Signit.com

CVR: 38363395

Databehandleraftale (SDBA) bilag til Forretningsbetingelser og vilkår for serviceydelser

Denne databehandleraftale med standardkontraktbestemmelser er et bilag til den mellem parterne (Kunden og Signit.com) indgåede aftale for serviceydelser og udgør en integreret del af Signit.com's bestemmelser vedrørende persondata. Se www.signit.dk/vilkaar

Denne Standard Databehandleraftale ("SDBA") gælder for enhver kunde ("Kunden"), der anvender Signit.dk ApS' tjenester, medmindre der er indgået en særskilt Kundespecifik Databehandleraftale ("KSDBA") mellem Kunden og Signit.dk ApS.

Alle øvrige forhold mellem os reguleres af den aftale, som dette dokument er eller bliver en integreret del af, herunder vores pligt til at behandle kundens informationer fortroligt og begrænsning af vores erstatningsansvar for misligholdelse af aftalen.

Databehandleraftalen kan kun bringes til ophør i forbindelse med opsigelse eller ophør af den hovedaftale, som den er knyttet til, i overensstemmelse med de varslingsbestemmelser, der er fastsat heri. Hvis en instruks fra Kunden begrænser eller hindrer Signit.com i at levere de aftalte ydelser, kan det medføre behov for opsigelse af hovedaftalen efter gældende varslingsfrister. Sådanne ændringer i instruksen anses ikke som misligholdelse, men kan få betydning for parternes videre samarbejde.

DATABEHANDLERAFTALE

Standardkontraktsbestemmelser

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

mellem

”Databehandleraftalen er gældende mellem databehandleren og de af IT Center Nords samarbejdsskoler, som har indgået en kontraktuel aftale om køb af ydelsen, som danner grundlag for denne databehandleraftale, og som IT Center Nord har en fuldmagt til at forhandle og underskrive databehandleraftaler på vegne af.

herefter ”den dataansvarlige”

“Kunden”

Kontaktpersoner:
Navn:
Telefonnummer:
E-mail:

herefter ”den dataansvarlige”

og

CVR: 38363395
Signit.dk ApS
Tysklandsvej 7
7100 Vejle
Danmark

herefter ”databehandleren”

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

HAR AFTALT følgende standardkontraktsbestemmelser (Bestemmelserne) med henblik på at overholde databeskyttelsesforordningen og sikre beskyttelse af privatlivets fred og fysiske personers grundlæggende rettigheder og frihedsrettigheder

1. Indhold

2. Præambel

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

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

3. I forbindelse med leveringen af SignIt.com web løsningen 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 fire bilag til disse Bestemmelser, og bilagene udgør en integreret del af Bestemmelserne.

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

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

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

9. Bilag D er Parternes regulering af andre forhold.

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

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

3. Den dataansvarliges rettigheder og forpligtelser

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

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

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

[1] Henvisninger til "medlemsstat" i disse bestemmelse skal forstås som en henvisning til "EØS medlemsstater".

4. Databehandleren handler efter instruks

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

5. Fortrolighed

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

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

6. Behandlingssikkerhed

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

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

   a. Pseudonymisering og kryptering af personoplysninger

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

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

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

2. Efter forordningens artikel 32 skal databehandleren – uafhængigt af den dataansvarlige – også vurdere risiciene for fysiske personers rettigheder som behandlingen udgør og gennemføre foranstaltninger for at imødegå disse risici. Med

henblik på denne vurdering skal den dataansvarlige stille den nødvendige information til rådighed for databehandleren som gør vedkommende i stand til at identificere og vurdere sådanne risici.

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

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

7. Anvendelse af underdatabehandlere

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

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

3. Databehandleren har den dataansvarliges generelle godkendelse til brug af underdatabehandlere. Databehandleren skal skriftligt underrette den dataansvarlige om eventuelle planlagte ændringer vedrørende tilføjelse eller udskiftning af underdatabehandlere med mindst 30 dages varsel og derved give den dataansvarlige mulighed for at gøre indsigelse mod sådanne ændringer inden brugen af de(n) omhandlede underdatabehandler(e). 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. Underdatabehandleraftale(r) og eventuelle senere ændringer hertil sendes – efter den dataansvarliges anmodning herom – i kopi til den dataansvarlige, som herigennem har mulighed for at sikre sig, at tilsvarende databeskyttelsesforpligtelser som følger af disse Bestemmelser er pålagt underdatabehandleren. Bestemmelser om kommercielle vilkår, som ikke påvirker det databeskyttelsesretlige indhold af underdatabehandleraftalen, skal ikke sendes til den dataansvarlige.

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

8. Overførsel til tredjelande eller internationale organisationer

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

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

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

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

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

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

9. Bistand til den dataansvarlige

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

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

    a. oplysningspligten ved indsamling af personoplysninger hos den registrerede
    b. oplysningspligten, hvis personoplysninger ikke er indsamlet hos den registrerede
    c. indsigtsretten
    d. retten til berigtigelse

e. retten til sletning (”retten til at blive glemt”)
f. retten til begrænsning af behandling
g. underretningspligten i forbindelse med berigtigelse eller sletning af personoplysninger eller begrænsning af behandling
h. retten til dataportabilitet
i. retten til indsigelse
j. retten til ikke at være genstand for en afgørelse, der alene er baseret på automatisk behandling, herunder profilering

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

    a. den dataansvarliges forpligtelse til uden unødig forsinkelse og om muligt senest 72 timer, efter at denne er blevet bekendt med det, at anmelde brud på persondatasikkerheden til den kompetente tilsynsmyndighed, Datatilsynet i Danmark, 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 i Danmark, 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.

