Persondatahåndbog

Skolevisioner ApS - CVR-nr.: 30535421

Sidst revideret:
26-06-2019

Indholdsfortegnelse

1. Indledning

Formålet for Skolevisioners persondatahåndbog er at give et samlet overblik over politikker, retningslinjer, procedurer, processer, arbejdsgange, skabeloner, fortegnelser og øvrig dokumentation, der vedrører Skolevisioners behandling af persondata.

Persondatahåndbogen er i sin udformning målrettet Skolevisioners medarbejdere og samarbejdspartnere.

En teknisk og organisatorisk praksis i overensstemmelse med denne persondatahåndbog medfører, at Skolevisioner i den grad det er muligt, imødekommer kundernes krav og forventninger, sikrer den registreredes rettigheder, lever op til egne standarder og i det hele taget overholder gældende persondatalovgivning.

2. Generelt

Skolevisioners formål er at udvikle, markedsføre og drive løsninger, der hjælper institutioner, virksomheder og organisationer, samt fællesskaber og andre relationelle grupperinger af personer, med at indsamle og dele viden om, samt danne overblik over, relationer, trivsel og klima/miljø/kultur mellem mennesker, for derigennem at kunne udvikle relationerne, trivslen og klimaet/miljøet/kulturen. På den måde medvirker Skolevisioner til at forbedre menneskers fællesskaber og livskvalitet.

I relation til ovenstående formål behandler Skolevisioner persondata, både som databehandler og som dataansvarlig.

2.1 Overordnede principper

I denne håndbog anvendes begrebsdefinitioner fra bogen "Persondataforordningen – en håndbog for praktikere"[1].

Begrebet 'persondata' er synonymt med bogens definition af begrebet 'personoplysninger' (Kap. 4, afsnit 4.1), dvs. *"enhver form for information om en identificeret eller identificerbar person, dvs. oplysninger, som kan henføres til den registrerede. Det kan være alt fra oplysninger om navn, adresse, telefonnummer, fødselsdag, familie, uddannelse, beskæftigelse, tjenstlige forhold, bolig, bil, eksaminer, løn og skat, sygefravær til oplysninger om arbejdstider. Begrebet skal således forstås bredt og omfatter eksempelvis e-mailadresser og IP-adresser (forudsat at det for nogle er muligt at identificere den/de personer, der står bag den pågældende e-mail eller IP-adresse) og oplysninger om enkeltmandsvirksomheder. Også oplysninger, som kræver særlig indsats, en særlig adgang eller særlig autorisation at henføre til den registrerede, vil være omfattet begrebet personoplysninger."*

Herudover anvendes begrebet 'behandling' (Kap 4. afsnit 4.8) ligeledes i overensstemmelse med persondataforordningens forståelse, dvs. "*enhver aktivitet eller række af aktiviteter, som personoplysninger gøres til genstand for. Behandlingen kan være elektronisk eller manuel. Det betyder, at alle aktiviteter, som personoplysninger udsættes for, fra de opstår, til de ophører, er omfattet af begrebet, herunder er bl.a. indsamling, systematisering, opbevaring, ændring, søgning i, brug, videregivelse, overladelse, sammenstilling samkøring og sletning omfattet."*

Skolevisioner håndterer persondata henholdsvis som dataansvarlig og databehandler og denne persondatahåndbog anvender begreberne 'dataansvarlig' og 'databehandler' iht. persondataforordningens definitioner:

Med 'dataansvarlig' (Kap 4, afsnit 4.9) menes: "*den fysiske eller juridiske person, offentlige myndighed, institution eller ethvert andet organ, der afgør, til hvilket formål og med hvilke hjælpemidler, der må foretages behandling af personoplysninger. Den dataansvarlige er altså den, der har dispositionsretten over de pågældende personoplysninger. Der kan i visse tilfælde være tale om et fælles dataansvar mellem flere dataansvarlige, jf. artikel 26."*

Med 'databehandler' (Kap 4, afsnit 4.10) menes: "*den fysiske eller juridiske person, offentlige myndighed, institution eller ethvert andet organ, der behandler personoplysninger på den dataansvarliges vegne. Databehandleren agerer alene under instruks fra den dataansvarlige, og databehandleren må ikke selv disponere over oplysningerne eller bruge disse til egne formål.*"

[1] Persondataforordningen – en håndbog for praktikere (Nis Peter Dall, Jesper Langemark & Amalie Langebæk), Første udgave, andet oplag, FairPublishing 2016

I det efterfølgende benævnes de persondata, som Skolevisioner behandler alene i rollen som databehandler som 'kundernes persondata'. Persondata som Skolevisioner behandler i rollen som dataansvarlig omtales 'persondata'.

Skolevisioner behandler persondata i overensstemmelse med principperne for "*lovlighed, rimelighed, gennemsigtighed, formålsbegrænsning, dataminimering, rigtighed, opbevaringsbegrænsning, integritet og fortrolighed*" (persondataforordningens artikel 5).

2.2 Persondatabehandling som dataansvarlig

Når Skolevisioner behandler persondata som dataansvarlig, behandler Skolevisioner udelukkende oplysninger, som er nødvendige for forretningen, herunder i forbindelse med abonnementshåndtering, levering af serviceydelser samt håndtering af kommunikation med samarbejdspartnere. Herudover behandler Skolevisioner også persondata i rollen som arbejdsgiver.

