LEMVIG
GYMNASIUM
STX HHX EUX EUD

Bilag 4

Retningslinje om fortegnelser over behandlingsaktiviteter

Anvendelsesområde

Retningslinje om fortegnelser over behandlingsaktiviteter er udarbejdet i overensstemmelse med kravene i Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (betegnet "forordningen" i det følgende) og gælder for alle ansatte på Lemvig Gymnasium, der behandler personoplysninger, samt for samarbejdspartnere (databehandlere), der udfører opgaver på vegne af Lemvig Gymnasium.

Formål

Formålet med denne retningslinje er at sikre, at Lemvig Gymnasium fører de lovpligtige fortegnelser over behandlingsaktiviteter, som efter anmodning skal stilles til rådighed for Datatilsynet. Fortegnelserne kan ligeledes anvendes som hjælp til at sikre, at der foreligger et grundlag for vurdering af risici for behandling af personoplysninger.

Fortegnelserne skal som hovedregel laves på hovedformålsniveau – eksempelvis "personaleadministration". Der kan dog være fordele ved at nedbryde fortegnelserne i delformål – eksempelvis "ansættelse", "under ansættelsesforholdet" og "efter ansættelsesophør".

Definitioner

Personoplysninger er enhver form for information om en identificeret eller identificerbar fysisk person (den registrerede); ved identificerbar fysisk person forstås en fysisk person, der direkte eller indirekte kan identificeres, navnlig ved en identifikator som f.eks. et navn, et identifikationsnummer, lokaliseringsdata, eller et eller flere elementer, der er særlige for denne fysiske persons fysiske, fysiologiske, genetiske, psykiske, økonomiske, kulturelle eller sociale identitet

Den registrerede er den fysiske person, som personoplysningerne vedrører, fx medarbejdere, elever, leverandører, samarbejdspartnere og andre.

Behandling af personoplysninger skal fortolkes bredt. Begrebet "behandling" dækker over enhver aktivitet eller en række af aktiviteter, som personoplysninger gøres til genstand for. Det kan fx være indsamling, registrering, organisering, systematisering, opbevaring, ændring, søgning, formidling og sletning.

Dataansvarlig er den person eller myndighed/organisation, der alene eller sammen med andre afgør, til hvilke formål og med hvilke hjælpemidler der må foretages behandling af personoplysninger.

Databehandler er den, der behandler personoplysninger på den dataansvarliges vegne – dvs. arbejder under instruks af den dataansvarlige. Databehandler er i henhold til forordningen forpligtet til at føre fortegnelse over behandlingskategorier, der føres på vegne af den dataansvarlige.

Databeskyttelsesrådgiveren (DPO) er en uafhængig person med ekspertise i databeskyttelsesret og –praksis, der skal inddrages i alle spørgsmål om databeskyttelse og rådgive om de databeskyttelsesretlige regler hos Lemvig Gymnasium. Databeskyttelsesrådgiverens funktion er at understøtte, at Lemvig Gymnasium overholder reglerne i forordningen. Databeskyttelsesrådgiveren er en integreret del af Lemvig Gymnasium, og kan efter omstændighederne have andre arbejdsopgaver.

Tekniske og organisatoriske sikkerhedsforanstaltninger skal vurderes ved en risikovurdering af behandlingen af personoplysninger.

Tekniske sikkerhedsforanstaltninger er blandt andet antivirusprogrammer og firewalls, som sikrer, at uvedkommende ikke kan få adgang til it-systemer med personoplysninger.

Organisatoriske sikkerhedsforanstaltninger består blandt andet i, at vores medarbejdere er instrueret i og uddannet til at håndtere behandlingen af personoplysningerne korrekt og sikkert.

Den dataansvarliges fortegnelse over behandlingsaktiviteter

I henhold til forordnings artikel 30, stk. 1, skal Lemvig Gymnasium, når vi er dataansvarlige myndighed, føre en fortegnelse over vores behandlingsaktiviteter – dvs. en fortegnelse over såvel almindelige som følsomme personoplysninger.