10. 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 24 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 9.2.a skal databehandleren bistå den dataansvarlige med at foretage anmeldelse af bruddet til den kompetente tilsynsmyndighed. Det betyder, at databehandleren skal bistå med at tilvejebringe nedenstående information, som ifølge artikel 33, stk. 3, skal fremgå af den dataansvarliges anmeldelse af bruddet til den kompetente tilsynsmyndighed:

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

b. de sandsynlige konsekvenser af bruddet på persondatasikkerheden

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

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

11. Sletning og returnering af oplysninger

1. Ved ophør af tjenesterne vedrørende behandling af personoplysninger, er databehandleren forpligtet til at slette alle personoplysninger, der er blevet behandlet på vegne af den dataansvarlige og bekræfte over for den dataansvarlig, at oplysningerne er slettet, medmindre EU-retten eller medlemsstaternes nationale ret foreskriver opbevaring af personoplysningerne.

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

   a. Opbevaring af regnskabsmateriale i 5 år herunder relevante specifikationer og regnskabsrelaterede data og andre lignende administrative kontaktpersoner som gemmes med navn, position og email.

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

12. Revision, herunder inspektion

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 nærmeret angivet i Bilag C.7. og C.8.

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.

13. Parternes aftale 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.

14. 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 uhensigtsmæssigheder 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.4, kan Bestemmelserne opsiges med skriftlig varsel af begge parter.

5. Underskrift / Elektronisk accept og gyldighed

Denne Standard Databehandleraftale ("SDBA") accepteres af Kunden elektronisk ved kontooprettelse eller ved senere digital accept (fx via login, in-app notifikation eller digital signering).

Accept kan ske ved hjælp af Signit.dk ApS' egne løsninger til elektronisk signatur, klik-baseret accept eller tilsvarende digitale processer. En sådan elektronisk accept har samme juridiske gyldighed som en fysisk underskrift i henhold til dansk aftaleret og eIDAS-forordningen (artikel 25).

Signit.dk ApS logger dato, klokkeslæt, bruger-ID og version af SDBA for hver accept og kan kræve, at Kunden (eller den registrerede Superadministrator) aktivt accepterer nye versioner, når væsentlige ændringer træder i kraft.

Seneste version af SDBA er til enhver tid tilgængelig på www.signit.dk/databeskyttelse/sdba, og tidligere versioner kan rekvireres ved henvendelse til legal@signit.dk.

På vegne af den dataansvarlige

For Kunden anses den til enhver tid registrerede Superadministrator og/eller Kontoejer i Signit.dk ApS' system som kundens officielle kontaktperson i henhold til denne databehandleraftale.

På vegne af databehandleren:

Databeskyttelsesansvarlig
88 62 60 70
dpo@signit.dk

15. Ændringer og versionering

Signit.dk ApS kan til enhver tid foretage ændringer i denne Standard Databehandleraftale ("SDBA"), når det er nødvendigt for at efterleve gældende lovgivning, forbedre sikkerheden eller tilpasse ydelserne.

Væsentlige ændringer meddeles Kunden med mindst 30 dages varsel pr. e-mail til den registrerede Superadministrator og/eller via in-app notifikation. Kunden kan i

varslingsperioden gøre indsigelse eller opsige hovedaftalen med det i de generelle vilkår fastsatte varsel, hvis Kunden ikke kan acceptere ændringerne.

Seneste version af SDBA vil til enhver tid være tilgængelig på [link til SDBA], og et versionsarkiv vil blive ført, så Kunden kan dokumentere, hvilken version der var gældende på et givent tidspunkt.

Fortsat brug af Signit.dk ApS' tjenester efter ikrafttrædelsesdatoen anses som accept af den opdaterede SDBA.

16. Kontaktpersoner hos den dataansvarlige og databehandleren

1. Parterne kan kontakte hinanden via nedenstående kontaktpersoner.

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

   For Kunden anses den til enhver tid registrerede Superadministrator og/eller Kontoejer i Signit.dk ApS' system som kundens officielle kontaktperson i henhold til denne databehandleraftale.

   Al kommunikation, herunder varsler om ændringer af denne SDBA, anses for korrekt afgivet, når den er sendt til den e-mailadresse, der er registreret for Superadministrator eller Kontoejer.

   For Signit.dk ApS:

   Databeskyttelsesansvarlig
   88 62 60 70
   dpo@signit.dk

Bilag A Oplysninger om behandlingen

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

Den dataansvarlige og databehandleren (Signit.com) har indgået aftale om levering af digitale services i form af en webservice-løsning (Servicen) til brug ved indgåelse af skriftlige aftaler og kontrakter samt underskrift, opbevaring og søgning af digitale dokumenter og data, der relaterer til sådanne aftaler eller kontrakter og tilknyttede kontraktrelationer. Servicen inkluderer yderligere relevante systemmoduler, som muliggør integration af dokumenter, betalinger og data i en samlet arbejdsgang, der kan automatiseres og struktureres i projekter, workflows, arkiver, opgave- og sagshåndteringssystemer. Disse moduler kan anvendes til HR-processer, salgsprocesser, samtykkeerklæringsprocesser, projektstyringsprocesser, kundeundersøgelser, indsamling af brugerfeedback, og præsentation af kommercielle tilbud til brugerne. Kunden accepterer, at persondata behandles i overensstemmelse med de specificerede anvendelsesscenarier og formål, der er nævnt i denne aftale.

I henhold til aftalen skal databehandlere behandle personoplysninger på den dataansvarliges vegne i forbindelse med levering af Servicen. Det vil sige Signit.com behandler personoplysninger på vegne af den dataansvarlige, fordi det er nødvendigt for at levere aftalte ydelser til den dataansvarlige.