Formål med behandlingen kan være et af følgende (listen er ikke udtømmende):

- ✓ Behandling af henvendelser til Skolevisioner
- ✓ Opfyldelse af anmodning om abonnement eller serviceydelse
- ✓ Tilpasning af vores kommunikation
- ✓ Administration af interessenters, kunders og samarbejdspartneres relation til Skolevisioner
- ✓ Håndtering af hjemmesider
- ✓ Opfyldelse af arbejdsgiverrelaterede forpligtelser

Personoplysninger om (potentielle) kunder indhentes via f.eks. e-mail eller kontaktformular via hjemmesiden. Det vil fremgå af de respektive formularer, om afgivelse af personoplysningerne er obligatorisk eller valgfri. Hvis afgivelse af personoplysningerne er obligatorisk, vil det pågældende felt være markeret med en stjerne (*). Kontaktoplysninger anvendes til at besvare henvendelsen. Skolevisioner anvender cookies på sine hjemmesider. Retsgrundlaget er persondataforordningens artikel 6, stk. 1, litra b.

Behandler Skolevisioner oplysningerne til andre formål (fx til markedsføring), informerer Skolevisioner de registrerede og indhenter som udgangspunkt samtykke, jf. persondataforordningens artikel 6, stk. 1, litra a.

Skolevisioner behandler oplysninger om virksomhedens egne medarbejdere. Persondata omhandlende virksomhedens medarbejdere er udelukkende oplysninger, som er relevante for Skolevisioner som arbejdsgiver. Eventuel anvendelse fotos af medarbejdere sker kun når medarbejderen har indgået skriftligt samtykke herom.

2.3 Persondatabehandling som databehandler

Når Skolevisioner behandler kundernes persondata på vegne af Skolevisioners respektive kunder, er Skolevisioner databehandler og kunden dataansvarlig. Databehandlingen sker gennem løsninger, som Skolevisioner udvikler, udbyder og drifter som SaaS-løsninger (software-as-a-service = onlinetjenester). Kunder har adgang til Skolevisioners SaaS-løsninger/onlinetjenester gennem personlige logins, som oprettes og aktiveres efter indgåelse af abonnementsaftale med Skolevisioner. Skolevisioner anvender aldrig en abonnents data til egne formål.

Kunden er dataansvarlig for alle oplysninger, som denne, og dennes ansatte (=brugere), indsamler og anvender gennem Skolevisioners onlinetjenester, og tjenesterne må kun anvendes i henhold til de gældende abonnementsvilkår.

Som databehandler behandler Skolevisioner kun persondata iht. instruks i indgåede databehandleraftaler og Persondataforordningens artikel 6, og der behandles kun oplysninger om følgende kategorier af registrerede: Børn/ unge/ voksne på kundens institution(er) samt kundens egne ansatte. Dette er beskrevet i databehandleraftalen der indgås med Kunden.

3. Politikker, retningslinjer og procedurer

3.1 Registreredes rettigheder

Skolevisioner har udarbejdet nedennævnte politikker for udøvelse af den registreredes rettigheder.

3.1.1 Som dataansvarlig

Alle personoplysninger indsamles direkte fra de registrerede (hhv. kunder, interessenter, samarbejdspartnere, hjemmesidebesøgende og medarbejderne). Skolevisioner udøver de registreredes rettigheder i henhold til reglerne i EU's Persondataforordning og dansk databeskyttelseslov, der supplerer reglerne i databeskyttelsesforordningen:

- gennem og i henhold til
  - ✓ Skolevisioners privatlivspolitik for kunder, hjemmesidebesøgende, samarbejdspartnere og interessenter
  - ✓ Skolevisioners privatlivspolitik for medarbejdere
- i overensstemmelse med den praksis, der er nærmere beskrevet i henholdsvis
  - ✓ 'Artikel 30 fortegnelse – dataansvarlig for kundeoplysninger - Skolevisioner ApS'
  - ✓ 'Artikel 30 fortegnelse – dataansvarlig for medarbejderoplysninger - Skolevisioner ApS'

3.1.2 Som databehandler

Iht. persondataforordningen er det den dataansvarliges pligt at sikre udøvelse af registreredes rettigheder.

Skolevisioner agerer som databehandler iht. dataansvarliges instruks.

Skolevisioner yder support og vejledning til dataansvarlige, som en del af kundernes abonnement på SaaS-løsning fra Skolevisioner, omkring dataansvarliges udøvelse af registreredes rettigheder ifm. anvendelsen af Skolevisioners SaaS-løsninger/onlinetjenester.

3.2 Opbevaring

Skolevisioner har udarbejdet nedennævnte politikker for opbevaring af persondata.

3.2.1 Som dataansvarlig

Skolevisioner opbevarer persondata så længe der er behov for at behandle dem til at opfylde et eller flere af Skolevisioners formål. Særlige lovregler, herunder i fx bogføringsloven, kan dog give pligt eller ret til at opbevare dem i længere tid.

Persondata opbevares kun i sikrede systemer, der kan leve op til Skolevisioners krav til og standarder for informationssikkerhed. Opbevaringsperiode, slettefrist og -metode i de respektive systemer fremgår af hhv.

