Retningslinje om behandlingssikkerhed

Indhold

Anvendelsesområde

Retningslinje om behandlingssikkerhed 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 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 gennemfører de nødvendige sikkerhedsmæssige foranstaltninger, der modsvarer de identificerede risici for den registrerede, jf. databeskyttelsesforordningens artikel 25 og 32.

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, 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.

Brud på persondatasikkerheden dækker over alle tilfælde, der fører til hændelig eller ulovlig tilintetgørelse, tab eller ændring af personoplysninger såvel som uautoriseret videregivelse af eller adgang til personoplysninger.

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 en integreret del af SOSU Esbjerg og kan efter omstændighederne have andre arbejdsopgaver.

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

Tekniske sikkerhedsforanstaltninger er bl.a. 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.

Hvad er behandlingssikkerhed?

Når SOSU Esbjerg er dataansvarlig, er det vigtigt, at vi i tilstrækkelig grad beskytter de personoplysninger, som vi behandler.

Som dataansvarlig sikrer vi os således, at der tilvejebringes et sikkerhedsniveau, der forhindrer, at der foretages databehandlinger i strid med forordningen, herunder at uvedkommende får adgang til personoplysningerne, at der sker sikkerhedsbrud, eller at personoplysningerne anvendes til usalige formål.

Vi fastlægger sikkerhedsniveauet ud fra en samlet vurdering af det aktuelle tekniske niveau, implementeringsomkostninger og den pågældende databehandlings karakter, omfang, sammenhæng og formål samt risiciene og alvoren for fysiske personers rettigheder og frihedsrettigheder.

På baggrund af den samlede vurdering gennemfører SOSU Esbjerg passende tekniske og organisatoriske foranstaltninger, således vi sikrer et sikkerhedsniveau, der passer til de identificerede risici, se endvidere *Retningslinje om risikovurdering*.

Beskyttelsesbehovet er større, jo mere følsomme personoplysningerne er. Derudover kan der være andre faktorer, der spiller ind i forbindelse med fastlæggelse af sikkerhedsniveauet, herunder risicienes varierende sandsynlighed samt mængden af data.

Hvis SOSU Esbjerg i forbindelse med samme databehandling behandler såvel almindelige/fortrolige som følsomme oplysninger, tilpasser vi vores sikkerhedsforanstaltninger efter de mest følsomme personoplysninger.

Såfremt én af de sikkerhedsmæssige foranstaltninger, der fremgik af den tidligere gældende sikkerhedsbekendtgørelse, stadig er relevante, vil det være hensigtsmæssigt at benytte sig heraf, fx kravet om logning og autorisation.

Organisatoriske og tekniske foranstaltninger

Hvor den hidtidige persondatalov pålagde offentlige myndigheder at efterleve sikkerhedsbekendtgørelsen, foreskriver databeskyttelsesforordningen ikke, hvilke foranstaltninger der skal træffes for at imødekomme forordningens krav.

SOSU Esbjerg vurderer således selv, hvordan vi løser opgaven med at skabe et tilstrækkeligt sikkerhedsniveau ud fra en risikovurdering.

Eksempler på foranstaltninger fremgår af bilag 1.

Nedenfor forklares nogle af de mulige foranstaltninger, som SOSU Esbjerg kan gøre brug af.

Pseudonymisering

Ved pseudonymiserede personoplysninger forstås, at SOSU Esbjerg behandler personoplysninger på en sådan måde, at de ikke længere direkte kan henføres til en bestemt person uden brug af supplerende oplysninger – en såkaldt omsætningsnøgle.

For at der er tale om pseudonymiserede personoplysninger, kræves det, at omsætningsnøglen opbevares særskilt, således det kun vil være udvalgte personer, der har adgang til omsætningsnøglen.

Omsætningsnøglen er også underlagt kravet om tekniske og organisatoriske foranstaltninger.