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

- Indsamling og registrering af personoplysninger i forbindelse med oprettelse af brugerkonti.
- Identifikation af brugeren og kommunikation med brugeren omkring løsningen.
- Sikker identifikation af brugeren i forbindelse med underskrift af og adgang til dokumenter.
- Sikker identifikation af brugeren i forbindelse med adgangskontrol til løsningen.
- Sikker digital mærkning af underskrevne dokumenter.
- Identifikation af brugerens computer med henblik på at øge sikkerheden af løsningen.
- Brugerens handlinger i løsningen logges med henblik på at kunne føre systembevis ved domstolene samt optimere brugeroplevelsen.
- Identifikation af de dokumenter, som den registrerede har tilknytning til.
- Digital og elektronisk underskrift af dokumenter og kontrakter.
- Opbevaring af underskrevne dokumenter og tilknyttede personoplysninger.
- Søgning og hentning af dokumenter og personoplysninger.
- Integration af dokumenter og data i automatiserede arbejdsgange og projektstyringssystemer.
- Præsentation af kommercielle tilbud og indsamling af brugerfeedback.
- Behandling af personoplysninger i forbindelse med HR-processer, salgsprocesser, samtykkeerklæringsprocesser og kundeundersøgelser.

Disse aktiviteter omfatter både automatisk og manuel behandling af personoplysninger med henblik på at levere de aftalte services og funktionaliteter til den dataansvarlige.

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

- Navn
- E-mailadresse
- Telefonnummer
- Adresse
- Fødselsdato

- Køn (via CPR-nummer)
- Personnummer (CPR-nummer)
- MitID UUID eller andre eID identitifikationsnumre herunder BankID m.m.
- Underskrift data relateret til digitale identiteter herunder pasoplysninger
- IP-adresse
- Betalingsoplysninger (f.eks. kreditkortnummer, bankkontonummer)
- Bruger-ID
- Rolle og tilladelser inden for systemet
- Metadata om dokumenter (f.eks. dokumenttitel, dato og klokkeslæt for underskrift)
- Oplysninger om samtykke og præferencer (f.eks. markedsføringssamtykke)
- Logdata og aktivitetsdata (f.eks. login-tidspunkter, handlinger foretaget inden for systemet)
- Oplysninger relateret til HR-processer (f.eks. ansættelseskontrakter, medarbejdernummer)
- Oplysninger relateret til salgsprocesser (f.eks. kundeaftaler, tilbud)
- Feedback og svar på kundeundersøgelser
- Eventuelle andre personoplysninger indeholdt i de dokumenter, der uploades af den dataansvarlige til underskrift og opbevaring.
- Data indsamlet via formularer oprettet eller bestilt af den dataansvarlige, som kan inkludere enhver type personoplysninger som specificeret af kunden.
- Oplysninger relateret til børn, deres forældre eller værger, som er indsamlet gennem skoler og institutioner.
- Data kan importeres i store mængder via CSV eller Excel-filer eller via Servicens API-endepunkter, som kan inkludere enhver type personoplysninger specificeret af den dataansvarlige.

Bemærk: Da den dataansvarlige kan uploade forskellige typer dokumenter, oprette formularer og importere data i store mængder via CSV, Excel eller API, kan andre typer af personoplysninger også blive behandlet afhængigt af dokumenternes og datafilernes indhold. Den dataansvarlige accepterer, at dette kan udvide omfanget af de personoplysninger, der behandles, og forstår og påtager sig ansvaret for denne udvidelse. Den dataansvarlige skal sikre, at de nødvendige samtykker er indhentet, især i forhold til behandling af data vedrørende børn, deres forældre eller værger, og at der foreligger passende privatlivspolitikker. Den dataansvarlige skal desuden sikre, at alle samtykker er dokumenteret i overensstemmelse med gældende lovgivning.

A.4. Behandlingen omfatter følgende kategorier af registrerede

- Kunder og klienter
- Medarbejdere hos kunder og klienter
- Elever og studerende (i tilfælde af skoler og institutioner)
- Forældre eller værger til elever og studerende
- Medarbejdere og personale hos den dataansvarlige
- Leverandører og samarbejdspartnere
- Brugere af systemet og webtjenesterne
- Modtagere af kommercielle tilbud og marketingmateriale
- Deltagere i kundeundersøgelser og feedbackprogrammer

Bemærk: Den dataansvarlige accepterer, at dette kan udvide omfanget af de personoplysninger, der behandles, da det er den dataansvarlige, der beslutter hvilke typer dokumenter, herunder hvilke personoplysninger, der uploades, oprettes via formularer eller importeres via CSV, Excel eller API. Den dataansvarlige er ansvarlig for at sikre, at de nødvendige samtykker er indhentet, og at der foreligger passende privatlivspolitikker. Den dataansvarlige skal desuden sikre, at alle samtykker er dokumenteret i overensstemmelse med gældende lovgivning.

A.5. Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige kan påbegyndes efter disse Bestemmelsers ikrafttræden. Behandlingen har følgende varighed

Varighed af Behandling:

Behandlingen fortsætter, så længe den dataansvarlige har en aktiv konto hos Signit.com. Kunden kan opsige kontoen på Signit.com webapplikationen online. Der gælder opsigelsesvarsel jf. generelle forretningsbetingelser.

Data opbevares, medmindre den dataansvarlige sletter dem via vores system.
Ved opsigelse af kontoen gemmes data indtil ophør, og slettes derefter inden for 90 dage fra sikkerhedskopier. Data, som skal opbevares længere ifølge dansk eller EU-lovgivning, opbevares i overensstemmelse med disse krav.

Brugeroprettelse og Ansvar:

Slutbrugere (modtagere af kontrakter eller tilbud) kan oprette egne konti og indgå direkte aftale med Signit.com. Deres data slettes ikke, selvom den dataansvarliges konto ophører.
Slutbrugeres adgang til dataansvarliges data og funktioner slettes ved opsigelse af dataansvarliges konto.

