Databeskyttelsespolitik for

Behandlings- og Specialskolen Magleby
Opdateret 01/03/2025

INDHOLD

OVERORDNET HÅNDTERING AF PERSONOPLYSNINGER

Behandlings- og Specialskolen Magleby anvender både eksterne løsninger og interne systemer til håndtering af personoplysninger – alt efter de specifikke aftaler, der er indgået i den enkelte sag.

Personoplysninger organiseres i bestemte systemer for at undgå, at data spredes over flere forskellige systemer, samt for at sikre, at kun relevant personale har adgang til dem.

Ud fra en analyse af den ønskede behandling af personoplysninger – herunder det tekniske niveau i løsningen, behandlingens karakter, risici for databrud samt implementerings- og driftsomkostninger – er det konkluderet, at det mest hensigtsmæssige er at etablere systemer til opbevaring af data på Behandlings- og Specialskolen Magleby, enten elektronisk og/eller fysisk.

FORMÅL

Databeskyttelsespolitikken fastlægger det ledelsesgodkendte sikkerhedsniveau for data på Behandlings- og Specialskolen Magleby. Den beskriver de overordnede sikkerhedsmålsætninger og udgør grundlaget for udarbejdelsen af skolens datasikkerhedshåndbog, som indeholder de specifikke retningslinjer og forretningsgange.

Retningslinjerne, der udarbejdes for at understøtte hovedmålsætningerne i databeskyttelsespolitikken, skal sikre, at alle medarbejdere forholder sig til og arbejder med datasikkerhed i den daglige behandling af personoplysninger.

Politikken er primært rettet mod beskyttelse af personoplysninger, men den gælder ligeledes for økonomiske og andre data.

Behandlings- og Specialskolen Magleby anser et højt sikkerhedsniveau for essentielt for at overholde lov- og myndighedskrav samt for at levere sikkerhed overfor elever, studerende, ansatte, kommuner og øvrige samarbejdspartnere. Datasikkerhed er derfor en central værdi og integreret i skolens behandling af alle typer oplysninger, særligt personoplysninger.

OMFANG

Databeskyttelsespolitikken gælder for alle ansatte på Behandlings- og Specialskolen Magleby.

Alle leverandører og samarbejdspartnere, der har fysisk eller logisk adgang til skolens systemer, data og oplysninger, skal gøres bekendt med politikken og overholde den.

Politikken dækker samtlige tekniske og administrative forhold, som har direkte eller indirekte indflydelse på driften og brugen af Behandlings- og Specialskolen Maglebys automatiske databehandlingssystemer samt manuelle arkiver og registre.

HOVEDMÅLSÆTNINGER OG SIKKERHEDSNIVEAU

Behandlings- og Specialskolen Magleby fastlægger følgende sikkerhedsmålsætning:

"Skolen har et passende og tilstrækkeligt teknisk og organisatorisk sikkerhedsniveau, der gælder for alle ansatte, leverandører og samarbejdspartnere ved behandling af personoplysninger og andre data – både ved hel eller delvis anvendelse af automatiske databehandlingssystemer og ved behandling af manuelle dokumenter."

Under hensyntagen til det aktuelle tekniske niveau, implementeringsomkostningerne samt den enkelte behandlings karakter, omfang, sammenhæng og formål, gennemfører skolen passende tekniske og organisatoriske foranstaltninger for at sikre et sikkerhedsniveau, der er afstemt med de identificerede risici.

Et passende og tilstrækkeligt databeskyttelsesniveau opnås gennem tekniske og organisatoriske foranstaltninger, der sikrer:

- **Vedvarende beskyttelse:**
  At fortrolighed, integritet, tilgængelighed og robusthed i skolens databehandlingssystemer og behandlingstjenester opretholdes i forhold til den gennemførte risikovurdering for de enkelte systemer og data.

- **Sikker dataudveksling:**
  At pseudonymisering og kryptering anvendes, hvor det er relevant – herunder ved dataudveksling med databehandlere, eksterne parter og offentlige myndigheder.

- **Hurtig genoprettelse:**
  At der er kapacitet til rettidigt at genoprette tilgængeligheden af data og adgangen til dem i tilfælde af en fysisk eller teknisk hændelse.