- ✓ 'Artikel 30 fortegnelse – dataansvarlig for kundeoplysninger – Skolevisioner ApS'
- ✓ 'Artikel 30 fortegnelse – dataansvarlig for medarbejderoplysninger – Skolevisioner ApS'

3.2.2 Som databehandler

Skolevisioner opbevarer kundernes persondata iht. gældende abonnementsvilkår og de indgåede abonnements- og databehandleraftaler samt i overensstemmelse med EU's Persondataforordning og dansk databeskyttelseslov, der supplerer reglerne i databeskyttelsesforordningen.

Kundernes persondata opbevares i Skolevisioners egne systemer og på Skolevisioners servere, som driftes af en certificeret og godkendt hosting-partner.

Hvilke kunders persondata, Skolevisioner aktuelt opbevarer, fremgår af

- ✓ 'Artikel 30 fortegnelse – databehandler for kundernes data – Skolevisioner ApS'

3.3 Håndtering af fysiske dokumenter

Skolevisioner har udarbejdet nedennævnte politikker for håndtering af fysiske dokumenter, som indeholder persondata.

3.3.1 Som dataansvarlig

Alle fysiske dokumenter som opbevares på Skolevisioners adresse, befinder sig i lokaler der er aflåste og forsynede med alarm, når medarbejdere eller ledelse ikke er til stede.

Personalemapper og andre kritiske dokumenter opbevares i Skolevisioners Safe (brandsikret boks med kodelås og nøgle), som kun ledelsen har kode og nøgle til.

Før bortskaffelse af dokumenter destrueres disse vha. Skolevisioners egen makulator.

3.3.2 Som databehandler

Skolevisioner lagrer ikke fysiske dokumenter indeholdende kundernes persondata, dvs. persondata, hvor Skolevisioner er databehandler.

3.4 Informationssikkerhedspolitik

Skolevisioner har udarbejdet nedennævnte informationspolitikker for informationer, som indeholder persondata.

3.4.1 Politik

Denne informationssikkerhedspolitik danner den overordnende ramme for informationssikkerheden hos Skolevisioner. Informationssikkerhedspolitikken definerer Skolevisioners sikkerhed omkring opbevaring og behandling af de persondata Skolevisioner behandler både i rollen som dataansvarlig og som databehandler.

Skolevisioner revurderer sin informationssikkerhedspolitik minimum en gang årligt.

3.4.1.1 Formål

Informationssikkerhedspolitikken danner udgangspunkt for Skolevisioners procedurer for regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske foranstaltninger til sikring af behandlingssikkerheden. Informationssikkerhedspolitikken har til formål at oplyse medarbejdere og samarbejdspartnere om retningslinjer, procedurer og ansvarlighed i relation til virksomhedens informationssikkerhed.

3.4.1.2 Omfang

Informationssikkerhedspolitikken omfatter alle persondata, som Skolevisioner behandler som databehandler og dataansvarlig.

Informationssikkerhedspolitikken gælder alle data, som er omfattet af persondataforordningen og gælder for alle ansatte og eksterne konsulenter, der udfører arbejde hos Skolevisioner med adgang til persondata gennem Skolevisioners informationstjenester og systemer. Alle disse personer betegnes her som 'medarbejdere'.

Ved anvendelse af underleverandør, sikres i samarbejde med leverandøren, at sikkerhedsniveauet fastholdes, så leverandøren, dennes faciliteter og de medarbejdere, som har adgang til persondata hos Skolevisioner, mindst lever op til Skolevisioners informationssikkerhedsniveau.

3.4.1.3 Sikkerhedsniveau

Det er Skolevisioners politik at beskytte alle persondata og udelukkende tillade brug, adgang og offentliggørelse af informationer i overensstemmelse med virksomhedens retningslinjer, dataansvarliges instruks, og under hensyntagen til den til enhver tid gældende lovgivning.

Skolevisioner gennemfører passende tekniske og organisatoriske foranstaltninger for at sikre Skolevisioners behandlingssystemer og -tjenester en vedvarende fortrolighed, integritet, tilgængelighed og robusthed. Ansvaret herfor er organisatorisk og operationelt placeret i virksomhedens ledelse.

Skolevisioners ledelse fastlægger på baggrund af en risikovurdering et sikkerhedsniveau som svarer til persondatabehandlingens karakter, omfang, sammenhæng og formål, og gennemfører en afbalanceret risiko- og konsekvensvurdering under hensyntagen til aktuelt teknisk niveau og økonomiske forhold.

3.4.1.4 Sikkerhedsbevidsthed

Skolevisioners ledelse er overordnet ansvarlig for informationssikkerheden. Ledelsen udpeger et medlem af direktionen som sikkerhedsansvarlig i den daglige praksis.

Gennemførelse af en informationssikkerhedspolitik kan dog ikke foretages af ledelsen alene. Alle medarbejdere med adgang til persondata hos Skolevisioner har et ansvar for at bidrage til at beskytte disse informationer mod uautoriseret adgang, ændring og ødelæggelse samt tyveri. Medarbejdere med adgang til persondata skal følge informationssikkerhedspolitikken og retningslinjer afledt heraf.

Medarbejderne må kun anvende virksomhedens informationer i overensstemmelse med det arbejde, de udfører i virksomheden, og skal beskytte informationerne på en måde, som er i overensstemmelse med informationernes følsomhed, særlige og/eller kritiske natur.

3.4.1.5 Brud på informationssikkerheden

Hvis en medarbejder har mistanke om eller opdager trusler mod eller brud på informationssikkerheden er medarbejderen forpligtet til straks at informere Skolevisioners ledelse og herefter samarbejde med ledelsen i overensstemmelse med virksomhedens beredskabsplaner.