Medarbejdere:

Medarbejdere inviteret til virksomhedskontoen registrerer også en privat konto, medmindre virksomheds-specifikke e-mails eller digitale identifikatorer (f.eks. MitID Erhverv, ADFS) bruges. Ved opsigelse slettes medarbejderens adgang til virksomhedens data, men deres private konto opretholdes.

Elev og Forældreportal:

Elever, Forældre og værger, der opretter konti via elev og forældreportalen, får adgang til børns data. Disse brugere indgår direkte aftale med Signit.com, og deres data opretholdes. Adgang til data registreret under dataansvarliges konto slettes ved opsigelse, men forældre- og værgekontoen opretholdes.

Nye Brugere og Signerede Dokumenter:

Når dataansvarlige sender dokumenter til underskrift af personer (f.eks. nye medarbejdere) med private e-mailadresser (f.eks. Gmail), kan disse personer oprette en konto inden for 60 dage for at få adgang til de underskrevne dokumenter ved at validere deres e-mailadresse.
De underskrevne dokumenter tilhører både den dataansvarlige og den private Signit.com-konto. Hvis den dataansvarlige sletter sin konto hos Signit.com, slettes dokumenterne ikke fra den private Signit.com-konto.

Bilag B Underdatabehandlere

B.1. Godkendte underdatabehandlere

Ved Bestemmelsernes ikrafttræden har den dataansvarlige godkendt brugen af følgende underdatabehandlere

NAVN	CVR/Business registration number	ADRESSE	BESKRIVELSE AF BEHANDLING
In Groupe Trust Services ApS (Tidligere Nets A/S)	44526778	C/O IN Groupe Denmark A/S Teknikerbyen 5, 2. Søllerød 2830 Virum	E-identifikation og validering af digital signering
Digitaliseringsstyrelsen	34051178	Landgreven 4 1301 København K	MitID løsning
In Groupe Denmark A/S (Tidligere Nets A/S)	30808460	Teknikerbyen 5, 2. Søllerød Danmark	Håndterer CPR, CVR-identifikationer og MitID-brokeridentifikationer samt andre eID-identifikationer og forsegling af dokumenter
Amazon Web Services EMEA SARL	LU26375245	38 Avenue John F. Kennedy, L-1855 Luxembourg	Bruges til at køre servere, opbevare dokumenter, loganalyse, dokumentscanning og e-mailservice. Kun brugt inden for EU-datacentre. Kunder kan fravælge lagring eller behandling af data med en separat serviceaftale.
Cybernetic ApS	39999331	Tysklandsvej 7, 7100 Vejle Danmark	Leverer IT-support, kører hosting af servere og arkivering af dokumenter. Kun brugt inden for EU-datacentre.
Atlassian Pty Ltd	161211108	Level 6, 341 George Street, Sydney, NSW 2000 Australia	Bruges til helpdesk og kundesupport via JIRA. Kun brugt inden for EU-datacentre.
Google Ireland Limited	27252642	Gordon House, Barrow Street, Dublin 4 Irland	Bruges til e-mails sendt til os (Gmail for business), men ikke til opbevaring af andre data. Kun brugt inden for EU-datacentre.
Visma e-conomic A/S	29403473	Gærtorvet 3, 1799 København V Danmark	Leverer økonomi- og regnskabssoftware. Kun brugt inden for EU-datacentre.
Odoo N.V.	0477472701	Chaussée de Namur 40, 1367 Grand-Rosière, Belgien	Leverer ERP-løsninger. Kun brugt inden for EU-datacentre.
Twilio Ireland Limited	557454	3 Dublin Landings, North Wall Quay Dublin 1 Ireland	Leverer SMS/Email løsninger. Kun brugt inden for EU-datacentre.

Epay A/S	44307499	Fredrik Bajers Vej 300 9220 Aalborg Danmark	Håndterer betalinger med kreditkort og mobile pay.
Criipto A/S / Idura ApS	35142207	Gammel Kongevej 3E, 1. 1610 København	Håndterer CPR, CVR-identifikationer og MitID-brokeridentifikationer samt andre eID-identifikationer

Ved Bestemmelsernes ikrafttræden har den dataansvarlige godkendt brugen af ovennævnte underdatabehandlere for den beskrevne behandlingsaktivitet.

B.2. Varsel for godkendelse af underdatabehandlere

Ved tilføjelser eller udskiftninger af underdatabehandlere skal dette ske i overensstemmelse med databehandleraftalens pkt. 7.3.

Bilag C Instruks vedrørende behandling af personoplysninger

C.1. Behandlingens genstand/instruks
Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige sker ved, at databehandleren udfører følgende:

- Dokumentopbevaring: Opbevaring af digitale dokumenter og kontrakter, som indeholder personoplysninger, på sikre servere inden for EU-datacentre.
- Elektronisk signatur: Facilitering af elektroniske signaturer på dokumenter og kontrakter, som kan indeholde personoplysninger.
- Identifikation: Håndtering af identifikationsprocesser ved hjælp af CPR, CVR, MitID, og andre eID-systemer for at sikre personers identitet.
- Dataanalyse: Udførelse af loganalyse og dokumentscanning for at opretholde sikkerhed og effektivitet i systemet.
- Support: Brug af helpdesk-systemer til at modtage og besvare kundehenvendelser, som kan indeholde personoplysninger.
- E-mailhåndtering: Modtagelse og opbevaring af e-mails fra kunder, som kan indeholde personoplysninger.
- Økonomistyring: Håndtering af økonomiske data, herunder fakturering og regnskab, som indeholder personoplysninger om kunder og brugere.
- ERP-løsninger: Levering af ERP-løsninger til at administrere forretningsprocesser, som kan omfatte behandling af personoplysninger.
- Betalingshåndtering: Håndtering af betalinger som en integreret del af databehandlingen, typisk som en del af en signeringsproces, men det behøver ikke nødvendigvis at være det.
- Projektstyring: Tilbydelse af værktøjer til projektstyring, der muliggør integration af dokumenter og data i automatiserede arbejdsgange og strukturerede projekter.
- Workflow- og arkivsystemer: Implementering af workflows og arkivsystemer for at organisere opgaver og sager, der kan involvere personoplysninger.
- HR-processer: Understøttelse af HR-processer, herunder rekruttering, ansættelseskontrakter og medarbejderadministration.
- Salgsprocesser: Håndtering af salgsprocesser, inklusive kundeaftaler og tilbud.
- Samtykkehåndtering: Administration af samtykkeerklæringer og brugerpræferencer.

