Databeskyttelsespolitik for Midtsjællands Efterskole

Overordnet organisering af personoplysninger

Midtsjællands Efterskole ønsker som hovedregel at anvende digitale databehandlingssystemer og digital opbevaring af personoplysninger hos eksterne leverandører, der sikkert hoster og stiller IT-systemer til rådighed, således at Midtsjællands Efterskole ikke selv har behov for at råde over kompetence til at stå for den daglige drift af sådanne systemer.

Midtsjællands Efterskole ønsker endvidere i videst muligt omfang at organisere opbevaringen af personoplysninger i bestemte centrale systemer, så personoplysninger om de enkelte personer ikke findes fordelt på flere systemer og både i elektronisk og manuel form.

1. Formål

Databeskyttelsespolitikken beskriver det ledelsesgodkendte niveau for sikkerhed i Midtsjællands Efterskole og indeholder de overordnede sikkerhedsmålsætninger og danner grundlag for udformning af Midtsjællands Efterskoles underliggende retningslinjer og forretningsgange.

De retningslinjer, der udformes for at understøtte databeskyttelsespolitikkens hovedmålssætninger skal sikre, at alle medarbejdere arbejder med og forholder sig til datasikkerhed i behandlingen af personoplysninger i det daglige arbejde.

Databeskyttelsespolitikken er især formuleret med henblik på beskyttelse af personoplysninger, men den finder tilsvarende anvendelse på økonomiske og andre data.

Datasikkerhed er derfor en nøgleværdi, og den er en naturlig del af Midtsjællands Efterskoles automatiske og manuelle databehandling af oplysninger, herunder især personoplysninger.

2. Omfang

Databeskyttelsespolitikken er gældende for alle, der er tilknyttet virksomheden enten som medarbejdere, ledelse, frivilligt tilknyttede, bestyrelse, leverandører og samarbejdspartnere.

Alle leverandører og samarbejdspartnere, som har fysisk eller logisk adgang til Midtsjællands Efterskoles IT-systemer, data og personoplysninger, skal gøres bekendt med politikken og forpligte sig til at følge den.

Databeskyttelsespolitikken dækker alle tekniske og administrative forhold, der har direkte eller indirekte indflydelse på drift og brug af Midtsjællands Efterskoles digitale databehandlingssystemer samt manuelle arkiver og registre.

3. Hovedmålsætninger og sikkerhedsniveau

Midtsjællands Efterskole har følgende sikkerhedsmålsætning:

Midtsjællands Efterskole har et passende og tilstrækkeligt teknisk og organisatorisk sikkerhedsniveau, der gælder for alle ansatte, leverandører og samarbejdspartnere ved behandling af personoplysninger og andre data ved hel eller delvis anvendelse af automatisk databehandling samt for behandling af manuelle dokumenter.

Et passende og tilstrækkeligt databeskyttelsesniveau[1] opnås igennem tekniske og organisatoriske foranstaltninger, der sikrer:

- vedvarende fortrolighed, integritet, tilgængelighed og robusthed af Midtsjællands Efterskoles digitale behandlingssystemer og behandlingstjenester i forhold til den risikovurdering, der gennemføres for de enkelte systemer og personoplysninger
- anvendelse af pseudonymisering og kryptering, hvor det er relevant, herunder ved dataudveksling med databehandlere og eksterne parter og offentlige myndigheder
- evnen til rettidigt at genoprette tilgængelighed af og adgangen til data i tilfælde af en fysisk eller teknisk hændelse
- procedurer for regelmæssig afprøvning, vurdering og evaluering af databeskyttelsessikkerheden
- beskyttelse af Midtsjællands Efterskoles IT-aktiver, personoplysninger og øvrige data i Midtsjællands Efterskoles varetægt

Et tilstrækkelige sikkerhedsniveau fastholdes ved:

- at der vedvarende forefindes retningslinjer og forretningsgange, som sikrer, at datasikkerheden er en integreret del af Midtsjællands Efterskoles drift og daglige arbejde
- at sikre en kontinuerlig forbedringsproces, der løbende vedligeholder og optimerer databeskyttelsespolitikken, retningslinjer og forretningsgange
- at det igennem kontrakt- og leverandørstyring sikres, at brugen af eksterne leverandører, konsulenter og samarbejdspartnere lever op til den gældende databeskyttelseslovgivning og Midtsjællands Efterskoles databeskyttelsesniveau
- at der i forbindelse med indførelse af nye IT-systemer gennemføres:
    - passede tekniske og organisatoriske foranstaltninger med henblik på gennem standardindstillinger at sikre, at kun personoplysninger, der er nødvendige, behandles
    - gennemførelse af analyse af den påtænkte behandling af personoplysningers konsekvenser for beskyttelse af oplysningerne, (Konsekvensanalyse), hvis det skønnes nødvendigt
- at Midtsjællands Efterskole følger op på datasikkerheden igennem løbende vedligeholdelse og optimering af databeskyttelsespolitikken og de dertilhørende retningslinjer og forretningsgange

4. Organisation og ansvar

Sikkerhedsmålsætning:

Alle medarbejdere har ansvar for datasikkerheden. De er bekendte med og efterlever Midtsjællands Efterskoles databeskyttelsespolitik, retningslinjer og forretningsgange.

Planlægning, implementering og kontrol af datasikkerheden er defineret af Midtsjællands Efterskole**s** ledelse, der også er ansvarlig for implementering og vedligeholdelse af databeskyttelsessikkerhedssystemet og er ansvarlig for opfølgning på sikkerhedshændelser (brud).