3.4.2 Retningslinjer og procedurer som dataansvarlig

Persondata, som Skolevisioner behandler i rollen som dataansvarlig, er underlagt de nedennævnte retningslinjer og procedurer til at sikre efterlevelse af den ovennævnte informationssikkerhedspolitik.

3.4.2.1 Systemer

Systemer til håndtering af persondata udvælges af ledelsen. Skolevisioner anvender kun systemer fra leverandører, som kan påvise et sikkerhedsniveau, der svarer til Skolevisioners og gældende, relevant lovgivnings krav til informationssikkerheden. Skolevisioner indgår databehandleraftaler med alle valgte systemleverandører. Oplysning om systemleverandører fremgår i bilagene

- ✓ 'Artikel 30 fortegnelse – dataansvarlig for kundeoplysninger – Skolevisioner ApS'

- ✓ 'Artikel 30 fortegnelse – dataansvarlig for medarbejderoplysninger – Skolevisioner ApS'

I bilagene beskrives vedtagne tekniske og organisatoriske sikkerhedsforanstaltninger omkring brugen af systemerne til behandling af persondata.

3.4.2.2 Persondataadgang

Adgang til kundeoplysninger må kun gives personligt, kun gennem systemer omtalt i foregående punkt, og kun til Skolevisioners medarbejdere.

Medarbejderoplysninger tilgås kun af Skolevisioners ledelse.

3.4.2.3 Reviews/ Sikkerhedsforanstaltninger

Skolevisioner har implementeret faste arbejdsgange for udførsel af sikkerhedsforanstaltninger og eftersyn af disse. Sikkerhedsforanstaltningerne udføres hhv. ugentlig, månedlig, halvårligt og helårligt iht. deres karakter og omfang. Foranstaltningerne er beskrevet i

- ✓ 'Artikel 30 fortegnelse – dataansvarlig for kundeoplysninger – Skolevisioner ApS'
- ✓ 'Artikel 30 fortegnelse – dataansvarlig for medarbejderoplysninger – Skolevisioner ApS'

og arbejdsgangene er beskrevet i 'Arbejdsgange – sikkerhedsforanstaltninger – Skolevisioner ApS'. Arbejdsgange og de dertil hørende foranstaltninger evalueres og revideres løbende.

3.4.3 Retningslinjer og procedurer som databehandler

Informationssikkerhedspolitikken vedrørende kundernes persondata sikres efterlevet gennem de her beskrevne retningslinjer og procedurer.

3.4.3.1 Internt hardware og software

Tilgang til kundernes persondata må kun ske fra Skolevisioners eget udstyr. Udstyret anskaffes, installeres, repareres, bortskaffes og sikres iht. nedenstående retningslinjer.

3.4.3.1.1 Anskaffelse og installation af nyt fysisk udstyr med drev

Før nyt fysisk udstyr med drev anvendes til midlertidig lagring af kundernes persondata, 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 antivirusprogram på alle personlige computere, der anvendes til at tilgå kundernes persondata.

3.4.3.1.2 Installation af software

Al software, der installeres på servere og personlige computere, som anvendes til at håndtere kundernes persondata har kun installeret software iht. ' Positivliste for softwareinstallation'.

3.4.3.1.3 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 kundernes persondata.

3.4.3.1.4 Bortskaffelse af fysisk udstyr med drev

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

3.4.3.1.5 Reparation af fysisk udstyr med drev

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

3.4.3.1.6 Sikring mod tyveri

Udstyr, der kan indeholde kundernes persondata, skal opbevares forsvarligt, og udstyret må ikke kunne tilgås uden brug af password. Stationære computer opbevares i lokaler, der er aflåste samt er forsynede med tyverialarm, når de ikke benyttes. Bærbare computere må aldrig efterlades uden opsyn med mindre det er i aflåste lokaler eller biler.

3.4.3.2 Adgang til kundernes persondata

Adgang til kundernes persondata tildeles kun personligt og kun til medarbejdere hos Skolevisioner og de respektive ansatte hos kunden, når betingelser for adgang er opfyldte.

3.4.3.2.1 Skolevisioners tekniske medarbejdere

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

A. Kunden er indforstået med, at oplysningerne tilgås.
B. Oplysningerne tilgås i kundens interesse, f.eks. i forbindelse med support eller fejlfinding.

Manipulation af data udenom driftssystemerne skal som udgangspunkt undgås. Hvis manipulation undtagelsesvis er nødvendig, skal følgende kriterier alle være opfyldte:

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.

3.4.3.2.2 Skolevisioners administrative medarbejdere

En medarbejders mulighed for adgang til kunders persondata i Skolevisioners systemer er betinget af at medarbejderen

- ✓ har læst og er indforstået med Skolevisioners persondatahåndbog
- ✓ har underskrevet Hemmeligholdelsesaftalen
- ✓ har og benytter hardware og software som tilhører og er stillet til rådighed af Skolevisioner
- ✓ har og benytter et personligt login, hvor password skal bestå af mindst 8 tegn, og indeholde mindst 3 ud af de fire følgende typer tegn: Små bogstaver, store bogstaver, tal og tegn.

Kundernes persondata må kun tilgås når mindst en af følgende betingelser er opfyldt:

A. Kunden er indforstået med at oplysningerne tilgås.
B. Oplysningerne tilgås i kundens interesse, f.eks. i forbindelse med support eller fejlfinding.

