39.50 access til bibliografisk data efter aftale med Kunden.

Ukrypteret http på port 80 stoppes i applikationslaget.

Reindex er en webapplikation hvor adgang kontrolleres primært af én af 10 sikkerhedsprofiler, som kunden vælger ved opstart. De baserer sig på kombinationer af login og pincode suppleret med en række valgbare sikkerhedsfunktioner. Passwords er internt MD5-krypterede.

Ved Single Signon-løsninger som f.eks. UNI-Login eller SAML sker autentificering hos tredjepart og suppleres af access control i Reindex, således at rollen tildeles i Reindex.

Digital Sikkerhed ved intern håndtering af data

Den oftest forekommende eksponering af persondata er datansvarliges utilsigtede citering af persondata ifm. supporthenvendelser og i forbindelse med filbaseret import af brugerdata.

Hvis en bibliotekar ved en fejltagelse sender potentielt personnære oplysninger såsom fuldt cpr.nr. om en bruger i en henvendelse på mail eller i Reindex' supportsystem, sletter vi sagen med det samme. Vi sletter også de notifikationer vi får om sagen i vore mailklienter, og vi opfordrer alle der får notifikation med det personnære indhold til også at slette.

Reindex modtager filbaseret leverance af persondata med cpr.nr. Disse accepteres kun som leveret i en særlig beskyttet upload-zone i Kundens eget Admin interface og slettes dér automatisk efter 3 dage eller ved import i Reindex. Kun HEB nævnt i afsnittet Persondataansvarlige hos Reindex nedenfor kan udføre disse opgaver.

Reindex sletter al filbaseret persondata eller data til konvertering straks efter brug eller godkendelse af konvertering af dataansvarlig.

Reindex har instrueret alle ansatte om sikker adgang til udstyr, der anvendes til udvikling og support. Dette indebærer regelmæssig ændring af login/passwords, deaktivering når arbejdspladsen forlades og forhindring af cachede adgangsoplysninger.

Der anvendes de bedste procedurer og software til beskyttelse mod hacker og virusangreb.

Adgang til servere og kundedata kan kun gennemføres gennem krypterede forbindelser.

Ved kassering af udstyr til udvikling, support og drift destrueres harddiske og RAM, hvis vi har adgang til hardware. Ved hostet hardware overskrives harddisk og RAM med software, som aktivt overskriver dataområder med ny data.

Digital Sikkerhed mod udefrakommende trusler

Trussel	Beskrivelse	Hvad gør vi
XSS. Cross-site Scripting	Cross-Site Scripting (XSS) attacks are a type of injection, in which malicious scripts are injected into otherwise benign and trusted websites. XSS attacks occur when an attacker uses a web application to send malicious code, generally in the form of a browser side script, to a different end user. Flaws that allow these attacks to succeed are quite widespread and occur anywhere a web application uses input from a user within the output it generates without validating or encoding it. An attacker can use XSS to send a malicious script to an unsuspecting user. The end user's browser has no way to know that the script should not be trusted, and will execute the script. Because it thinks the script came from a trusted source, the malicious script can access any cookies, session tokens, or other sensitive information retained by the browser and used with that site. These scripts can even rewrite the content of the HTML page. For more details on the different types of XSS flaw **Ref**	Sanitize på alle input fra forms
SQL injection	SQL injection is a code injection technique, used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker).[1] SQL injection must exploit a security vulnerability in an	Sanitize af al database input.

Trussel	Beskrivelse	Hvad gør vi
	application's software, for example, when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and unexpectedly executed. SQL injection is mostly known as an attack vector for websites but can be used to attack any type of SQL database. **Ref**	
DDoS. Denial-of-service attacks	A cyber-attack in which the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet. Denial of service is typically accomplished by flooding the targeted machine or resource with superfluous requests in an attempt to overload systems and prevent some or all legitimate requests from being fulfilled **Ref**	Funktion på applikationsniveau som forhindrer excessiv tilgang fra samme IP-adresse.
Ajax security	Asynchronous JavaScript + XML (Ajax) is not a web technology; it is a collection of technologies created specifically to build dynamic web applications. Because of its range of functions and ease of use, Ajax is one of the most widely used tools for building web applications today. All applications, including those built using Ajax technologies, are vulnerable to exploits that compromise websites and the databases that drive them **Ref**	Alle ajax funktioner har samme adgangskontrol som websider og der returneres ikke persondata i JSON eller XML som resultat af en JSON process.