C.2. Behandlingssikkerhed

Sikkerhedsniveauet skal afspejle:

Behandlingen omfatter en større mængde personoplysninger, herunder potentielt fortrolige og/eller følsomme oplysninger som CPR-numre og andre identifikationsoplysninger, hvorfor der skal etableres et højt sikkerhedsniveau. Sikkerhedsniveauet skal afspejle behandlingens karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder.

Databehandleren er certificeret af PWC for at sikre, at vi følger god IT-praksis i Danmark og har tilstrækkelig sikkerhed. Databehandleren er berettiget og forpligtet til at træffe beslutninger om, hvilke tekniske og organisatoriske sikkerhedsforanstaltninger der skal gennemføres for at etablere det nødvendige (og aftalte) sikkerhedsniveau.

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

- Kryptering: Personoplysninger skal krypteres, både under transmission og opbevaring, for at sikre dataenes fortrolighed og integritet, hvor det er praktisk muligt. Specificerede metoder udelades her for at beskytte vores sikkerhedsforanstaltninger. Certificeringsrapporter kan rekvireres efter anmodning, som inkluderer flere detaljer.
- Vedvarende fortrolighed, integritet, tilgængelighed og robusthed: Systemer og tjenester skal sikre vedvarende fortrolighed, integritet, tilgængelighed og robusthed ved hjælp af opdaterede sikkerhedsprotokoller og -teknologier. Detaljer udelades for at beskytte sikkerhedsforanstaltningerne.
- Genopretningsevne: Systemer skal have evnen til rettidigt at genoprette tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse, gennem etablerede backup- og gendannelsesprocedurer. Specifikke metoder er ikke beskrevet her af sikkerhedsmæssige årsager.
- Regelmæssig afprøvning, vurdering og evaluering: Der skal være procedurer for regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske foranstaltninger til sikring af behandlingssikkerheden. Metoder udelades her for at beskytte vores sikkerhedsforanstaltninger.
- Adgang via internettet: Adgang til oplysninger via internettet skal være begrænset og sikret gennem stærke autentifikationsmetoder og adgangskontrolforanstaltninger. Detaljer er ikke beskrevet her for at beskytte sikkerhedsforanstaltningerne.
- Beskyttelse under transmission: Oplysninger skal beskyttes under transmission ved hjælp af krypteringsmetoder som SSL/TLS for at forhindre uautoriseret adgang. Specifikke tekniske detaljer udelades af sikkerhedsmæssige årsager.
- Beskyttelse under opbevaring: Oplysninger skal beskyttes under opbevaring ved hjælp af krypterede databaser og adgangskontrol for at forhindre uautoriseret adgang og datalækage. Metoder udelades her for at beskytte sikkerhedsforanstaltningerne.
- Fysisk sikring: Lokaliteternes fysiske sikkerhed, hvor der behandles oplysninger, skal sikres gennem adgangskontrol, overvågning og andre relevante foranstaltninger. Specifikke sikkerhedsdetaljer udelades af hensyn til sikkerheden.
- Hjemme-/fjernarbejdspladser: Der skal være sikkerhedsforanstaltninger for hjemme- og fjernarbejdspladser, herunder brug af VPN og sikre forbindelser for at beskytte oplysninger. Detaljer er udeladt for at beskytte sikkerhedsforanstaltningerne.
- Logning: Al adgang til og handlinger på systemet skal logges for at kunne overvåge og gennemgå adgangen til personoplysninger og sikre overholdelse af sikkerhedspolitikkerne. Specifikke metoder er ikke beskrevet her af sikkerhedsmæssige årsager.

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

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

Orientering om væsentlige ændringer: Ved væsentlige ændringer af it-systemer og infrastruktur orienterer databehandleren den dataansvarlige herom med henblik på, at den dataansvarlige har mulighed for at foretage fornyede risikovurderinger og sikkerhedsforanstaltninger.

Generel overholdelse af love og regler: Databehandleren skal til enhver tid sikre, at det leverede system overholder love og regler herunder bl.a. databeskyttelsesforordningen og databeskyttelsesloven. Databehandleren skal derigennem sikre vedvarende fortrolighed, integritet, tilgængelighed og robusthed af behandlingssystemer og -tjenester.

Procedure for GDPR-sikkerhedshændelser: Databehandleren skal som følge af GDPR-sikkerhedshændelser eller andre identificerede forhold, der truer sikkerheden, iværksætte foranstaltninger, der nedsætter eller eliminerer konsekvenserne af de uhensigtsmæssige forhold. I øvrigt skal den dataansvarlige orienteres herom. Der skal desuden foreligge fastlagte procedurer for håndtering af GDPR-sikkerhedshændelser, som sikrer, at der hurtigt bliver grebet ind og fulgt op på disse, samt at den dataansvarlige bliver orienteret jf. databehandleraftalens punkt 10.2.