Tilgang til kundernes persondata foregår kun gennem Skolevisioners udstyr og kun gennem browsere i inkognito/privat tilstand i følgende browsere:

1. Google Chrome: Ny Inkognito-vindue (Ctrl+Shift+N)
2. Mozilla Firefox: Nyt privat vindue (Ctrl+Shift+P)
3. Safari: Start privat browsing
4. Microsoft Edge: Nyt InPrivate-vindue (Ctrl+Shift+P)

Hvis det i forbindelse med hjælp/support bliver nødvendigt at downloade filer indeholdende kundernes persondata, håndterer Skolevisioners medarbejdere disse filer iht. følgende retningslinjer:

1. Al overførsel af filer over det åbne Internet foregår via en krypteret forbindelse.
2. Efter brug slettes filerne 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. Filerne gemmes aldrig i Dropbox, Google Drev, OneDrive eller andre mapper, der automatisk kopierer data til skyen.
4. Filerne sendes aldrig via e-mail.

Herudover udskrives kundernes persondata aldrig på papir og udleveres ej heller aldrig til andre, med mindre dataansvarlig har givet skriftlig instruks om denne udlevering.

3.4.3.2.3 Kundens ansatte

Kundernes adgang til udbudte onlinetjenester/webapplikationer/SaaS sker gennem de ansattes personligt oprettede og anvendte brugerkonti. Ved oprettelse af brugerkonto accepteres gældende abonnementsvilkår. En brugerkonto kan kun tilgås med personligt brugernavn og password. Bruger med personlig brugerkonto har kun adgang til indhold på egen brugerkonto. De respektive kunder har kun adgang til egne kundernes persondata[2].

3.4.3.2.4 Tildeling af brugerrettigheder

Tildeling af rettigheder til brugerne af onlinetjenesterne hos Skolevisioners kunder, der giver adgang til den pågældende kundes persondata, må kun foretages af Skolevisioner, hvis der er sikkerhed og dokumentation for, at vedkommende, der tildeles rettigheden også er berettiget til den. Dokumentationen kan f.eks. være en e-mail sendt fra et anerkendt domæne og/eller verifikation af brugerens ansættelsesforhold og rolle via EMU brugeradministration eller kundens hjemmeside.

3.4.3.2.5 Login

Brugernavne og password skal skrives hver gang en bruger logger ind. Der anvendes ikke "Husk mig" funktioner. Ved gentagne fejlslagne forsøg på login for en brugerkonto låses den relevante brugerkonto i et tidsrum.

3.4.3.2.6 Passwords

Passwords skal bestå af mindst 8 tegn, og indeholde mindst 3 ud af de fire følgende typer tegn: Små bogstaver, store bogstaver, tal og tegn.

Brugerpasswords forelægger ikke i klartekst, dvs. password gemmes krypteret, på en måde der forhindrer, at passwords kan genskabes.

3.4.3.2.7 Brugerstyring

Der kan oprettes en særlig brugerkonto[3] hos kunden, som giver adgang til Brugeradministrationen:

1. Se hvilke brugere, der har adgang hos kunden
2. Se hvornår kundens brugerne sidst har været logget ind
3. Tildele og fratage brugere rettigheder
4. Inaktivere brugere, så de ikke længere har adgang til at logge ind
5. Slette brugerkonti

[2] Se afsnit om separation af kundernes persondata

[3] Er yderligere beskrevet i faktaark om brugerstyring, som er internt tilgængelig her: Team Drives\SV-ALLE\01 SV DRIFT\GDPR\Skolevisioner ApS\SaaS-fakta og tilgængelig for brugerne i SaaS-løsningen.

3.4.3.3 Systemdrift og -håndtering

Skolevisioner forestår selv drift, håndtering, vedligehold og udvikling af webapplikationer og databaser, der anvendes til virksomhedens udbudte tjenester, hvorigennem kundernes data behandles. Arbejdet udføres af Skolevisioners egne medarbejdere og af eksterne konsulenter iht. Skolevisioners instruks.

3.4.3.3.1 Serveradgang

Adgang til og administration af servere er kun muligt for Skolevisioners ledelse og autoriseret underleverandør og kan kun ske med personligt to-faktor-login.

3.4.3.3.2 Opdatering

Styresystemer på servere opdateres mindst hver 14. dag.

3.4.3.3.3 Backup

Der er implementeret fuldautomatisk, overvåget backup, der sikrer at kritiske data automatisk kopieres dagligt til mindst 2 lokationer. Backup gemmes i mindst 30 dage og slettes efter 3 måneder. Der testes månedligt, om backup kan bruges til at genskabe produktionsmiljø og kundernes data.

3.4.3.3.4 Opbevaring af kundernes persondata

Driftssystemer indeholdende kundernes persondata er placeret på Skolevisioners servere hos en hosting-partner, der lever op til Skolevisioners krav til hosting-faciliteter.

Der anvendes kun hosting-partnere indenfor EØS. Skolevisioner stiller krav om, at en hosting-partner kan dokumentere deres sikkerhed gennem enten en ISAE 3402 eller ISAE 3000 baseret revisionserklæring eller en ISO 27001 certificering. En revisionserklæring skal som minimum omfatte revision af hhv. organisation, risikostyring (herunder responstid og hardware på lager), fysisk sikkerhed (herunder nødstrøm, adgangskontrol til bygninger, brandsikring, overvågning og alarmsystemer), backup og kontroller af procedurer. Hosting-partneren er ansvarlig for daglig drift, opdatering og patches på serveren, og er til rådighed omkring øvrig installation og fejlsøgning.