Ledelsen fastsætter, hvem der har ansvaret for hver af institutionens digitale og manuelle databehandlingssystemer, styring af systemadgang og netværksadgang, tildeling af rettigheder, indgåelse af IT-kontrakter og andre kontrakter, indkøb af hardware og installation af software, behandling af henvendelser fra de registrerede, opsamling og styring af anmeldelse af brud på persondatasikkerheden til Datatilsynet og de registrerede, der er berørt af bruddet.

Databeskyttelsespolitikken revurderes og godkendes i forbindelse med eventuelle situationer, der nødvendiggør det.

[1] Som beskrevet i Databeskyttelsesforordningen artikel 32

Ledere og medarbejdere er ansvarlige for at efterleve retningslinjer og procedurer for datasikkerhed i det daglige arbejde. Medarbejdere, der konstaterer eller oplever brud på datasikkerheden, skal anmelde det hurtigst muligt til nærmeste leder eller den udpegede kontaktperson for persondata.

Den nødvendige viden og kompetence om databeskyttelse og sikkerhed kommunikeres til alle medarbejdere, og der bliver løbende arbejdet med holdninger og viden omkring databeskyttelse og sikkerhed.

Ledelsen er ansvarlig for, at databeskyttelsespolitikken overholdes.

5. Principper og forretningsgange for behandling af personoplysninger

Ledelsen fastsætter principper og forretningsgange for behandling af personoplysninger, der sikrer overholdelse af Databeskyttelsesforordningen og Persondataloven.

Forretningsgangene, der dokumenteres, omfatter:

- Principper for behandling af personoplysninger
- Anvendelse af samtykke som grundlag for behandling af personoplysninger
- Procedurer for udøvelse af den registreredes rettigheder, herunder underretning ved registrering og udøvelse af retten til berigtigelse, sletning eller begrænsning af behandling og ret til dataportabillitet
- Fortegnelser udarbejdet over behandlingsaktiviteter med personoplysninger

6. Risikovurdering og klassifikation af data

Risikovurdering

Midtsjællands Efterskole ønsker at være bevidst om enhver risiko og ud fra en risikovurdering at opnå et passende og tilstrækkeligt sikkerhedsniveau, der etableres både elektronisk og fysisk. Ledelsen deltager aktivt i risikovurderingen og er ansvarlig for at vurdere trusler, konsekvenser og risici ved automatisk og manuel databehandling. Det tages op i ledelsen, om risikovurderingen skal revurderes, samt ved eventuelle større ændringer i opgaver, leverandører eller databehandlingssystemer.

Klassifikation

For at sikre at systemer og data har det rigtige sikkerhedsniveau, skal disse klassificeres. Data og systemer skal klassificeres efter både tilgængelighed, integritet (pålidelighed) og fortrolighed.

Tilgængelighed

I tilgængelighedskriteriet ligger, at det skal være muligt at tilgå systemer og data for autoriserede personer, når dette er nødvendigt.

Det er for Midtsjællands Efterskole især vigtigt med høj tilgængelighed til data og IT-systemer, der indeholder oplysninger, der anvendes i forbindelse med personoplysninger, personaleadministration, herunder lønudbetaling og indberetninger til myndigheder

Tilgængeligheden sikres først og fremmest igennem bestemmelser i de IT-kontrakter og/eller databehandleraftaler, der indgås med leverandørerne.

Integritet og pålidelighed

Med integritet og pålidelighed menes, at data om og i systemerne er korrekte, pålidelige, nøjagtige, opdaterede og fuldstændige.

Det er for Midtsjællands Efterskole især vigtigt med høj integritet og pålidelighed i data og IT-systemer, der indeholder oplysninger, der anvendes i forbindelse med behandling af personoplysninger og personaleadministration.

Integritet og pålidelighed sikres først og fremmest gennem den kvalitetskontrol, der finder sted under de fastlagte forretningsgange for behandling af personoplysninger og sager.

Fortrolighed
Med fortrolighed menes der, at kun autoriserede personer har ret til at tilgå personoplysningerne, og personoplysningerne kun skal være tilgængelige for autoriserede personer.

Personoplysninger behandles altid fortroligt og videregives eller offentliggøres kun med samtykke fra den registrerede, med mindre videregivelse har anden hjemmel i lovgivningen.

7. Overtrædelse af databeskyttelsespolitikken

Alle medarbejdere hos Midtsjællands Efterskole er forpligtet til at efterleve den til enhver tid gældende datasikkerhedspolitik med tilhørende retningslinjer, forretningsgange og relaterede bilag.

Alle medarbejdere modtager ved deres tiltræden af stillingen en kopi af de vigtigste bestemmelser om data- og persondatasikkerhed rettet til medarbejderne.

8. Afvigelser

Hvis der opstår situationer, hvor kravene i Databeskyttelsespolitikken helt undtagelsesvist ikke kan efterleves, skal det godkendes af ledelsen og dokumenteres, og der indføres alternative sikringsforanstaltninger.

9. Udarbejdelse og ikrafttrædelse

Databeskyttelsespolitikken er godkendt den 29/05/2018, og træder i kraft den 29/05/2018. Ændringer i sikkerhedsdokumentationen forelægges og godkendes af ledelsen.

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
Retningslinjer, forretningsgange og instrukser	I retningslinjerne udfyldes de målsætninger, der er fastlagt i politikken i konkrete beskrivelser af, hvordan sikkerhedspolitikken implementeres. Forretningsgange og instrukser udgør specifikke vejledninger til, hvordan retningslinjerne på detaljeret niveau overholdes og implementeres
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