



Databeskyttelsespolitik for Lemvig Gymnasium

Formål

Politikkens formål er at vejlede beslutningstagere i organisationen om, hvilke principielle beslutninger om databeskyttelse som organisationen har truffet og efterlever.

Databeskyttelsespolitikken er ikke et selvstændigt lovkrav, men understøtter institutionens beskrivelse af de foranstaltninger, som sikrer at institutionen kan dokumentere vigtige tiltag for at sikre sin efterlevelse af GDPR art. 5 stk. 2.

Dataetiske overvejelser

Lemvig Gymnasiums kerneydelse er uddannelse.

Skolen bruger data om elevernes fravær, præstationer i opgaver og adfærd i klassen til at risikovurdere, om elever kan være i fare for at droppe ud eller underpræstere.

Der kan opstå et etisk dilemma:

- Positive sider:
Systemet kan hjælpe med at spotte og støtte elever, som har problemer, og dermed forbedre deres trivsel samt muligheden for at færdiggøre uddannelsen.
- Negative sider:
Elever og forældre har måske ikke fuldt kendskab til, hvilke data der indsamles og opbevares.
En overvurdering af risikoen for bestemte elever kan i nogle tilfælde stigmatisere elever og påvirke lærernes syn på dem.
Hvis eleverne overvåges og bedømmes, kan det skabe mistillid mellem elever, lærere og skolen.

Lemvig Gymnasium opbevarer fravær og præstationer i et system, som kun kan tilgås af ledelsen, administrationen samt klassens lærere. Øvrige data om eksempelvis adfærd opbevares, så de kun kan tilgås af ledelsen, administrationen samt klassens studievejleder.

Derved er det vurderet, at skolen på bedst mulig måde kan hjælpe eleven under hensyntagen til evt. negative sider.

Organisering og ansvar

Organisering og ansvar i fm. databeskyttelse er forankret hos rektor og vicerector i samarbejde med en sekretær, og disse har også ansvaret for skolens persondatapolitik.



Hovedformål og hjemmel

Lemvig Gymnasiums hovedformål er uddannelse.

Der udbydes STX, HHX, EUD, EUX og 10. klasse.

Hjemmelsgrundlag er beskrevet i Lemvig Gymnasiums persondatapolitik samt underliggende bilag.

Beskrivelse af evt. trusselsbillede for institutionen

Fysiske trusler:

Indbrud eller uvedkommende ophold på institutionens matrikel – herunder risiko for adgang til personoplysninger ved aflæsning af skærme eller overhøring af fortrolige samtaler.

Dette forsøges imødegået ved:

- Når skolen er lukket, er der alarm på lokaler, hvor oplysninger kan tilgås.
- Ledelse, administration og medarbejdere afholder møder i lukkede lokaler.
- Skærme låses, når ansatte forlader deres arbejdsplads

Organisatoriske trusler:

F.eks. manglende adgangsstyring eller uklare arbejdsgange.

Dette imødegås ved:

- Vores medarbejdere deltager i awareness-kurser
- Medarbejdere modtager mail med link til "Håndbog til ansatte om sikker databehandling", hvor sikker brug af pc beskrives
- Ved ansættelsen informeres om tavshedspligt ved underskrift af ansættelsesbrevet samt i ovennævnte håndbog

Tekniske trusler:

- Lemvig Gymnasium er hostet hos EFIF, som har opsat antivirus, sikkermail m.m.
- Institutionens systemer og risici er beskrevet i Lemvig Gymnasiums risikovurdering, som findes på fællesdrevet.
- Medarbejdere har adgang til "Håndbog om sikker databehandling", hvor f.eks. hjemme- og fjernarbejde er beskrevet

Risici for institutionens registrerede

Eksempler på sandsynlige risici:

- Data til forkerte modtagere pga. auto-complete:
Det anbefales medarbejdere at slå auto-complete fra – beskrives i håndbogen
- Videregivelse af data via ikke-sikker-mail:
I håndbogen er det beskrevet, hvordan man anvender skolens systemer – og ikke egne private mails eller computere
- Fejludlevering af data ved sagsbehandling:
Ved fejlagtig udlevering af data f.eks. ved fremsendelse til forkert mail, kontaktes modtageren straks med anmodning om at slette mailen og de vedhæftede filer. Bruddet rapporteres til den sikkerhedsansvarlige.



- Videregivelse af data gemt i skabelon- og blanketløsninger:
Det tilstræbes, at skabeloner m.v. kun er tilgængelige i det administrative fællesdrev – dvs. at kun et begrænset antal medarbejdere har adgang til skabelonerne.