Lemvig Gymnasiums fortegnelse skal som minimum indeholde kontaktoplysninger på Lemvig Gymnasium samt vores databeskyttelsesrådgiver. Hvis vi er fælles dataansvarlige med en anden dataansvarlig, skal denne dataansvarlig ligeledes fremgå af fortegnelsen.

I fortegnelsen skal der være en beskrivelse af formålet med databehandlingen. Det kan i mange tilfælde være muligt at samle flere behandlingsaktiviteter i ét sammenhængende logisk formål – eksempelvis ”sagsbehandling” eller ”personaleadministration”.

Fortegnelsen skal give et klart overblik over hvilke personoplysningskategorier vi behandler, eksempelvis ”identifikationsoplysninger”, ”billeder”, ”helbredsoplysninger”. Derudover skal vi beskrive hvilke kategorier af registrerede vi behandler personoplysninger om, eksempelvis ”ansatte”, ”elever” og /eller ”forældre”.

Hvis Lemvig Gymnasium får hjælp til at behandle personoplysninger af en databehandler eller hvis vi videregiver personoplysninger til en ny dataansvarlig, skal dette fremgå af fortegnelsen. Her skal det også beskrives, hvorvidt

oplysningerne overlades/videregives til lande uden for EU, ligesom det skal fremgå hvad hjemmelsgrundlaget for overladelsen/videregivelsen er.

I videst muligt omfang skal Lemvig Gymnasium beskrive, hvornår vi påtænker at slette personoplysningerne igen, samt hvilke tekniske og organisatoriske foranstaltninger vi har indført for at mindske risikoen i forhold til den registreredes rettigheder og frihedsrettigheder, når vi behandler dennes oplysninger.

Se endvidere bilag 1, hvor kravene til dataansvarliges fortegnelse er oplistet.

Databehandlers fortegnelse over kategorier af behandlingsaktiviteter

Når Lemvig Gymnasium behandler personoplysninger på vegne af en anden dataansvarlig, er vi databehandlere.

I tilfælde af at Lemvig Gymnasium er databehandlere, er vi forpligtet til at føre en fortegnelse over alle de kategorier af behandlingsaktiviteter, som vi foretager på vegne af den dataansvarlige.

Fortegnelsen skal som minimum indeholde kontaktoplysninger på Lemvig Gymnasium samt kontaktoplysninger på den dataansvarlige, herunder dennes repræsentant og eventuelle databeskyttelsesrådgiver.

Som databehandlere er Lemvig Gymnasium udelukkende forpligtet til at føre en fortegnelse over de kategorier af behandlingsaktiviteter, som vi foretager på vegne af den dataansvarlige.

Hvis Lemvig Gymnasium får hjælp til at behandle personoplysninger af en underdatabehandler skal dette fremgå af fortegnelsen. Her skal det også beskrives, hvorvidt oplysningerne overlades til lande uden for EU, ligesom det skal fremgå, hvad hjemmelsgrundlaget for overladelsen er.

I videst muligt omfang skal Lemvig Gymnasium beskrive hvilke tekniske og organisatoriske foranstaltninger, vi har indført for at mindske risikoen i forhold til den registreredes rettigheder og frihedsrettigheder, når vi behandler dennes oplysninger på vegne af den dataansvarlige.

Se endvidere bilag 2, hvor kravene til databehandlers fortegnelse er oplistet.

Formkrav og opdatering

Fortegnelsen skal foreligge i skriftlig og elektronisk form.

Fortegnelsen skal opdateres løbende, således Lemvig Gymnasium altid på anmodning kan levere et korrekt overblik over vores behandlingsaktiviteter til Datatilsynet.

LEMVIG
GYMNASIUM
STX HHX EUX EUD

Kontrol og dokumentation

Lemvig Gymnasium skal sikre, at vi løbende foretager en dokumenteret kontrol af, at denne retningslinje overholdes. Kontrollen skal godkendes af bestyrelsen for Lemvig Gymnasium.