Processer og beredskab: Databehandleren har processer og et beredskab, som sikrer at driften af et system genoptages i tilfælde af et nedbrud. Databehandleren skal kunne genoprette tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse. For sikring af databehandlerens evnen til at genoprette tilgængeligheden af og adgangen til data rettidigt, i tilfælde af en fysisk eller teknisk hændelse, implementerer databehandleren backups og redundante værktøjer.

Databehandleren skal ligeledes have procedurer for regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske foranstaltninger til sikring af behandlingssikkerhed.

Kryptering: At Databehandlerens generelle sikkerhedssetup skal sikre en sikkerhedsmæssig forsvarlig behandling af personoplysninger både fra arbejdspladsen og fra distancen (opkobling til webkontorer fra en hvilken som helst pc med internetadgang) – herunder i form af kryptering af data. Ovenstående foregår gennem en vpn-forbindelse. Dertil skal personoplysninger under transmission krypteres på transportlageret (TLS), hvilket som minimum skal ske ved at bruge version 1.2 eller højere.

Fortrolighed: Alle medarbejdere hos Databehandleren, der har adgang til personoplysninger, skal være underlagt fortrolighedsaftaler.

Firewalls og antivirus: Databehandleren sørger for, at alle arbejdsmaskiner og servere er udstyret med antivirussoftware med henblik på at blokere vira, malware m.v. Netværket er placeret bag firewalls for at kunne beskytte netværket mod uautoriseret adgang. Dertil skal det sikres, at alle systemer opdateres løbende og ligeledes jævnligt scannes for eventuelle sårbarheder.

Fysisk sikring af lokaliteter, hvor der behandles personoplysninger: Databehandleren skal sikre fysisk sikring af lokaliteter, hvor der behandles personoplysninger, hvorfor beskyttelsen også skal afspejle fysisk beskyttelse mod risici for forhold, som kan bringe personoplysningerne i fare, ødelægge data eller komme i uvedkommendes varetægt. Det skal således sikres, at når udstyr og mobile enheder ikke anvendes, skal udstyret og enhederne være låst med adgangskode og/eller være låst inde. Kontorer og bygninger skal være aflåst, når de forlades. Lokationer med adgang til personoplysninger skal være under videoovervågning.

Hjemmearbejdspladser: Hjemmearbejdspladser skal være beskyttet på tilsvarende måde som arbejdspladser i databehandlingsfaciliteterne. I tilfælde, hvor en medarbejder gør brug af hjemme-/fjernarbejdspladser, må computere og andre enheder aldrig forlades uden at

være låst eller slukket. Der skal være indført 2-faktor-validering for at sikre uvedkommende ikke kan få adgang til personoplysninger. Adgang til virksomhedens netværksressourcer, herunder også adgang til systemer, skal ske via VPN.

Patch Management: Databehandleren er forpligtet til løbende og inden for rimelig tid at anvende værktøjer til sårbarhedsscanninger og derefter sikkerhedsopdatere alle enheder og systemer, hvorfra der tilgås personoplysninger.

Adgangsrettigheder: Databehandleren skal sikre, at modstridende funktioner og ansvarsområder adskilles så vidt muligt for at nedsætte muligheden for uautoriseret eller utilsigtet anvendelse, ændring eller misbrug af den dataansvarliges informationsaktiver. I tilfælde, hvor det er særligt vanskeligt eller ikke kan lade sig gøre at gennemføre egentlig funktionsadskillelse, skal andre sikkerhedsforanstaltninger iværksættes gennem overvågning af aktiviteter, tilsyn og lignende.

Databehandleren skal sikre, at adgangsrettigheder løbende bliver gennemgået, således at ansatte kun har adgang til de personoplysninger, der er nødvendige for vedkommendes jobfunktion. I tilfælde hvor en medarbejder fratræder sin stilling eller tiltræder en anden stilling, skal Databehandleren sikre at adgangsrettigheder lukkes eller ændres.

Adgangsbegrænsninger baseret på tofaktorgodkendelse (2FA), såsom MitID eller MitID erhverv eller andre lignende teknologier, er underlagt ekstra omkostninger, som kunden skal betale. Visse 2FA/MFA-teknologier vil ikke være tilgængelige, medmindre kunden har valgt sådanne moduler.

C.3 Bistand til den dataansvarlige

Databehandleren skal så vidt muligt – inden for det nedenstående omfang og udstrækning – bistå den dataansvarlige i overensstemmelse med Bestemmelse 9.1 og 9.2 ved at gennemføre følgende tekniske og organisatoriske foranstaltninger:

- Teknisk support: Databehandleren skal yde løbende teknisk support til den dataansvarlige i forbindelse med implementering, vedligeholdelse og drift af databehandlingsaktiviteterne.

- Incident response: Databehandleren skal bistå den dataansvarlige i tilfælde af databrud eller sikkerhedsincidenter ved at deltage i undersøgelsen, indrapporteringen og afhjælpningen af sådanne hændelser.

- Bistand med registreredes rettigheder: Databehandleren skal bistå den dataansvarlige i opfyldelsen af forpligtelser vedrørende registreredes rettigheder. Dette omfatter, men er ikke begrænset til:
    - At reagere på anmodninger om adgang til personoplysninger.
    - At lette rettelse eller sletning af data.
    - At støtte dataoverførsel, hvis relevant.
    - At håndtere anmodninger om begrænsning af databehandling.

- Bistand ydes inden for rimelige tekniske og praktiske rammer. Hvis en anmodning kræver væsentlige ressourcer, kan databehandleren kræve betaling for denne bistand, medmindre andet er aftalt.

