Version 1.0.4
Databehandleraftale mellem

Dataejer: Skolevisioner ApS, Ry Væksthus, Ellemosen 3, 8680 Ry, CVR nr. 30535421

Databehandler: CreativeMinds IVS, Kærgade 33, 8940 Randers SV, CVR nr. 37659223

01. Databehandleraftale

01.01 Aftalens formål

Aftalens formål er at regulere rettigheder og forpligtelser i relation til behandling af personfølsomme oplysninger. Aftalen skal sikre, at data-subjekters personfølsomme oplysninger ikke bliver anvendt ulovligt, eller kommer uberettiget i hænderne på 3. part.

Aftalen vedrører databehandlerers anvendelse af data på vegne af dataejeren, herunder indsamling, optagelse, opbevaring, behandling og sletning, eller en kombination af disse.

01.02 Roller i samarbejdet

Databehandleren er en virksomhed der er specialiseret i at udvikle, drifte og supporte software. Dataejeren køber konsulentbistand hos databehandleren. Konsulentbistanden omfatter bl.a. udvikling af software der bruges til håndtering af personfølsomme oplysninger, samt drift og support af systemer der indeholder personfølsomme oplysninger. Databehandlern har adgang til driftsystemer, og vil i supportsammenhæng kunne hjemtage produktionsdata, og kan derfor betegnes som databehandler.

01.03 Databehandlerens forpligtelser

Under behandling af personfølsomme data skal medarbejdere hos databehandleren følge de rutiner og instruktioner som dataejeren angiver.

Medarbejdere hos databehandleren, der har adgang til personfølsomme oplysninger på vegne af databehandleren, skal i forhold til håndtering af personfølsomme oplysninger opfylde kravene i denne aftale. Derudover skal de underskrive en fortrolighedserklæring der udleveres af dataejeren. Databehandleren skal implementere regler og procedurer i denne aftale på en måde der sikrer, at medarbejdere der har adgang til personfølsomme oplysninger er i stand til at overholde alle elementer i denne aftale.

01.04 Dataejerens forpligtelser

Dataejeren er ansvarlig for månedlige og årlige sikkerhedsreviews, og inddrager databehandleren i det omfang det er nødvendigt.

Dataejeren er ansvarlig for sikkerhedsreviews og checklister i forbindelse med ny release af produktionssoftware og nyt produktionsmiljø, og inddrager databehandleren i det omfang det er nødvendigt.

01.05 Anvendelse af underleverandører

Databehandleren må ikke anvende underleverandører til behandling af personfølsomme oplysninger på vegne af dataejeren. Det er databehandlerens ansvar at sikre, at dennes eventuelle underleverandører ikke får adgang til personfølsomme oplysninger.

01.06 Sikkerhedsaudit

Databehandler skal stille personale og dokumentation til rådighed i forbindelse med sikkerhedsaudits, der gennemføres på foranledning af dataejeren.

01.07 Aftalens varighed

Aftalen er gældende så længe databehandleren behandler personfølsomme oplysninger for dataejeren. I forbindelse med krænkelser af denne aftale kan dataejeren instruere databehandleren om at stoppe videre behandling af data med umiddelbar virkning.

Aftalen vil automatisk ophøre, når én eller begge parter ophører samarbejdet i overensstemmelse med den generelle samarbejdsaftale mellem parterne.

01.08 Ophør af aftalen

Ved ophør af denne aftale skal databehandleren slette eller destruere alle medier, der indeholder personfølsomme oplysninger, på en måde der umuliggør genskabelse af data.

01.09 Notifikationer

Notifikationer i forbindelse med denne aftale skal sendes på mail til: info@skolevisioner.dk

01.10 Valg af lov og domstol

Aftalen af omfattet af dansk lov, og eventuelle tvister skal behandles ved en dansk domstol.