- **Løbende evaluering:**
  At der er etableret en procedure for regelmæssig afprøvning, vurdering og evaluering af datasikkerheden.

- **Beskyttelse af IT-aktiver:**
  At skolens IT-aktiver, oplysninger og data beskyttes i relation til skolens samlede varetægt.

Et tilstrækkeligt sikkerhedsniveau fastholdes ved:

- **Integrerede retningslinjer og forretningsgange:**
  At der løbende findes retningslinjer og forretningsgange, som sikrer, at datasikkerheden er en naturlig del af skolens drift og daglige arbejde. Målet er en kontinuerlig forbedringsproces, der vedligeholder og optimerer databeskyttelsespolitikken samt tilhørende retningslinjer og procedurer.

- **Kontrakt- og leverandørstyring:**
  At brugen af eksterne leverandører, konsulenter og samarbejdspartnere gennem kontraktstyring sikrer, at de lever op til gældende databeskyttelseslovgivning og skolens fastlagte sikkerhedsniveau.
- **Indførelse af nye IT-systemer:**
  At der ved indførelse af nye IT-systemer:
    - Implementeres passende tekniske og organisatoriske foranstaltninger, så standardindstillinger sikrer, at kun nødvendige personoplysninger behandles.
    - Eventuelt udføres en konsekvensanalyse af de påtænkte behandlingsaktiviteters påvirkning på beskyttelsen af personoplysninger, hvis det vurderes nødvendigt.
- **Opfølgning og vedligeholdelse:**
  At skolen løbende følger op på datasikkerheden gennem vedligeholdelse og optimering af databeskyttelsespolitikken, retningslinjerne og forretningsgangene.

ORGANISATION OG ANSVAR

Sikkerhedsmålsætning:
"Alle ansatte har ansvar for datasikkerheden. De skal være bekendte med og efterleve Behandlings- og Specialskolen Maglebys databeskyttelsespolitik, retningslinjer og forretningsgange, som beskrives i datasikkerhedshåndbogen."

Planlægning, implementering og kontrol af datasikkerheden fastlægges af ledelsen på Behandlings- og Specialskolen Magleby. Ledelsen har desuden ansvaret for både implementering og vedligeholdelse af databeskyttelsessikkerhedssystemet samt for opfølgning på sikkerhedshændelser.

I datasikkerhedshåndbogen og i "Organisation og Ansvar" bilaget, fastsætter ledelsen, hvem der har ansvaret for:

- Institutionens automatiske og manuelle databehandlingssystemer
- Styring af system- og netværksadgang samt tildeling af rettigheder
- Indgåelse af IT-kontrakter og øvrige aftaler
- Indkøb af hardware og installation af software
- Behandling af henvendelser fra de registrerede
- Opsamling og håndtering af anmeldelser af brud på datasikkerheden til Datatilsynet og de registrerede, der er berørt af et brud

Databeskyttelsespolitikken revurderes og godkendes årligt eller i forbindelse med situationer, der nødvendiggør en opdatering.

Ledere og ansatte er forpligtede til at efterleve de fastlagte retningslinjer og procedurer for datasikkerhed i det daglige arbejde. Ansatte, der konstaterer eller oplever brud på datasikkerheden, skal omgående anmelde dette til den dataansvarlige.

Den nødvendige viden og kompetence om datasikkerhed kommunikeres løbende til alle ansatte, og der arbejdes kontinuerligt med at styrke både holdninger og viden omkring datasikkerhed.

Ledelsen har det overordnede ansvar for, at databeskyttelsespolitikken overholdes.

DATASIKKERHEDSHÅNDBOGEN

Ledelsen uddyber databeskyttelsespolitikken gennem retningslinjer og forretningsgange. Tilsammen – databeskyttelsespolitikken, retningslinjerne, beredskabspolitikken og forretningsgangene – udgør datasikkerhedshåndbogen, som er inddelt i følgende hovedområder:

1. Retningslinjer for ansattes håndtering af sikkerhed
    - Personoplysninger behandles altid fortroligt.
    - Regler for login og adgangskoder.
    - Regler for anvendelse af mobilt udstyr, PC'er, USB-nøgler, mobiltelefoner mv.
    - Regler for brug af private PC'er til behandling af personoplysninger vedrørende de unge/beboere og ansatte.
    - Regler for anvendelse af internettet.
    - Regler for e-mails, herunder brug af sikker mail samt privat anvendelse af skolens e-mail.
    - Regler for eller forbud mod download af IT-programmer, spil, billeder mv.
    - Regler for brug af privat IT-udstyr til arbejde med personfølsomme data.