3.4.3.3.5 Separation af kundernes persondata

Driftssystemer er opbygget, 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.

3.4.3.3.6 Udveksling af kundernes persondata

De hentes/afleveres kun persondata iht. kundernes instruks. Driftssystemer kommunikerer eksternt kun med Styrelsen for IT og Lærings UNI-Login-infotjeneste og – webservice.

Driftssystemer udveksler data med kundens browser med en SSL-kryptering på mindst 256 bit.

3.4.3.3.7 Sletning af kundernes persondata

Sletning af brugeroplysninger og sletning af alt eller udvalgt indhold på en brugerkonto eller på kundens konto/konti kan foretages af kunden selv eller af Skolevisioner iht. skriftlig instruks fra kunden (brugeren/dataansvarlig).

3.4.3.3.8 Kryptering

Driftssystemer udveksler data med kundens browser med en SSL-kryptering på mindst 256 bit. Flytning af data til backup og i forbindelse med fejlsøgning foregår ligeledes via krypteret forbindelse.

3.4.3.3.9 Firewall

Web-servere er åbne for alle IP-adresser, men kun via SSL-kryptering på mindst 256 bit.

Der er opsat firewall på alle driftsservere for at sikre minimal 'attack surface'. Der er lukket for alle unødvendige porte.

Fjernstyring af server, FTP-adgang, databaseadgang og øvrige porte, der er nødvendige for systemdrift, er kun åbnet for specifikke IP-adresser[4]. Alle øvrige porte er blokerede i firewallen.

3.4.3.3.10 Logning

Al aktivitet på webapplikationen, inklusive de IP-adresser aktiviteten foregår fra, logges.

Derudover logges følgende hændelser i en specifik logfil og opbevares minimum i 6 måneder:

1. Administratorer, der tilgår persondata.
2. Brugere, der tilgår persondata.

Fejl- og systemlogning er indbygget. Der logges til en række filer dagligt. Disse filer er delt op i 5 typer: Debug, Error, Event, Performance, ParticipantLogin. Disse er alle en del af backupproceduren.

3.4.3.4 Aftaler

Skolevisioner indgår skriftlige aftaler med alle involverede parter. Udover ansættelseskontrakter, samarbejdsaftaler og abonnementsaftaler skal parterne indgå hhv. hemmeligholdelsesaftaler og databehandleraftaler.

3.4.3.4.1 Medarbejdere

Alle medarbejdere, der i kraft af deres ansvarsområde og arbejdsopgaver skal have adgang til kundernes persondata, skal, udover en ansættelseskontrakt, forinden have underskrevet Skolevisioners hemmeligholdelsesaftale samt skrive under på at have læst og være indforstået med denne persondatahåndbog.

3.4.3.4.2 Samarbejdspartnere

Før en samarbejdspartner kan få adgang til kundernes persondata, skal der, udover en kontrakt vedrørende arbejdets udførelse / samarbejdsaftale, være indgået en databehandleraftale. Udvælgelse af samarbejdspartner som underdatabehandler skal se i overensstemmelse med bestemmelserne i persondataforordningens artikel 28, pkt. 2.

Gives der adgang til kundernes persondata til eksterne konsulenter i en organisation, som ikke selv enten har en ISAE 3402 eller ISAE 3000 baseret revisionserklæring, der sikrer forsvarlig håndtering af personfølsomme data eller er ISO 27001 certificeret, skal disse underskrive en hemmeligholdelsesaftale, før de gives adgang til kundernes persondata.

Derudover skal der indgås en databehandleraftale med organisationens ledelse, hvor ledelsen forpligter sig til at medvirke til at konsulenterne er bekendte med og overholder relevante afsnit i denne persondatahåndbog, på lige fod med Skolevisioners egne ansatte.

3.4.3.4.3 Kunder

Adgang til Skolevisioners online-tjenester (webapplikation) er kun mulig for ansatte hos kunder, som har indgået både abonnementsaftale (herunder at have accepteret Skolevisioners abonnementsvilkår) og databehandleraftale med Skolevisioner.

[4] Se liste over hvilke IP-adresser: G:\Fællesdrev\SV-ALLE\01 SV DRIFT\GDPR\Skolevisioner ApS

3.4.3.5 Reviews

Skolevisioners ledelse fører systematisk tilsyn med det organisatoriske og tekniske sikkerhedsniveau hver måned og årligt.

3.4.3.5.1 Ugentligt sikkerhedsreview

Det udføres ugentligt et sikkerhedsreview. Det ugentlige sikkerhedsreview sikrer at de organisatoriske sikkerhedsforanstaltninger overholdes bl.a. brugen af File Shredder og oprydning på Skolevisioners bestå̊e. G:\Fællesdrev\SV-ALLE\01 SV DRIFT\GDPR\Skolevisioner ApS\Sikkerhedsreviews

3.4.3.5.2 Månedligt sikkerhedsreview

Der udføres et internt sikkerhedsreview på månedsbasis, med en fleksibilitet der strækker sig fra d. 20 i forrige måned til d. 10 i næste måned. Det vil sige, at f.eks. juli måneds sikkerhedsreview skal foretages i perioden fra og med d. 20/6 til og med 10/8. Det tilstræbes, at sikkerhedsreviewet ligger i midten af måneden.