02. Generelle procedurer omkring informationssikkerhed

02.01 Impersonering af brugere

Impersonering af brugere må kun finde sted, når mindst én af følgende betingelser er opfyldt:

1) Kunden er indforstået med, at en bruger impersoneres
2) Impersonering foretages i kundens interesse, f.eks. i forbindelse med support eller fejlfinding.

Al impersonering skal foregå i inkognito/privat tilstand. Det kan gøres i følgende browsere:

1. Google Chrome: Ny Inkognito-fane (Ctrl+Shift+N)
2. Mozilla Firefox: Nyt privat vindue (Ctrl+Shift+P)
3. Safari: Start privat browsing
4. Internet Explorer: New tab + Start InPrivate Browsing

Hvis det er nødvendigt at downloade filer med personfølsomme oplysninger i forbindelse med hjælp og support, skal disse håndteres efter retningslinierne i nedenstående afsnit.

02.02 Flytte og gemme personfølsomme oplysninger

Personfølsomme oplysninger må aldrig udskrives på papir.

Filer med personfølsomme oplysninger skal håndteres efter følgende retningslinier:

1) Al overførsel af filer over det åbne Internet skal foregå via en krypteret forbindelse.
2) Filer skal efter brug slettes permanent med værktøjet "File Shredder" (http://www.fileshredder.org/) eller et tilsvarende værktøj, som giver samme grad af sikkerhed for at filen ikke kan genskabes.
3) Filer må aldrig gemmes i Dropbox, Google Drev, OneDrive eller andre mapper der automatisk kopierer data til skyen.
4) Filer må aldrig sendes via email.

Personfølsomme oplysninger må aldrig udleveres til andre, med mindre dataejer har givet skriftlig instruks om denne udlevering.

02.03 Fysisk udstyr

02.03.01 Anskaffelse og installation af nyt fysisk udstyr med drev

Før nyt fysisk udstyr med drev anvendes til midlertidig lagring af personfølsomme oplysninger, skal der installeres et program som f.eks. "File Shredder", som gør det let at slette filer permanent på en sikker måde.

Derudover skal der installeres et anerkendt anti-virus program på alle personlige computere, der anvendes til at tilgå personfølsomme oplysninger.

02.03.02 Anskaffelse og installation af nyt fysisk udstyr uden drev

Fysisk udstyr uden drev kan f.eks. være router, switche eller andet netværksudstyr, som indgår i håndteringen af persondata.

Der skal ved anskaffelse og installation sikres, at der anvendes kryptering af alle trådløse forbindelser, der anvendes til transmission af personfølsomme oplysninger.

02.03.03 Bortskaffelse af fysisk udstyr med drev

Når udstyr ikke længere skal anvendes efter de ovenstående retningslinjer, skal alle fysiske drev der indeholder personfølsomme data slettes permanent, på en måde der forhindrer genskabelse af data, før maskinen kan overgå til anden brug.

02.03.04 Reparation af fysisk udstyr med drev

Fysisk udstyr der indeholder drev må ikke sendes til reparation, med mindre alle personfølsomme oplysninger er slettet permanent.

02.03.05 Sikring mod tyveri

Stationære computere der anvendes til håndtering af personfølsomme oplysninger skal opbevares i lokaler, der er aflåste, når de ikke benyttes, samt er forsynede med tyverialarm.

Bærbare computere der anvendes til håndtering af personfølsomme oplysninger skal opbevares forsvarligt, og må aldrig efterlades uden opsyn med mindre det er i aflåste lokaler eller biler.

02.04 Password politik

Passwords der anvendes til beskyttelse af personfølsomme oplysninger skal bestå af mindst 8 tegn, og indeholde mindst 3 ud af de fire følgende typer tegn: Små bogstaver, store bogstaver, tal og tegn.

02.05 Personlig konto

Alle, der har adgang til personfølsomme oplysninger skal have dette gennem en personlig konto. Dette gælder også for konti som Databehandler opretter til brugere af systemet.