2. Retningslinjer for adgangsstyring
3. Retningslinjer for behandling af data på mobile enheder
4. Retningslinjer for anvendelse af sikker mail ved kommunikation med pårørende til de unge/beboere, kommuner og andre offentlige myndigheder.

5. Retningslinjer for netværksstyring, herunder trådløse netværk.
6. Retningslinjer for styring af sikkerhedshændelser
    - Anmeldelse af brud på persondatasikkerheden til Datatilsynet og de registrerede, herunder procedurer, kontakt til databehandler og indhold i anmeldelsen.
    - Forretningsgange for behandling, reetablering og rettelser af data.
7. Principper og forretningsgange for behandling af personoplysninger
8. Retningslinjer for styring af leverandører og databehandlere

PRINCIPPER OG FORRETNINGSGANGE FOR BEHANDLING AF PERSONOPLYSNINGER

Ledelsen fastsætter principper og forretningsgange for Behandlings- og Specialskolen Maglebys behandling af personoplysninger for at sikre overholdelse af både Databeskyttelsesforordningen og Databeskyttelsesloven. De dokumenterede forretningsgange omfatter:

- **Behandlingsprincipper:**
  Fastlæggelse af grundlæggende principper for håndtering af personoplysninger.
- **Anvendelse af samtykke:**
  Regler for, hvordan samtykke anvendes som retsgrundlag for behandling af personoplysninger.
- **Registreredes rettigheder:**
  Procedurer for udøvelse af de registreredes rettigheder, herunder underretning ved registrering og udøvelse af retten til berigtigelse, sletning, begrænsning af behandling samt retten til dataportabilitet.
- **Dokumentation:**
  Udarbejdelse af fortegnelser over behandlingsaktiviteter med personoplysninger.

RISIKOVURDERING OG KLASSIFIKATION AF DATA

1. Risikovurdering

Behandlings- og Specialskolen Magleby ønsker at være bevidst om enhver risiko. På baggrund af en risikovurdering opnås et passende og tilstrækkeligt sikkerhedsniveau – både elektronisk og fysisk. Ledelsen deltager aktivt i risikovurderingen og har ansvaret for at vurdere trusler, konsekvenser og risici ved både automatisk og manuel databehandling. Risikovurderingen revurderes mindst én gang årligt eller ved større ændringer i opgaver, leverandører eller databehandlingssystemer.

2. Klassifikation

For at sikre, at systemer og data opnår det rette sikkerhedsniveau, klassificeres de ud fra følgende kriterier:

2.1 Tilgængelighed

- Det skal være muligt for autoriserede personer at tilgå systemer og data, når det er nødvendigt.
- Høj tilgængelighed er særligt vigtig for data og IT-systemer, der anvendes til:
    - Behandling af institutionens beboere og klienter
    - Medicinadministration
    - Personaleadministration, herunder lønudbetaling og indberetninger til myndigheder
- Tilgængeligheden sikres primært gennem bestemmelser i IT-kontrakter og/eller databehandleraftaler med leverandørerne.

2.2 Integritet/Pålidelighed

- Integritet handler om, at data er korrekte, pålidelige, nøjagtige, opdaterede og fuldstændige.
- Høj integritet er afgørende for data og IT-systemer, der understøtter:
    - Beslutninger vedrørende beboernes/klienternes behandling og udarbejdelse af handleplaner
    - Medicinadministration
    - Personaleadministration
- Integriteten sikres primært gennem den kvalitetskontrol, der udføres i henhold til de fastlagte forretningsgange.

2.3 Fortrolighed

- Fortrolighed betyder, at kun autoriserede personer har adgang til oplysningerne, og at data udelukkende er tilgængelige for disse.
- Personoplysninger behandles altid fortroligt og videregives eller offentliggøres kun med samtykke fra den registrerede, medmindre en videregivelse er hjemlet i lovgivningen.