Reviewet skal omfatte de punkter der fremgår af Checklisten for månedligt sikkerhedsreview. Checklisten udfyldes af ledelsen og indscannes som dokumentation.

3.4.3.5.3 Årligt sikkerhedsreview

Mindst én gang årligt afholdes et sikkerhedsreview der som minimum indeholder en gennemgang af

- ✓ ROS-analyse (Risiko- og sårbarhedsanalyse)
- ✓ Seneste ”OWASP-top-10”
- ✓ Checkliste til årligt sikkerhedsreview

Deltagerne i det årlige sikkerhedsreview er som minimum den sikkerhedsansvarlige ledelse i Skolevisioner og en teknisk ekspert. Checklisten for årligt sikkerhedsreview udfyldes, udskrives, underskrives og indscannes som dokumentation.

3.4.3.6 Årlig ekstern revision

Mindst én gang årligt foretages revision af informationssikkerheden. Denne foretages af en ekstern revisor, der gennemgår Skolevisioners procedurer for og håndtering af informationssikkerheden. Revisionen munder ud i en revisionserklæring, som er offentlig tilgængelig på Skolevisioners hjemmesider, eks. her: https://skolevisioner.dk/downloads/revision-og-certificeringer/

3.4.4 Beredskabsplan ved sikkerhedsbrud

Skolevisioner har vedtaget 2 beredskabsplaner:

1. Ved (mistanke om) sikkerhedsbrud vedr. øvrige kundeoplysninger og medarbejderoplysninger (Skolevisioner som dataansvarlig).
2. Ved (mistanke om) sikkerhedsbrud vedr. kundernes persondata (Skolevisioner som databehandler).

De respektive beredskabsplaner træder i kraft ved

- ✓ mistanke om brud på informationssikkerheden / læk af (kundernes) persondata
- ✓ overhængende risiko for brud på informationssikkerheden / læk af (kundernes) persondata
- ✓ brud på informationssikkerheden / læk af (kundernes) persondata.

Den praktiske udførsel af beredskabsplanernes punkter, og punkternes indbyrdes rækkefølge, kan variere alt efter problemets omfang og karakter.

Beredskabsplanerne er internt tilgængelige her: G:\Fællesdrev\SV-ALLE\01 SV DRIFT\Interne processer\Skolevisioner ApS.

3.5 'Åbent-hus'-dag hos databehandler

Af Skolevisioners skabelon til databehandleraftale med kunder pkt. 10.4. fremgår det at:

> *"Leverandøren inviterer mindst en gang årligt Kunden til et besøg på Leverandørens adresse. Sammen med Leverandørens øvrige Kunder, vil Kunden få en gennemgang af Leverandørens sikkerhedslogbog og procedurer for det seneste år. Kunden vil i forbindelse med sit besøg kunne foretage en inspektion, stille Leverandøren relevante spørgsmål og komme i dialog med andre af Leverandørens Kunder. Udover Kundens transportudgifter og tidsforbrug er besøget uden yderligere omkostninger for Kunden."*

'Åbent-hus'-dagen tilstræbes afholdt hvert år i november måned og har til hensigt at

1. give kunderne indsigt i Skolevisioners databehandling og informationssikkerhed
2. få kundernes input til Skolevisioners fremtidige arbejde med Skolevisioners SaaS-løsninger
3. give kunderne mulighed for at netværke og erfaringsudveksle

Dagen foregår som et møde i åben dialog, hvor kundernes input undervejs i ledelsens fremlæggelse er velkommen og ønskelig/nødvendig.

Udover Skolevisioners ledelse deltager relevante medarbejdere og samarbejdspartner(e).

4. Processer og arbejdsgange

Skolevisioner opererer iht. nedennævnte processer og arbejdsgange.

4.1 Som dataansvarlig

Processer for hhv. indsamling, ajourføring og sletning af personoplysninger omhandlende ansatte hos kunder, potentielle kunder, samarbejdspartnere og interessenter er nærmere defineret og beskrevet i disse bilag, som opdateres løbende:

- ✓ 'Artikel 30 fortegnelse – dataansvarlig for kundeoplysninger – Skolevisioner ApS'
- ✓ 'Artikel 30 fortegnelse – dataansvarlig for medarbejderoplysninger – Skolevisioner ApS'

Fortegnelserne er internt tilgængelige her: G:\Fællesdrev\SV-ALLE\01 SV DRIFT\GDPR\Skolevisioner ApS\Fortegnelser.

Arbejdsgange relevante for håndteringen af kundeoplysninger er beskrevet i dokumenter med titel 'Arbejdsgange' samt i 'CRM-procedurer - Skolevisioner ApS'. Dokumenterne er internt tilgængelige her: G:\Fællesdrev\SV-ALLE\01 SV DRIFT\Interne processer\Skolevisioner ApS.

De registrerede oplyses vha. privatlivspolitikken, der findes på Skolevisioners hjemmesider.

4.2 Som databehandler

Kundernes persondata håndteres af kundernes ansatte gennem Skolevisioners Software-as-a-service-løsninger iht. indgåede abonnements- og databehandleraftaler og de gældende abonnementsvilkår.