02.06 Tildeling af brugerrettigheder

Tildeling af brugerrettigheder, der giver adgang til personfølsomme oplysninger, må kun ske hvis der er sikkerhed for, at kontoen der tildeles rettigheder er berettiget til det. Dette kan f.eks. være via en email, der er sendt fra et anerkendt domæne, eller en verifikation af brugerens lederrolle via EMU brugeradministration og skolens hjemmeside.

03. Ledelsesprocedurer omkring informationssikkerhed

03.01 Ny ansat eller skift i ansvarsområder

Hvis en person ansættes eller får nye arbejdsopgaver, og dermed får adgang til kunders personfølsomme oplysninger, skal medarbejderen orienteres om dataejers sikkerhedspolitikker, samt underskrive en fortrolighedserklæring der udleveres af dataejeren.

04. Krav til driftsystemer der anvendes til håndtering af personfølsomme data

04.01 Password politik indbygget i systemer

Driftsystemer skal i videst muligt omfang sikre, at passwords der anvendes til beskyttelse af personfølsomme oplysninger skal bestå af mindst 8 tegn, og indeholde mindst 3 ud af de fire følgende typer tegn: Små bogstaver, store bogstaver, tal og tegn.

Systemerne skal bygges, så de lægger op til at der anvendes personlige brugerkonti.

Der må ikke være mulighed for at anvende "Husk mig" funktioner. Brugernavne og passwords skal skrives hver gang man som bruger logger ind.

04.02 Passwords må ikke foreligge i klar tekst

Driftsystemer skal gemme brugerpasswords krypteret, på en måde der forhindrer at passwords kan genskabes.

04.03 Blokering af gentagne loginforsøg

Ved gentagne fejlslagne forsøg på login for en brugerkonto skal systemerne låse den relevante brugerkonto i et tidsrum.

04.04 Logning

Driftsystemer skal opbygges, så der bliver foretaget logning af al aktivitet på hjemmesiden, inklusiv de IP adresser aktiviteten foregår fra.

Derudover skal der logges følgende hændelser i en specifik logfil:

1) Administratorer, der tilgår personfølsomme oplysninger.
2) Brugere, der tilgår personfølsomme oplysninger.

Logfiler opbevares i mindst 6 måneder.

04.05 Separation af data

Driftsystemer skal opbygges, så:

1) Der er sikker separation af de enkelte kunders data
2) Der er indbyggede mekanismer der sikrer, at den enkelte brugerkonto kun kan tilgå relevante informationer

04.06 Oversigt over brugere

Der skal være mulighed for oprettelse af en særlig brugerkonto hos kunden, som giver adgang til:

1. Se hvilke brugere der har adgang hos kunden
2. Inaktivere brugere, så de ikke længere har adgang til at logge ind

04.07 Krypteret forbindelse

Driftssystemer der udveksler data over det åbne internet skal fungere ved hjælp af en krypteret forbindelse.

Version 1.0.4

05. Procedurer omkring informationssikkerhed for teknikere

05.01 Tilgang til og manipulation af data

Tilgang til data udenom driftsystemerne må kun finde sted, når mindst én af følgende betingelser er opfyldt:

1) Kunden er indforstået med, at personfølsomme oplysninger tilgåes
2) Tilgang til data foretages i kundens interesse, f.eks. i forbindelse med support eller fejlfinding.

Manipulation af data udenom driftsystemerne skal som udgangspunkt undgås. Hvis manipulation skønnes nødvendig, skal alle følgende kriterier være opfyldt for at det må foregå:

1. Der må ikke ændres i afgivne personoplysninger, med mindre det er på opfordring fra den registrerede, eller i den registreredes åbenbare interesse.
2. Der må ikke ændres i øvrige data, med mindre det er på kundens opfordring eller i kundens åbenbare interesse.

På vegne af Skolevisioner ApS	På vegne af CreativeMinds IVS
Navn: Tanja Lang Flaaten	Navn: Steen Fredberg Tøttrup
Dato og sted: 7/11 - 17	Dato og sted: 7-11-2017
Underskrift:	Underskrift