STEPTO Databehandleraftale

Standardkontraktsbestemmelser

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

mellem

Navn	STEPTO A/S
Adresse	Juelstrupparken 10A
	9530 Støvring
CVR/VAT	DK31600413

Navn	Margrethe Brandt
Titel	Direktør
Telefon	40255010
Mail	margrethe@stepto.dk

herefter "databehandleren"

og

Jer som kunde

herefter "den dataansvarlige"

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.

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 de i bilag D aftalte tjenesteydelser 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 indeholder parternes "hovedaftale", herunder instruks og leveringsbetingelser.
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 EØS-medlemsstaternes 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.

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 samlet være specificeret i bilag A, C og D. 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 45 dages forudgående 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. Databehandleren skal i sin aftale med underdatabehandleren indføje den dataansvarlige som begunstiget tredjemand i tilfælde af databehandlerens konkurs, således at den dataansvarlige kan indtræde i databehandlerens rettigheder og gøre dem gældende over for underdatabehandlere, som f.eks. gør den dataansvarlige i stand til at instruere underdatabehandleren i at slette eller tilbagelevere personoplysningerne.
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.

8. Overførsel af oplysninger 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 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 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.

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 Datatilsynet inden 72 timer, 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 D 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 tilbagelevering af oplysninger

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

   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 nærmere angivet i Bilag C.7. og C.8.
3. Databehandleren er forpligtet til at give tilsynsmyndigheder, som efter gældende lovgivning har adgang til den dataansvarliges eller databehandlerens faciliteter, eller repræsentanter, der optræder på tilsynsmyndighedens vegne, adgang til databehandlerens fysiske faciliteter mod behørig legitimation.

13. Parternes aftaler om andre forhold

1. Parterne kan aftale andre bestemmelser vedrørende tjenesten og 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 accept 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 skriftligt varsel af begge parter.

Bilag A. Oplysninger om behandlingen

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

Personkategori	Formål
Dataansvarliges kunder	For at kunne lave bogføringsservice og bilagshåndtering i henhold til kundeaftale.
Dataansvarliges leverandører	For at kunne lave bogføringsservice og bilagshåndtering i henhold til kundeaftale.
Dataansvarliges ansatte	For at kunne lave lønadministration i henhold til kundeaftale.

A.2. Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige drejer sig primært om de i Bilag D eller hovedaftalen beskrevne ydelser (karakteren af behandlingen)

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

Almindelige persondata (f.eks. navn, adresse, e-mail, telefonnummer mv.).

Fortrolige persondata (CPR-nummer)

A.4. Behandlingen omfatter følgende kategorier af registrerede

Personkategori	Beskrivelse
Dataansvarliges kunder	Personer, som er eller har været kunder hos den dataansvarlige, eller er potentielle kunder.
Dataansvarliges leverandører	Personer som er eller har været forretningsforbindelser, herunder leverandører og samarbejdspartnere hos den dataansvarlige, eller er potentielle forretningsforbindelser
Dataansvarliges ansatte	Personer, som er eller har været ansatte/bestyrelsesmedlemmer hos den dataansvarlige.

A.5. Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige kan påbegyndes efter disse Bestemmelsers ikrafttræden. Behandlingen har den i Bilag D eller hovedaftalen anførte varighed

Bilag B. Underdatabehandlere

B.1. Godkendte underdatabehandlere

Leverandør	Land	Lovligt grundlag for processering uden for EU	Funktion
Visma Dataløn A/S	Danmark		Lønadministration
Systemgruppen	Danmark		Fillagring og backup for STEPtool - digital bilagshåndtering
Microsoft C5 (kundeopgaver)	Irland		Bogføring

Ved Bestemmelsernes ikrafttræden har den dataansvarlige godkendt brugen af ovennævnte 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 eller gøre brug af en anden underdatabehandler til denne behandlingsaktivitet.

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 den i hovedaftalen/kontrakt eller i bilag D beskrevne behandling

C.2. Behandlingssikkerhed

Følgende sikkerhedsforanstaltninger er truffet:

Hvis der er tale om behandling af fortrolige, følsomme eller særlige kategorier af personoplysninger, skal der altid etableres et ”højt” sikkerhedsniveau.

Sikkerhedspolitik:

Firewall

Der er etableret og løbende vedligeholdt en firewall, som sikrer gennemførelse af virksomhedens sikkerhedspolitik, herunder har Stepto opsat en Sonicwall (firewall) på hver af deres lokationer, der har aktiveret CFS (Content Filtering Service) hvilket går ind og blokere for harmfulde hjemmesider.

