

Retningslinje om fortegnelser over behandlingsaktiviteter

Indhold

Retningslinje om fortegnelser over behandlingsaktiviteter	1
Anvendelsesområde	2
Formål	2
Definitioner	2
Den dataansvarliges fortegnelse over behandlingsaktiviteter	3
Databehandlers fortegnelse over kategorier af behandlingsaktiviteter	4
Formkrav og opdatering	4
Kontrol og dokumentation	4
Dokumentejer, godkender og versionering	5

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 SOSU Esbjerg, der behandler personoplysninger samt for samarbejdspartnere (databehandlere), der udfører opgaver på vegne af SOSU Esbjerg.

Formål

Formålet med denne retningslinje er at sikre, at SOSU Esbjerg 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 – fx "personaleadministration". Der kan dog være fordele ved at nedbryde fortegnelserne i delformål – fx "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 fx 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, kursister, 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 på SOSU Esbjerg. Databeskyttelsesrådgiverens funktion er at understøtte, at SOSU Esbjerg overholder reglerne i forordningen. Databeskyttelsesrådgiveren er ansat ved IT Center Nord og via kontrakt tilknyttet SOSU Esbjerg som DPO.

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 SOSU Esbjerg, når vi er dataansvarlige myndighed, føre en fortegnelse over vores behandlingsaktiviteter – dvs. en fortegnelse over såvel almindelige som følsomme personoplysninger.

SOSU Esbjergs fortegnelse skal som minimum indeholde kontaktoplysninger på SOSU Esbjerg 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 – fx ”sagsbehandling” eller ”personaleadministration”.

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

Hvis SOSU Esbjerg 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 overlevering/videregivelsen er.

I videst muligt omfang skal SOSU Esbjerg 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 1.1., Dataansvarliges fortegnelse over behandlingsaktiviteter på elev- og kursistadministration.

Se endvidere bilag 1.2., Dataansvarliges fortegnelse over behandlingsaktiviteter på løn- og personaleadministration.

Databehandlers fortegnelse over kategorier af behandlingsaktiviteter

Når SOSU Esbjerg behandler personoplysninger på vegne af en anden dataansvarlig, er vi databehandlere.

I tilfælde af at SOSU Esbjerg 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 SOSU Esbjerg samt kontaktoplysninger på den dataansvarlige, herunder dennes repræsentant og eventuelle databeskyttelsesrådgiver.

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

Hvis SOSU Esbjerg 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 SOSU Esbjerg 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.

Formkrav og opdatering

Fortegnelsen foreligger i såvel skriftlig som elektronisk form.

Fortegnelsen vil løbende blive opdateret, således SOSU Esbjerg altid på anmodning kan levere et korrekt overblik over vores behandlingsaktiviteter til Datatilsynet.

Kontrol og dokumentation

SOSU Esbjerg skal sikre, at vi løbende foretager en dokumenteret kontrol af, at denne retningslinje overholdes. Kontrollen skal godkendes af bestyrelsen på SOSU Esbjerg.

SOSU Esbjerg skal kunne dokumentere (påvise), at:

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

Der henvises i øvrigt til *"Procedure for intern GDPR-audit"*

Dokumentejer, godkender og versionering

Ejer: Claus Larsen

Godkender: Direktør Lisbeth Nørgaard

Dato	Version	Forfatter	Ændringsbeskrivelse
16. februar 2021	1.2	BEK	Der er foretaget ændringer som følge af SOSU Esbjergs nye samarbejde med IT Center Nord og drift af IT
19. februar 2020	1.1	BEK	I afsnittet Kontrol og dokumentation, henvises der til "Procedure for intern GDPR-audit"
29. august 2019	1.0	BEK	