Databehandling af medarbejdere

Medarbejder:

Ved ansættelse af en medarbejder indhentes persondata ved, at medarbejderen har fremsendt ansøgning med de relevante data. Efterfølgende indhentes f.eks. cpr.nr., straffeattest, og på længere sigt opbevares data om barsel, sygedage, pårørende, ferieoplysninger m.m.

Alle data opbevares i systemet IMS Case, som kun kan tilgås af et begrænset antal medarbejdere i ledelsen samt i administrationen.

Modtagere af personoplysninger om den ansatte er beskrevet i skolens fortegnelse over behandlingsaktiviteter for personaleadministration.

I IMS Case oprettes alle medarbejdere med en kassationskode, så medarbejderen ved fratrædelse slettes automatisk efter 5 år.

Jobansøgere:

Persondata indhentes, når ansøgere har ansøgt via gymnasiejob eller mail. Alle ansøgere slettes fra gymnasiejob og mail, når ansættelsesproceduren er overstået. Ansøgerens oplysninger kan efter samtykke fra ansøgeren gemmes i ½ år med en kassationskode i IMS Case, hvorefter data slettes som ovenfor nævnt.

Databehandling af elever

Data på elever indhentes fra optagelse.dk og opbevares i elevadministrationssystemet Ludus. Efterfølgende gemmes også data om fravær, karakterer, lægeerklæringer m.m.

Modtagere af personoplysninger om eleven er beskrevet i skolens fortegnelse over behandlingsaktiviteter for elever.

Når elever er indberettet i Ludus som ophørt, slettes alle oplysninger om eleven efter 5 år. Eksamensbeviser samt SU-oplysninger opbevares i et aflåst lokale i ht. opbevaringskravet i 30 år.

Opfyldelse af oplysningspligten

Elever:

Før sommerferien sendes via e-boks et velkomstbrev til de nye elever, som skal starte det kommende skoleår. I velkomstbrevet henvises til "Elever – behandling af dine personoplysninger" på <https://www.lemvig-gym.dk/officielt/persondataforordning>.

Ansatte:

Ved underskrift i fm. ansættelse henvises der i ansættelsesbrevet til "Ansatte – behandling af dine personoplysninger" på <https://www.lemvig-gym.dk/officielt/persondataforordning>. Der oplyses endvidere om tavshedspligt.

Efter underskrift af ansættelsesbrevet sendes dette til medarbejderens e-boks.



Ansøgere:

Hvis en ansøger ønsker at give samtykke til opbevaring af persondata i ½ år, henvises der til "Jobansøgere – behandling af dine personoplysninger" på <https://www.lemvig-gym.dk/officielt/persondataforordning>.

Principper for lovlig behandling

Databeskyttelsesforordningen beskriver principper for lovlig behandling i forordningens artikel 5.

Lovlighed, rimelighed og gennemsigtighed

Personoplysninger skal behandles lovligt, rimeligt og på en gennemsigtig måde i forhold til den registrerede.

Formålsbegrænsning

Personoplysninger skal indsamles til udtrykkeligt angivne og legitime formål og må ikke viderebehandles på en måde, der er uforenelig med disse formål. Personoplysninger indsamlet til et formål må ikke genbruges til et andet.

Dataminimering

Personoplysninger skal være tilstrækkelige, relevante og begrænset til, hvad der er nødvendigt i forhold til de formål, hvortil de behandles.

Rigtighed

Persondata skal være korrekte og om nødvendigt ajourførte; der skal tages ethvert rimeligt skridt for at sikre, at personoplysninger, der er urigtige i forhold til de formål, hvortil de behandles, straks slettes eller berigtiges.

Opbevaringsbegrænsning

Persondata opbevares på en sådan måde, at det ikke er muligt at identificere de registrerede i et længere tidsrum end det, der er nødvendigt til de formål, hvortil de pågældende personoplysninger behandles.

Integritet og fortrolighed

Persondata skal behandles på en måde, der sikrer tilstrækkelig sikkerhed for de pågældende personoplysninger, herunder beskyttelse mod uautoriseret eller ulovlig behandling og mod hændeligt tab, tilintetgørelse eller beskadigelse, under anvendelse af passende tekniske eller organisatoriske foranstaltninger.

Ansvarlighed

Den dataansvarlige er ansvarlig for og skal kunne påvise at ovenstående principper overholdes.

Risikostyring og konsekvensanalyser

Som beskrevet i Lemvig Gymnasiums Persondatapolitik foretages der en risikovurdering ved behandling af personoplysninger. Hvis det i risikovurderingen vurderes, at en behandling vil indebære høj risiko, udføres der en konsekvensanalyse.