Opdateringer

Servere og computere ajourføres løbende med sikkerhedsopdateringer, som sikrer mod ondsindet udnyttelse af sårbarheder i de anvendte programmer. Stepto har server i et delt servermiljø, der hver måned bliver opdateret med de sidste nye sikkerhedsopdateringer, samt har alle deres klienter installeret Heimdal antivirus, der har en patch management feature, der sørger for opdatering både til selve maskinens styresystem men også programmerne.

Antivirus

Der er etableret et virusværn, som løbende holdes ajourført . Stepto har i dag Heimdal Antivirus, hvor Systemgruppen laver en manuel gennemgang hver fredag for at se om der har været nogle udfald på Steptos maskiner.

Internet og e-mail

Opsætning af sikkerhedsindstillingerne i browseren og e-mail programmet på de enkelte computere er etableret, så der opnås den ønskede sikkerhedspolitik omkring websteder, cookies og modtagelse af eksekverbar kode (plug-ins, m.v.). Dette håndteres af Heimdal Antivirus som løbende monitorerer og blokerer uhensigtsmæssige hjemmesider/mails.

Overførsel af følsomme data

Når der sker overførsel af personfølsomme data sker det via sikre kanaler såsom e-signatur og krypterede mails. Dette gælder også for overførsel af evt. login oplysninger. Herudover er det via medarbejderinstruks angivet overfor medarbejderne at der skal udvises særlig agtpågivenhed når sådanne data sendes, særligt at der bliver sendt til korrekt modtaget.

Logning

Det registreres, hvis der er forgæves forsøg på at få adgang til it-systemer med følsomme personaleoplysninger. Hvis der bliver foretaget for mange loginforsøg på en konto vil den automatisk blive låst i systemet, samt vil Systemgruppen i loggen kunne se hvad der forårsager låsningen.

Fjernadgang

Der er dobbelt logon (2-factor) ved fjernadgang til virksomhedens IT-systemer. Til dette har Stepto opsat DUO Cloud security, hvilket Stepto bruger til 2-factor login remote.

Sletning

Det udføres løbende kontrol med at der gennemføres sletning af personoplysninger, ud fra hvad der er beskrevet i den interne fortegnelse.

Adgang

Systemer sættes op, så ansatte kun har adgang til de personoplysninger, som de har brug for i forbindelse med løsning af deres arbejdsopgaver. Hertil kan det tilføjes at når en ny bruger bliver oprettet, så bliver der defineret hvad der skal gives adgang til, hvor der ellers vil være lukket for alt andet

It værktøjer

Systemet sættes op, så det er enkelt for de ansatte at arbejde med personfølsomme data, således det foregår på en sikker og forsvarlig måde. Herunder at personfølsomme data kan sendes sikkert via e-signatur og krypteret.

Backup

Der bliver taget backup af Steptos serversetup hver dag. Denne bliver gemt på flere forskellige lokationer. Derudover er der også backup af Steptos maildata.

Organisatoriske sikkerhedsforanstaltninger:

- Alle medarbejdere er instrueret i beskyttelsen af personoplysninger og har underskrevet en medarbejderinstruks.
    - Medarbejderinstruksen opdateres og gennemgås mindst en gang årligt.
    - Medarbejderinstruksen gennemgås altid med nye medarbejdere i forbindelse med ansættelsen.
- Alle medarbejdere er pålagt tavshedspligt.
- Det overordnede ansvar for overholdelse af sikkerhedskravene, ligger ved databehandlerens ledelse, som typisk repræsenteres af IT-chefen.
- Persondata er kun tilgængelige for de medarbejdere der har en godkendelse og årsag til at skulle kunne tilgå disse data, og skal altid behandles fortroligt.
- Hvis der er tale om en stor mængde følsomme personoplysninger, så bør data adskilles hvor det er muligt, således at adgangen begrænses til absolut minimum.

Fysiske sikkerhedsforanstaltninger:

- Kontorer og bygninger aflåses, når de forlades.
- Sikre at driften kan fortsætte ved strømafbrydelser og evt. redundante kommunikationsforbindelser
- Arkiver med følsomme personoplysninger opbevares altid aflåst, hvor der ligeledes er alarm og overvågning etableret.
- Backup opbevares aflåst (både interne og eksterne), der laves en løbende genindlæsningstest, således at det sikres at backup'en virker og indeholder valide data.
- Alle fysiske medier (papir, USB drev mv.) destrueres på forsvarligvis, hvis de har været benyttet til at opbevare persondata.