De specifikke tekniske og organisatoriske foranstaltninger, som databehandleren skal gennemføre for at bistå den dataansvarlige, inkluderer:

- Implementering af sikkerhedsforanstaltninger: Databehandleren skal implementere passende tekniske og organisatoriske sikkerhedsforanstaltninger for at beskytte personoplysninger mod uautoriseret adgang, ændring, tab eller ødelæggelse.

- Datafortrolighed og -integritet: Databehandleren skal sikre, at personoplysninger behandles fortroligt og med integritet, herunder sikkerhedskopiering og hensigtsmæssige procedurer for at sikre datasikkerhed og -integritet.

- Adgangskontrol: Databehandleren skal implementere adgangskontrolmekanismer for at sikre, at kun autoriserede personer har adgang til personoplysninger i overensstemmelse med gældende adgangsrettigheder og -beføjelser.

- Overvågning og revision: Databehandleren skal etablere mekanismer til overvågning og revision af databehandlingsaktiviteter for at identificere og reagere på eventuelle sikkerhedsrisici eller brud på databeskyttelsesbestemmelser.

- Denne bistand skal udføres effektivt og professionelt for at sikre, at den dataansvarlige kan opfylde sine forpligtelser som fastsat i databeskyttelseslovgivningen.

Alle ydelser, der ikke er direkte påkrævet i forbindelse med databrud eller registreredes rettigheder, betragtes som betalbare supportydelser og kræver separate aftaler.

C.4 Opbevaringsperiode/sletterutine

Data opbevares, medmindre den dataansvarlige sletter dem via vores system.

Ved opsigelse af kontoen gemmes data indtil ophør, og slettes derefter inden for 90 dage fra sikkerhedskopier. Data, som skal opbevares længere ifølge dansk eller EU-lovgivning, opbevares i overensstemmelse med disse krav.

Brugeroprettelse og Ansvar:

Slutbrugere (modtagere af kontrakter eller tilbud) kan oprette egne konti og indgå direkte aftale med Signit.com. Deres data slettes ikke, selvom den dataansvarliges konto ophører.
Slutbrugeres adgang til dataansvarliges data og funktioner slettes ved opsigelse af dataansvarliges konto.

Medarbejdere:

Medarbejdere inviteret til virksomhedskontoen registrerer også en privat konto, medmindre virksomheds-specifikke e-mails eller digitale identifikatorer (f.eks. MitID Erhverv, ADFS) bruges. Ved opsigelse slettes medarbejderens adgang til virksomhedens data, men deres private konto opretholdes.

Elev og Forældreportal:

Elever, Forældre og værger, der opretter konti via elev og forældreportalen, får adgang til børns data. Disse brugere indgår direkte aftale med Signit.com, og deres data opretholdes. Adgang til data registreret under dataansvarliges konto slettes ved opsigelse, men forældre- og værgekontoen opretholdes.

Nye Brugere og Signerede Dokumenter:

Når dataansvarlige sender dokumenter til underskrift af personer (f.eks. nye medarbejdere) med private e-mailadresser (f.eks. Gmail), kan disse personer oprette en konto inden for 60 dage for at få adgang til de underskrevne dokumenter ved at validere deres e-mailadresse.
De underskrevne dokumenter tilhører både den dataansvarlige og den private Signit.com-konto. Hvis den dataansvarlige sletter sin konto hos Signit.com, slettes dokumenterne ikke fra den private Signit.com-konto.

C.5 Lokalitet for behandling

Behandling af de af Bestemmelserne omfattede personoplysninger kan ikke uden den dataansvarliges forudgående skriftlige godkendelse ske på andre lokaliteter end følgende:

Behandlingen er begrænset til at finde sted på de i bilag B, afsnit B.1 anførte lokaliteter samt eventuelle hjemmearbejdspladser.

C.6 Instruks vedrørende overførsel af personoplysninger til tredjelande

Databehandleren skal forud for overførsel af den dataansvarliges personoplysninger til tredjelande identificere og indgå et passende overførselsgrundlag og sikre, at overførslen af personoplysninger kan ske på lovlig vis.

Såfremt der er tredjelandeoverførsler:

Overførslen af personoplysninger skal ske på ét af følgende mekanismer:

- Retligt bindende instrumenter mellem myndigheder
- Bindende virksomhedsregler
- Adfærdskodeks og certificeringsmekanismer
- Europa-Kommissionens standardbestemmelser om databeskyttelse (SCC)
- Ad-hoc kontrakter

I forbindelse med overførsel af personoplysninger til tredjelande, jf. afsnit 8, godkender den dataansvarlige hermed anvendelsen af Europa-Kommissionens standardbestemmelser om databeskyttelse (SCC) med underdatabehandlere udenfor EU/EØS som overførelsesgrundlag.

Ved anvendelse af Europa-Kommissionens standardbestemmelser om databeskyttelse (SCC) som grundlag for overførsel af personoplysninger udenfor EU/EØS, er databehandleren forpligtiget til at implementere og overgå til de nye standardbestemmelser pr. 27. december 2022.

Databehandleren forpligter sig endvidere til at udarbejde Transfer Impact Assessment (TIA) for de overførsler af personoplysninger, som sker til usikre tredjelande med henblik på at afgøre, om behandlingen kan ske i overensstemmelse med reglerne for tredjelandsoverførsler.

I forbindelse med overførsel til underdatabehandlere udenfor EU/EØS vil overførselsgrundlaget være EU-Kommissionens tilstrækkelighedsafgørelse EU-U.S. Data Privacy Framework ved overførsler til USA. Såfremt denne tilstrækkelighedsafgørelse vurderes ugyldig ved EU-Domstolen eller hvis de specifikke underdatabehandlere ikke er certificeret herunder, forpligter databehandleren sig til at anvende EU-Kommissionens gældende standardbestemmelser om databeskyttelse (SCC) som overførselsgrundlag. I den forbindelse forpligter databehandleren sig endvidere til at udarbejde Transfer Impact Asessment (TIA) for de overførsler af personoplysninger, som sker til usikre tredjelande med henblik på at afgøre, om behandlingen kan ske i overensstemmelse med databeskyttelsesforordningen.