Risikovurderingen opbevares på det administrative fællesdrev, som kan tilgås af lederne og administrationen.



Det er ligeledes beskrevet i Persondatapolitikken, hvordan Lemvig Gymnasium sikrer, at databehandlere kan leve op til forordningens krav. Der indhentes en databehandleraftale, som sendes til EFIF til gennemsyn inden underskrift. Der følges løbende op på databehandleraftalerne.

Brug af billeder og videooptagelser

Elever:

Anvendelse af foto er beskrevet i "Elever – behandling af dine personoplysninger" på <https://www.lemvig-gym.dk/officielt/persondataforordning>.

Ansatte:

Ved underskrift af ansættelsesbrev giver den ansatte tilladelse til, at foto må bruges på Lemvig Gymnasiums hjemmeside, på ludus og andre steder i fm. den ansattes arbejde på Lemvig Gymnasium.

Der henvises til "Ansatte – Behandling af dine personoplysninger" på <https://www.lemvig-gym.dk/officielt/persondataforordning>.

Principper for adgangsstyring og tildeling af rettigheder

Ludus (elevers persondata):

Ledelse og administration har adgang til alle data

Lærere har adgang til deres egne elevers data i form af navn, adresse, mobilnr., fravær.

Studievejleder har adgang til alle data på de elever, som de er vejledere for.

Adgangsstyring og tildeling af rettigheder styres af en brugeradministrator i administrationen via Ludus Web-systemdelen.

Silkeborg Data:

To personer i administrationen har adgang til alle data. Derudover er der bevilget adgang til én ekstern medarbejder i det lønadministrative samarbejde.

Adgange og rettigheder styres af en brugeradministrator i administrationen.

SU og SPSA:

To personer har adgang til data vedrørende SU samt til data om specialpædagogisk støtte.

Rettigheder tildeles af bruger-administratoren på Lemvig Gymnasium.

Digital medarbejdersignatur:

Rettigheder tildeles af brugeradministratoren på Lemvig Gymnasium.

Ved medarbejderes afgang slettes alle adgange og rettigheder.

Anskaffelsespolitik

DPO v/EFIF inddrages ved køb af nye systemer, hvis der er tale om behandling af persondata. Behandling af persondata i det nye system risikovurderes, og hvis der er tale om høj risiko ved behandlingen, foretages der en konsekvensanalyse.

Indgåelse af aftaler om nye systemer underskrives af rektor eller vicerektor, og der indhentes en databehandleraftale, som sendes til gennemsyn hos DPO v/EFIF.



Bortskaffelsespolitik

Dokumenter med persondata til bortskaffelse makuleres enten straks eller kommer i en aflåst affoldsbeholder, som sendes til godkendt makulation.

Ved bortskaffelse af lagringsmedier foretager vores IT-medarbejder overskrivning med special software.

Kassation

Kassationsregler er beskrevet i Lemvig Gymnasiums Slettepolitik, som findes på vores hjemmeside <https://www.lemvig-gym.dk/officielt/persondataforordning>.

Elever:

I systemet Ludus dannes en kørsel med sletning af data 5 år efter ophørsdato.

Undtagelser herfra er eksamensbeviser samt SU-oplysninger, som skal opbevares i 30 år. De opbevares i aflåst lokale.

Ansatte:

I systemet Silkeborg Data (EG) dannes en kørsel af EG med sletning af data 5 år efter ophørsdato.

I systemet IMS Case er der påsat kassationsdatoer, som effektueres ud fra lukkedato (foretages af en ansvarlig i administrationen).

Regnskabsmateriale:

Regnskabsmateriale opbevares uden ophør i regnskabsprogrammet Navision. Alt papirmateriale makuleres manuelt efter 5 år.

Procedurer for regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de organisatoriske og tekniske foranstaltninger

Hvert år afholdes et møde med vores DPO fra EFIF, hvor DPO'en forud for dette møde har udfærdiget en stikprøveerklæring samt en compliancevurdering.

Ved dette møde vurderes effektiviteten af vores politikker, procedurer og retningslinjer.

Effektiviteten vurderes endvidere ved eventuelle sikkerhedsbrud.

Tekniske foranstaltninger

Hvis man ønsker at behandle personoplysninger til et andet formål end det oprindelige, skal behandlingen være forenelig, dvs. der skal anvendes pseudonymisering. Dette har ikke været relevant på Lemvig Gymnasium.

Ved fremsendelse af følsomme personoplysninger sendes altid til e-boks eller sikkermail.