Lemvig Gymnasium skal kunne dokumentere (påvise), at:

- Fortegnelsen er udarbejdet, og at den opfylder minimumskravene, som beskrevet i denne retningslinje
- Fortegnelsen foreligger skriftligt og i elektronisk format
- Den løbende kontrol overholdes

Udarbejdet maj 2018

LEMVIG GYMNASIUM
STX HHX EUX EUD

Bilag 1:
Dataansvarliges fortegnelse over behandlingsaktiviteter

Den dataansvarliges fortegnelse skal som minimum indeholde følgende oplysninger:

a) Navn på og kontaktoplysninger på Lemvig Gymnasium og, hvis det er relevant, den fælles dataansvarlige, den dataansvarliges repræsentant og databeskyttelsesrådgiveren	Lemvig Gymnasiums navn og kontaktoplysninger skal oplyses samt databeskyttelsesrådgiverens navn og kontaktoplysninger.
b) Formålene med behandlingen	Samtlige formål med behandlingsaktiviteten skal fremgå – det gælder således også de behandlinger, som eventuelt foretages af en databehandler. Der skal formuleres et samlet logisk sammenhængende formål – eksempelvis ”*personaleadministration*” eller ”*sagsbehandling*”
c) En beskrivelse af kategorierne af registrerede og kategorierne af personoplysninger	Kategorier af registrerede: Eksempelvis ”*ansatte*”, ”*elever*”, ”*tidligere ansatte*”, ”*forældre*”. Kategorier af personoplysninger: Eksempelvis ”*identifikationsoplysninger*”,”*lønoplysninger*”, ”*helbredsoplysninger*”, ”*fagforeningsmæssigt tilhørsforhold*”
d) De kategorier af modtagere, som personoplysningerne er eller vil blive videregivet til, herunder modtagere i tredjelande	Eksempelvis: ”*Offentlige myndigheder – så vidt muligt myndighedens navn, såsom SKAT*”, ”*sociale medier*”, ”*banker*”
e) Hvor det er relevant, overførsler af personoplysninger til et tredjeland, herunder angivelse af dette tredjeland.	Her skal angives om Lemvig Gymnasium har samarbejdspartnere, der er etableret uden for EU. Eksempelvis ”*Google*”, ”*Amazon*”, ”*Facebook*”.

f) Hvis det er muligt, de forventede tidsfrister for sletning af de forskellige kategorier af oplysninger	Eksempelvis: "*Oplysninger om tidligere ansatte slettes 5 år efter fratrædelse".*
g) Hvis det er muligt, en generel beskrivelse af de tekniske og organisatoriske sikkerhedsforanstaltninger omhandlet i artikel 32, stk. 1.	Eksempelvis: "*Personoplysninger opbevares i krypteret og pseudonymiseret form og transmitteres krypteret.* *Fysisk materiale opbevares bag 2 låse*".

LEMVIG
GYMNASIUM
STX HHX EUX EUD

Bilag 2:

Databehandlers fortegnelse over kategorier af behandlingsaktiviteter

Databehandlers fortegnelse skal som minimum indeholde følgende oplysninger:

a) Navn på og kontaktoplysninger på Lemvig Gymnasium og for hver dataansvarlig, på hvis vegne Lemvig Gymnasium behandler personoplysninger, samt, hvis det er relevant, den dataansvarliges eller databehandlerens repræsentant og databeskyttelsesrådgiveren	Lemvig Gymnasiums navn og kontaktoplysninger skal oplyses samt databeskyttelsesrådgiverens navn og kontaktoplysninger.
b) De kategorier af behandlinger, Lemvig Gymnasium foretager på vegne af den enkelte dataansvarlige	Her beskrives hvilke databehandlinger, Lemvig Gymnasium foretager på vegne af den dataansvarlige.
c) Hvor det er relevant, overførsler af personoplysninger til et tredjeland, herunder angivelse af dette tredjeland.	Her skal angives om Lemvig Gymnasium har samarbejdspartnere, der er etableret uden for EU. Eksempelvis "*Google*", "*Amazon*", "*Facebook*".
d) Hvis det er muligt, en generel beskrivelse af de tekniske og organisatoriske sikkerhedsforanstaltninger omhandlet i artikel 32, stk. 1.	Eksempelvis: "*Personoplysninger opbevares i krypteret og pseudonymiseret form og transmitteres krypteret.* *Fysisk materiale opbevares bag 2 låse*".