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

Den dataansvarlige kan efter behov, vederlagsfrit og skriftligt, få besvaret spørgsmål i forbindelse med den dataansvarliges lovpligtige kontrol af databehandleren. Kontrollen indebærer databehandlerens overholdelse af denne databehandleraftale, samt databehandlerens overholdelse af Databeskyttelsesforordningen og andre databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse bestemmelser.

Der er enighed mellem parterne om, at følgende typer af revisionserklæringer kan anvendes i overensstemmelse med en revisionserklæring:

ISAE 3000
ISAE 3402
ISO 27001/2
ISO 27701
SOC2

Revisionserklæringen fremsendes uden unødig forsinkelse til den dataansvarlige til orientering.
Hvis den dataansvarlige har spørgsmål eller bemærkninger til rammerne for eller metoden i erklæringen, kan dette drøftes med databehandleren, og begge parter skal i fællesskab forsøge at finde en løsning, der sikrer, at revisionen opfylder kravene i gældende lovgivning og parternes aftaler.

Baseret på resultaterne af erklæringen er den dataansvarlige berettiget til at anmode om yderligere foranstaltninger for at sikre overholdelsen af databeskyttelsesforordningen, relevante databeskyttelsesbestemmelser og denne databehandleraftale. Databehandleren forpligter sig til at samarbejde i rimeligt omfang om sådanne foranstaltninger.

Såfremt parterne ikke kan nå til enighed om nødvendige foranstaltninger, kan spørgsmålet håndteres efter opsigelsesbestemmelserne i hovedaftalen. Opsigelse er alene muligt, hvis det er klart, at manglende overholdelse af standarder udgør en væsentlig misligholdelse af denne aftale eller hovedaftalen.

C.8 Tilsyn med underdatabehandlere

Databehandleren skal sikre, at alle underdatabehandlere, der anvendes til behandling af personoplysninger på vegne af den dataansvarlige, overholder de samme databeskyttelsesforpligtelser, som er fastsat i denne databehandleraftale, og som pålægges databehandleren i henhold til Databeskyttelsesforordningen og gældende lovgivning.

For at sikre dette forpligter databehandleren sig til følgende tilsynsforanstaltninger:

1. Kontraktuelle krav:
   Databehandleren sikrer, at der indgås en skriftlig aftale med underdatabehandlere, som indeholder krav svarende til dem, der er fastsat i denne databehandleraftale, herunder krav om sikkerhedsforanstaltninger, databehandlingens formål, og bistand til den dataansvarlige i opfyldelse af registreredes rettigheder.

2. Løbende kontrol og tilsyn:
   Databehandleren udfører regelmæssigt tilsyn med underdatabehandlernes overholdelse af de kontraktuelle krav, herunder:

   - Indhentelse og vurdering af relevante certificeringer, auditrapporter eller revisionserklæringer, såsom ISAE 3000, ISO 27001 eller SOC2.
   - Gennemgang af underdatabehandlernes sikkerhedsforanstaltninger og procedurer.
   - Regelmæssig dialog og rapportering om databeskyttelsesforanstaltninger.

3. Håndtering af brud og manglende overholdelse:
   Hvis databehandleren bliver opmærksom på, at en underdatabehandler ikke lever op til sine forpligtelser, træffer databehandleren straks

nødvendige foranstaltninger for at sikre overholdelse, herunder opsigelse af aftalen med underdatabehandleren, hvis det er påkrævet.

4. Orientering af den dataansvarlige:
Den dataansvarlige orienteres om anvendelsen af nye underdatabehandlere og om eventuelle væsentlige mangler i overholdelsen, som opdages under tilsynet. Den dataansvarlige kan anmode om yderligere oplysninger om underdatabehandlere efter behov.

5. Registrering af underdatabehandlere:
Databehandleren skal føre en opdateret oversigt over alle anvendte underdatabehandlere og stille denne til rådighed for den dataansvarlige efter anmodning.

Bilag D Parternes regulering af andre forhold

D.1. Servicegebyr for Compliance-dokumentation og Revisionserklæringer

Kunden kan indgå en særskilt Kundespecifik Databehandleraftale (KSDBA) efter behov. Fremsendelse af Signit.dk ApS' generelle, periodiske revisionserklæringer (såsom ISAE 3402, ISAE 3000, SOC2, eller lignende) er underlagt et servicegebyr for dokumentationshåndtering, som fastsat i de generelle vilkår (jf. afsnit 10.14), medmindre andet er aftalt i KSDBA'en eller en Individuel Hovedaftale.

Gebyr for fremsendelse af revisionserklæring:

Hvor intet andet er specifikt aftalt i en Individuel Hovedaftale (jf. afsnit 14.1 i de generelle vilkår), opkræves et servicegebyr på 5.000 DKK (ekskl. moms for erhverv/offentlig) pr. henvendelse for fremsendelse af en kopi af Signit.dk ApS' generelle, periodiske revisionserklæring.

Undtagelser fra gebyret:

Kunder på en Enterprise-plan eller kunder, der har indgået en separat Kundespecifik Databehandleraftale (KSDBA), hvori levering af specifik revisionserklæring er indregnet, er undtaget fra dette gebyr.

Gebyret dækker alene fremsendelse af eksisterende dokumentation og dækker ikke udarbejdelse af en ny, kundespecifik erklæring. Udarbejdelse af en ny kundespecifik erklæring kræver særskilt skriftlig aftale og faktureres efter forbrug.