Skolevisioner behandler kundernes persondata iht. instruks i de respektive databehandleraftaler. Oversigt over gældende databehandleraftaler findes i dette bilag, som opdateres løbende:

- ✓ 'Artikel 30 fortegnelse – databehandler for kundernes data – Skolevisioner ApS'.

Fortegnelsen er internt tilgængelig her: G:\Fællesdrev\SV-ALLE\01 SV DRIFT\GDPR\Skolevisioner ApS\Fortegnelser.

Skolevisioners medarbejdere håndterer kundernes persondata i overensstemmelse med retningslinjer og procedurer, der er beskrevet i afsnittet vedrørende informationssikkerhed. Nogle procedurer er yderligere beskrevne i dokumenter med titel 'Arbejdsgange' samt i 'CRM-procedurer - Skolevisioner ApS'. Dokumenterne er internt tilgængelige her: G:\Fællesdrev\SV-ALLE\01 SV DRIFT\Interne processer\Skolevisioner ApS.

De registrerede skal oplyses af dataansvarlige (kunden). Skolevisioner yder kunderne (de dataansvarlige) vejledning og support vedrørende indsamling, ajourføring, sletning og deres pligt til at oplyse de registrerede. Skriftlige vejledninger og vejledningsvideoer ligger til brugernes (kundernes ansatte) frie afbenyttelse, og support ydes af Skolevisioner pr. telefon og e-mail.

5. Behandlingsaktiviteter

Skolevisioners behandlingsaktiviteter er beskrevet nærmere i det nedenstående.

5.1 Som dataansvarlig

Skolevisioners behandlingsaktiviteter som dataansvarlig er beskrevet i bilagene

- ✓ 'Artikel 30 fortegnelse – dataansvarlig for kundeoplysninger – Skolevisioner ApS'
- ✓ 'Artikel 30 fortegnelse – dataansvarlig for medarbejderoplysninger – Skolevisioner ApS'

Fortegnelserne ajourføres løbende ved enhver ændring og er internt tilgængelige her: G:\Fællesdrev\SV-ALLE\01 SV DRIFT\GDPR\Skolevisioner ApS\Fortegnelser.

I fortegnelserne beskrives de behandlingsaktiviteter Skolevisioner har i de respektive systemer, som Skolevisioner benytter. Af bilagene fremgår også hvilke kategorier af registrerede og hvilke kategorier af personoplysninger, der håndteres gennem de respektive systemer og hvem der er de respektive systemers databehandler(e).

Kundeoplysninger behandles iht. Skolevisioners privatlivspolitik, som de fremgår af Skolevisioners hjemmesider, eks: https://skolevisioner.dk/information/privatlivspolitik/

Medarbejderoplysninger behandles iht. Skolevisioners privatlivspolitik for medarbejdere.

Begge privatlivspolitikker forefindes internt her: G:\Fællesdrev\SV-ALLE\01 SV DRIFT\GDPR\Skolevisioner ApS\Privatlivs- og cookiepolitikker.

5.2 Som databehandler

Skolevisioners behandlingsaktiviteter som databehandler er beskrevet i de respektive databehandleraftaler, som Skolevisioner har indgået med sine kunder.

Oversigt over kategorier af behandlingsaktiviteter og de dataansvarlige kunder (inkl. kontaktoplysninger) findes i dette bilag:

- ✓ 'Artikel 30 fortegnelse – databehandler for kundernes data – Skolevisioner ApS'.

Fortegnelsen ajourføres løbende ved enhver ændring og er internt tilgængelige her: G:\Fællesdrev\SV-ALLE\01 SV DRIFT\GDPR\Skolevisioner ApS\Fortegnelser.

6. Awareness og uddannelse

Behandling af persondata og håndtering af informationssikkerhed er en del af Skolevisioners daglige opgaver, arbejdsgange og rutiner.

Skolevisioners ledelse sørger for at medarbejdere og relevante samarbejdspartnere til enhver tid er opdaterede omkring gældende udgave af denne persondatahåndbog.

Seneste udgave af persondatahåndbogen findes internt tilgængelig her:

G:\Fællesdrev\SV-ALLE\01 SV DRIFT\GDPR\Skolevisioner ApS\Håndbog\Gældende

Desuden skal den aktuelle udgave være tilgængelig for relevante samarbejdspartnere her:

https://skolevisioner.dk/persondatahaandbog/

Skolevisioners ledelse og medarbejdere deltager i relevante Erfa-grupper samt kurser udbudt af erhvervs- og brancheforeninger.

7. Løbende opfølgning og evaluering

Denne persondatahåndbog revideres ved behov og som minimum en gang årligt.

Skolevisioners interne arbejdsgange (herunder internt årshjul) sikrer løbende opfølgning og evaluering af de respektive politikker, retningslinjer, processer og arbejdsgange samt ajourføring af skabeloner, fortegnelser og øvrig dokumentation.

8. Bilagsfortegnelse

Fortegnelse over alle relevante bilag/dokumenter (skabeloner, procesark, artikel30-fortegnelser, reviews, erklæringer, aftaler, vilkår og politikker samt SaaS-politikker og -fakta) forefindes internt tilgængelig her:

G:\Fællesdrev\SV-ALLE\01 SV DRIFT\GDPR\Skolevisioner ApS\Håndbog\Gældende\

Af fortegnelsen fremgår hvor og hvordan de respektive bilag/dokumenter opbevares, hvad deres formål er og (hvor relevant) hvornår de hhv. er blevet og vil blive revideret.