Til eksamen benyttes ministeriets netprøver, hvor elevernes data er anonymiseret ved erstatning af identifikation.



Beskyttelse af oplysninger under opbevaring og transmission

I forbindelse med personaleadministration behandles oplysninger om medarbejderes sygdom, orlov og advarsler. Data opbevares i IMS Case, hvor der kun er adgang for ledelsen og administrationen. Ved fremsendelse af oplysninger til f.eks. den ansatte eller en sagsbehandler, sendes oplysninger kun til e-boks eller sikkermail.

Elevernes oplysninger opbevares i ludus, og fremsendelse af oplysninger foregår som ovenfor beskrevet.

Adgang til oplysninger via internet

Elever og medarbejdere kan tilgå Lemvig Gymnasiums hjemmeside, hvor de kan tilgå relevante oplysninger. Via hjemmesiden kan de tilgå ludus, hvor der logges på med personlig kode.

Sikring af kontorer og andre særlige rum

Politik for sikring af rum og kontorer

1. Formål

Formålet med denne politik er at etablere retningslinjer for sikring af bygninger, rum og kontorer. Denne politik skal beskytte institutionens IT-systemer og fortrolige oplysninger, herunder personoplysninger, mod uautoriseret adgang, manipulation og misbrug.

2. Anvendelsesområde

Denne politik gælder for alle ansatte, studerende, eksterne konsulenter og gæster.

3. Sikring af rum med netværk og tekniske installationer

Adgangskontrol

- Adgang til rum med netværksudstyr, servere, varmestyring (CTS), alarmsystemer og lignende tekniske installationer skal begrænses til autoriseret personale.

Fysisk sikring

- Døre til tekniske rum skal altid være låst.
- Rummene kan kun tilgås med A-nøgle, som er udleveret til autoriseret personale.
- Vinduer skal være sikret og lukkede, når rummet ikke er i brug.
- Rummet skal være underlagt videoovervågning, hvor det er relevant og tilladt.



4. Sikring af kontorer med fortrolige oplysninger

Låst-skærm politik

- Medarbejdere skal låse deres computerskærm, når de forlader deres arbejdsplads, også i korte perioder.
- Computere skal indstilles til automatisk at låse skærmen efter en kort periode med inaktivitet.

Opbevaring af dokumenter

- Fortrolige forretningsoplysninger og personoplysninger skal opbevares i låste skabe eller skuffer, når de ikke er i brug.
- Dokumenter med fortroligt indhold skal makuleres, når de ikke længere er nødvendige.
- Personoplysninger skal behandles i overensstemmelse med institutionens GDPR-politik.
- Kontorer kan kun tilgås med A-nøgle, som er udleveret til autoriseret personale.

5. Alarmsystemer

- Alarmsystemer skal aktiveres, når bygninger og kontorer forlades.
- Alle ansatte, der har adgang til alarmsystemet, skal have en unik personlig kode.
- Koder må ikke deles med andre.

6. Ansvar og konsekvenser

- Alle medarbejdere er ansvarlige for at overholde denne politik.
- Overtrædelse af politikken kan føre til disciplinære handlinger.

Krav til hjemme- og fjernarbejdspladser

Krav til hjemme- og fjernarbejdspladser er beskrevet i "Håndbog til ansatte om sikker databehandling" som findes på <https://www.lemvig-gym.dk/officielt/persondataforordning>.

Overvågning og logning

Kontorer og øvrige sikrede rum har alarm og bevægelsessensor, som bliver slået til, når skolen er lukket.

Logning kan aflæses af systemerne:

- Ludus
- Silkeborg Data
- Navision

EFIF overvåger aktivt login og adfærd på de registrerede, der anvender M365.



Passwordpolitik

Medarbejdere som har adgang til fortrolige oplysninger, skal sørge for at oprette sikre passwords. Sikre password kan eksempelvis indeholde 16 karakterer med store og små bogstaver og mindst et specialtegn.

Flere systemer har automatisk indbygget skift af passwords, og øvrige passwords skal skiftes mindst én gang årligt.

Flere systemer indeholder tofaktor-godkendelse – f.eks.:

- Microsoft outlook (tofaktor-godkendelse ca. hver 30. dag)
- Navision
- Danske Bank
- Vestjysk Bank
- Economic

Og andre systemer kan kun tilgås med personligt MitID, når rettighed er tilføjet af institutionen:

- E-boks
- Su-net
- SPSA
- Tilskudsportalen
- Mobilepay
- Skat.dk
- Nemrefusion

Udarbejdet juni 2026