Driftsmæssig sikkerhed.

- Udvikling, Test og Produktionsmiljøer er adskilte.
    - Udvikling og Test foretages af forskellige personer.
- Der tilpasses og kontrolleres løbende kapaciteter i forhold til opretholdelse af driften.
- Løbende password skift på både interne og eksterne systemer.
- Logning af afviste logon forsøg med automatisk alarmering.

C.3. Bistand til den dataansvarlige

Databehandleren skal så vidt muligt, bistå den dataansvarlige i overensstemmelse med Bestemmelse 9.1 og 9.2 ved at gennemføre de i Bilag C.2 angivne tekniske og organisatoriske foranstaltninger.

C.4. Opbevaringsperiode / sletterutine

Personoplysninger opbevares hos databehandleren, indtil den dataansvarlige anmoder om at få oplysningerne slettet eller tilbageleveret, med mindre andet er aftalt i Bilag D / hovedaftalen eller i særlige vilkår.

Ved ophør af tjenesten vedrørende behandling af personoplysninger, skal databehandleren enten slette eller tilbagelevere personoplysningerne i overensstemmelse med bestemmelse 11.1, medmindre den dataansvarlige - efter underskriften af disse bestemmelser - har ændret den dataansvarlige oprindelige valg. Sådanne ændringer skal være dokumenteret og opbevares skriftligt, herunder elektronisk, i tilknytning til bestemmelserne.

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 databehandlerens eller underdatabehandlerens lokaliteter

C.6. Instruks vedrørende overførsel af personoplysninger til tredjelande

Databehandleren overfører ikke personoplysninger til tredjelande, undtagen til de generelt godkendte underdatabehandlere listet i Bilag B

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

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

Databehandleren skal hvert andet år for egen regning indhente en erklæring/inspektionsrapport fra en uafhængig tredjepart vedrørende databehandlerens overholdelse af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser.

Der er enighed mellem parterne om, at der kan anvendes følgende type af erklæring

”Underskrevne uafhængige tredjepart (Navn, adresse, kontaktperson, telefon, email, evt. DPO med angivelse af navn, adresse, tlf og mail bekræfter at have gennemgået de tekniske og organisatoriske sikkerhedsforanstaltninger, som databehandleren har oplyst til den dataansvarlige i forbindelse med indgåelse af denne databehandleraftale.”

Erklæringen/inspektionsrapporten synliggøres/fremsendes uden unødig forsinkelse til den dataansvarlige til orientering. Den dataansvarlige kan anfægte rammerne for og/eller metoden i erklæringen/inspektionsrapporten og kan i sådanne tilfælde anmode om en ny erklæring/inspektionsrapport under andre rammer og/eller under anvendelse af anden metode.

Baseret på resultaterne af erklæringen/inspektionsrapporten, er den dataansvarlige berettiget til at anmode om gennemførelse af yderligere foranstaltninger med henblik på at sikre overholdelsen af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser.

Den dataansvarlige eller en repræsentant for den dataansvarlige har herudover adgang til at foretage inspektioner, herunder fysiske inspektioner, af 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 nødvendig, Vurderingen skal bero på fakta og ikke fornemmelse. Fysisk inspektion kræver forudgående aftale med databehandlerne, og med et forudgående varsel på 3 uger, så databehandleren er forberedt på at kunne afsætte de nødvendige ressourcer til det.”

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.

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

Databehandlerens revisioner, herunder inspektioner, med behandlingen af personoplysninger, som er overladt til underdatabehandleren, sker på samme måde som den dataansvarliges revisioner hos databehandleren, se punkt C.7.

Bilag D. Parternes regulering af andre forhold, herunder instruks vedr. behandling af personoplysninger

Instruks
STEPTO behandler kun personoplysninger efter dokumenteret instruks fra den dataansvarlige.

STEPTO's kundeaftale, aftale om brug af STEPtool og denne databehandleraftale udgør denne instruks. Instruksen omfatter bogføring, lønadministration og bilagshåndtering i STEPtool.

Se det mellem parterne indgåede aftalegrundlag.

Brud på datasikkerheden
Hvis der sker brud på datasikkerheden, skal databehandler medsende dokumentation for de faktiske omstændigheder ved bruddet, dets virkninger, de trufne afhjælpende foranstaltninger, og hvis databehandleren har fået bemyndigelse til at foretage underretning til de registrerede, at oplyse om der er foretaget underretning til de registrerede og i givet fald hvorledes.

Dato: 19.09.2022