OVERTRÆDELSE AF DATABESKYTTELSESPOLITIKKEN

Alle ansatte i Behandlings- og Specialskolen Magleby er forpligtet til at efterleve den til enhver tid gældende datasikkerhedspolitik samt de tilhørende retningslinjer, forretningsgange og bilag. Ved tiltrædelse modtager alle medarbejdere en kopi af de centrale bestemmelser om data- og persondatasikkerhed, og de underskriver

en erklæring om at overholde politikken. Overtrædelse af datasikkerhedsreglerne eller forkerte behandlinger af personoplysninger kan, alt efter omstændighederne, medføre ansættelsesretlige konsekvenser.

Afvigelser

Hvis der opstår situationer, hvor kravene i databeskyttelsespolitikken ikke kan efterleves, skal dette godkendes af ledelsen og dokumenteres. I sådanne tilfælde skal der indføres alternative sikringsforanstaltninger, der kompenserer for afvigelsen.

UDARBEJDELSE, DATAANSVARLIG OG IKRAFTTRÆDELSE

Databeskyttelsespolitikken blev oprindeligt godkendt den 25.05.2018 og trådte i kraft samme dag. Den er senest blevet opdateret den 01.03.2025.

Behandlings- og Specialskolen Magleby har udnævnt André S. D. Henriksen som dataansvarlig. Ved spørgsmål vedrørende databeskyttelsespolitikken kan du kontakte:

André S. D. Henriksen
Mobil: 27 82 14 50
E-mail: anhen@magleby.dk

Adresse:
Behandlings- og Specialskolen Magleby
Søhusevej 79
Skælskør 4230

BEGREBER OG DEFINITIONER

Begreb	Definition
Fortrolighed	Kun autoriserede personer har ret til at behandle oplysningerne, der kun skal være tilgængelige for autoriserede personer.
Integritet	Det er muligt at validere, om data på systemerne er korrekte, pålidelige, nøjagtige, opdaterede og fuldstændige. Herunder sikring af Backup og eller systemdublering
Tilgængelighed	Det skal være muligt at tilgå systemer og data for autoriserede personer, når dette er nødvendigt.
Robusthed	Behandlingssystemers- og tjenesters tekniske og organisatoriske modstandsdygtighed, der beskytter dem mod skadelige hændelser. Dette kan f.eks. være sikring mod udfald ved dublering, køling, nødstrømsanlæg, brandslukning mv.
Pseudonymisering	Behandling af personoplysninger på en sådan måde, at personoplysningerne ikke længere kan henføres til en bestemt registreret uden brug af supplerende oplysninger, der opbevares separat og sikkert.
Kryptering	En proces, der omdanner de oprindelige oplysninger til oplysninger, der er ulæselig for en tredjepart.
Vedvarende	Evnen til at sikre fortrolighed, integritet, tilgængelighed og robusthed af behandlingssystemer og -tjenester er en løbende teknisk og organisatorisk forpligtelse
Databeskyttelsespolitik	Databeskyttelsespolitikken indgår i en dokumentstruktur, hvor politikken er det overordnede dokument, som besluttes af ledelsen, og som udstikker de overordnede krav og målsætninger, som opfyldes igennem specifikke retningslinjer, forretningsgange og instrukser, der findes i Datasikkerhedshåndbogen.
Retningslinjer	I retningslinjerne udfyldes de målsætninger, der er fastlagt i politikken i konkrete beskrivelser af, hvordan sikkerhedspolitikken implementeres. Retningslinjerne fungerer på et overordnet niveau og indeholder ikke tekniske og systemrelaterede beskrivelser.
Forretningsgange og instrukser	Forretningsgange og instrukser udgør specifikke vejledninger til, hvordan retningslinjerne på detaljeret niveau overholdes og implementeres i den enkelte afdeling.
Sikkerhedsforhold	Med sikkerhedsforhold menes alle de forhold, som kan påvirke oplysningers sikkerhed i forhold til fortrolighed, pålidelighed og tilgængelighed.
Sikkerhedshændelser	Begrebet forstås bredt som alle de hændelser, der påvirker databeskyttelsessikkerheden, herunder brud på sikkerheden