

Retningslinje om god databehandlingskik

Indhold

Retningslinje om god databehandlingskik.....	1
Anvendelsesområde.....	2
Formål.....	2
Definitioner	2
God databehandlingskik	3
Formålsbegrænsning	3
Dataminimering.....	3
Opbevaringsbegrænsning	3
Integritet og fortrolighed	3
Kontrol og dokumentation	3
Dokumentejer, godkender og versionering	4

Anvendelsesområde

Retningslinje om god databehandlingsskik 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, om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (betegnet "forordningen" i det følgende) - gældende for alle ansatte på SOSU Esbjerg, der behandler personoplysninger.

Formål

Formålet med denne retningslinje er at sikre, at SOSU Esbjerg behandler personoplysninger i overensstemmelse med god databehandlingsskik.

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.

Almindelige/fortrolige personoplysninger er alle oplysninger om en identificeret eller identificerbar person, der ikke er omfattet af nedenstående kategori, fx navn, adresse, CPR-nummer, e-mail, billeder og telefonnummer.

Følsomme personoplysninger er oplysninger om helbredsforhold, fagforening, racemæssig eller etnisk baggrund, politisk, religiøs eller filosofisk overbevisning, seksuelle forhold og genetiske oplysninger. Der er tale om en udtømmende liste.

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 Fyn og via kontrakt tilknyttet SOSU Esbjerg som DPO.

God databehandlingskik

SOSU Esbjerg skal sikre, at vi behandler personoplysninger på en lovlig, rimelig og gennemsigtig måde.

Lovlig henviser til, at SOSU Esbjerg sikrer, at der er et lovligt hjemmelsgrundlag, se desuden *retningslinje om behandlingsgrundlag*.

Rimelig henviser til, at SOSU Esbjerg kun må behandle personoplysninger, hvis behandlingens formål med rimelighed ikke kan opfyldes på anden måde.

Gennemsigtig indebærer, at SOSU Esbjerg skal oplyse den registrerede om den behandling, vi foretager om vedkommende. Behandlingen af personoplysninger skal således ske på en åben og oplyst måde.

Formålsbegrænsning

Når der indsamles oplysninger, skal SOSU Esbjerg gøre sig klart, hvilke formål oplysningerne indsamles til, og det skal være saglige formål. Vi må således ikke indsamle oplysninger med den begrundelse, at det *måske* senere kan vise sig nyttigt at være i besiddelse af oplysningerne.

Dataminimering

Når SOSU Esbjerg behandler personoplysninger, skal vi sikre, at behandlingen begrænses til det, der er nødvendigt for at opfylde formålet.

Vi skal således vurdere, om den konkrete behandling kan opfyldes ved at behandle færre personoplysninger.

Opbevaringsbegrænsning

Personoplysninger skal slettes eller gøres anonyme, når det ikke længere er nødvendigt for SOSU Esbjerg at have oplysningerne.

Integritet og fortrolighed

SOSU Esbjerg skal beskytte oplysningerne mod uautoriseret eller ulovlig behandling, ligesom vi skal sikre, at oplysninger ikke går tabt eller bliver beskadiget. Dette sikrer vi ved at etablere passende tekniske og organisatoriske sikkerhedsforanstaltninger.

SOSU Esbjerg må således ikke behandle personoplysninger, førend det er sikret, at der er tilstrækkelig sikkerhed til stede ved behandlingen.

Kontrol og dokumentation

SOSU Esbjerg skal sikre, at der løbende foretages en dokumenteret kontrol af, at denne retningslinje efterleves. Kontrollen godkendes af direktør Lisbeth Nørgaard på vegne af bestyrelsen på SOSU Esbjerg.

SOSU Esbjerg dokumenterer:

- At vi har et lovligt formål med behandlingen af personoplysninger
- At vi overholder kravene til god databehandlingskik
- At 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
18. februar 2020	1.1	BEK	I afsnittet Kontrol og dokumentation, henvises der til "Procedure for intern GDPR-audit"
28. juni 2018	1.0	BEK	-