Persondataansvarlige hos Reindex

- Martin W. Hultén (MH)
- Hans Erik Büscher (HEB)

Adgang til persondata logges

På applikationsniveau logges ethvert view af persondata, ethvert fejlslagent loginforsøg og disse log data kan inspiceres af den dataansvarlige. Der stilles på den dataansvarliges eventuelle instruks yderligere sikkerhed til rådighed i form af Ban IP-funktionalitet, som lukker for yderligere login-forsøg for anvendt IP-nummer efter et antal fejlslagne forsøg på login.

Dataansvarlig kan gennem en Admin konto i Reindex inspicere log for tilgang til persondata.

Dataansvarlig kan gennem en Admin konto i Reindex inspicere log for forkerte login forsøg.

Disse logs trunkeres automatisk, således at der kun findes data for de sidste 2 års anvendelse

Kun én af de persondataansvarlige (HEB) hos Reindex har adgang til persondata uden om logning ifm. test og support

Logning af Reindex' interne sikkerhedsprocedurer

Reindex udstiller gennemført logning for dataansvarlig gennem en Admin konto i Reindex.

Loggen dokumenterer:

- Restore test af aktuel backup
- Aplication server upgrade
- Database server upgrade
- Web server log analyse
- Database server log analyse
- Dokumentation vedr. sikkerhedsprocedurer gennemgået og evt. aktualiseret
- Micro update - dvs. opdatering af Reindex applikationen inkl. ny superuser pinkode
- Password fornyelse

For loganalyse anvendes for real-time status standard Apache mod_status, som giver et øjebliksbillede af aktiviteterne på webserverne. Disse views er aktive på alle hverdage og logges ikke. Som loganalyseværktøj anvendes udover manuelle checks Nagios, der integrerer analyse af netværkshændelser fra såvel webservere som databaseservere.

Applikationsserver og databaseserver upgrades følger Best Practice-anbefalingerne for Debian stable, og sekvensen afgøres af annonceringerne på *The Debian Security Announce mailing list*

Second line support, test og udvikling af Reindex

I forbindelse med second line support, generel test og udvikling af Reindex hjemtages data inklusive persondata til et udviklingsmiljø, hvor der ikke er ekstern adgang. Det vil sige at man ikke kan opnå adgang til disse data fra nettet.

Umiddelbart efter disse opgaver slettes data fuldstændigt fra udviklingsmiljøet.

Kun HEB nævnt i afsnittet Persondataansvarlige hos Reindex kan udføre disse opgaver.

Udfasning af hardware

I forbindelse med nedlukning af servere overskrives diske med et Single Overwrite utility, som udelukker evt. genetablering af data.

Opbevaringsperiode/sletterutine

Den dataansvarlige er ansvarlig for sletning af persondata fra tjenesten, når det ikke længere er relevant at opbevare data om den eller de berørte personer.

Databehandleren kan på instruks fra den dataansvarlige bistå med automatiserede rutiner til sletning af brugere, herunder i forbindelse med import af brugerdata som beskrevet ovenfor.

Databehandleren kan stille funktionalitet til rådighed for den dataansvarlige, hvormed sletning af brugerdata lettes.

Opsigelse af Reindex

Hvis en dataansvarlig opsiger samarbejdet med Reindex kan den dataansvarlige selv trække data inklusive persondata og kontoinformation ud til lokalt brug i anerkendte dataformater.

Reindex sletter umiddelbart al relevant materiale efter ophør af samarbejde efter samråd med den dataasvarlige.

Se i øvrigt om udlevering og sletning af personoplysninger ved ophør af aftalen i denne aftales afsnit 10.1.

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

Den dataansvarlige eller en repræsentant for den dataansvarlige har adgang til at foretage inspektioner, herunder fysiske inspektioner, med lokaliteterne hvorfra databehandleren foretager behandling af personoplysninger, herunder fysiske lokaliteter og systemer, der benyttes til eller i forbindelse med behandlingen. Sådanne inspektioner kan gennemføres, når den dataansvarlige finder det nødvendigt.

Den dataansvarliges eventuelle udgifter i forbindelse med en fysisk inspektion afholdes af den dataansvarlige selv. Databehandleren er dog forpligtet til at afsætte de ressourcer (hovedsageligt den tid), der er nødvendig(e) for, at den dataansvarlige kan gennemføre sin inspektion.

Databehandleren er behjælpelig med løbende at levere dokumentation for alle sikkerhedspoltikker og konkrete valg foretaget af den dataansvarlige, således at den dataansvarlige på denne måde kan føre det nødvendige tilsyn med databehandleren. Dokumentationen er omtalt ovenfor i afsnittet om behandlingssikkerhed og bistand til den dataansvarlige.