Eksempel:

De sidste 4 cifre i CPR-nummeret erstattes med en "kode", som kan genfindes på en separat liste, hvor man efterfølgende kan se koblingen mellem fødselsdagen og "koden", hvilket giver et personnummer.

Pseudonymiserede personoplysninger kan således give en bedre beskyttelse af den registrerede person, idet det ikke umiddelbart er muligt at identificere personen.

Kryptering

Kryptering skal forstås således, at udvalgte personoplysninger gøres ulæselige ved hjælp af en krypteringsnøgle. For at tilgå de krypterede oplysninger, skal man være i besiddelse af den anvendte krypteringsnøgle.

Overførsel af almindelige og fortrolige personoplysninger via hjemmesider bør beskyttes ved kryptering.

Kommunikationen via hjemmesider kan sikres ved hjælp af SSL-kryptering eller lignende. Der er mulighed for at implementere forskellige grader af kryptering, herunder også det der betegnes som "stærk kryptering" (256 bit SSL/TLS-forbindelse).

Hvis brugere via hjemmesiden får adgang til personoplysninger – fx om sig selv – skal der også skabes sikkerhed for, at oplysningerne ikke udleveres til uvedkommende. Dette kan fx ske ved anvendelse af adgangskode eller digital signatur. Hvis der gives adgang til følsomme personoplysninger, bør der anvendes digital signatur eller lignende (stærk kryptering).

Beredskab i tilfælde af en fysisk eller teknisk hændelse

SOSU Esbjerg har nedsat et beredskab for, hvordan adgangen til personoplysninger genoprettes i tilfælde af fysiske eller tekniske hændelser, herunder fx brand, hacking, overgravede kabler m.v.

Et beredskab handler om at planlægge, hvordan it-driften på baggrund af sådanne hændelser kan genoprettes inden for et nærmere bestemt tidsrum, samt hvordan vi bedst undgår en lignende hændelse – fx ved hjælp af regelmæssige sikkerhedskopier eller overgange til backupsystemer.

Afprøvning af procedure

SOSU Esbjergs hosting-leverandør IT-Center Fyn afprøver regelmæssigt vores firewalls, krypterede forbindelser, adgangskontroller, brugeradministrationsprocesser m.v. med henblik på at sikre, at vi hele tiden er sikkerhedsmæssigt opdateret. Endvidere modtages hvert år en it-revisionserklæring.

Organisatoriske foranstaltninger

Ved nogle ældre it-systemer kan implementeringsomkostninger, der er forbundet med, at SOSU Esbjerg fx skal bringe systemet – der ikke på alle områder helt modsvarer det aktuelle tekniske niveau – op på et passende sikkerhedsniveau, være uforholdsmæssigt store. I disse tilfælde har SOSU Esbjerg mulighed for at imødekomme behovet for større sikkerhed ved hjælp af organisatoriske foranstaltninger. Der er således ingen forpligtelse til at efterkomme sikkerhedskravene alene rent teknisk, hvis der efter en konkret vurdering findes tilstrækkelige organisatoriske løsninger, der også kan bidrage til at sikre det aktuelle tekniske niveau.

På baggrund af vores risikovurdering etablerer SOSU Esbjerg således passende organisatoriske foranstaltninger, herunder fx undervisning af medarbejdere, generelle oplysningskampagner (awareness) eller begrænsning af de medarbejdere, der har adgang til personoplysningerne.

Hvordan griber vi det praktisk an?

1. Identifikation og vurdering af risici

Inden SOSU Esbjerg kan fastlægge, hvilke sikkerhedsforanstaltninger vi skal implementere, er det vigtigt, at vi foretager en risikovurdering, se desuden *retningslinje om risikovurdering*.

2. Identifikation af mulige sikkerhedsmæssige foranstaltninger

Når SOSU Esbjerg har identificeret og vurderet de risici, der kan være i forbindelse med en konkret databehandling, skal vi vurdere, hvilke foranstaltninger vi skal gennemføre for at hindre, at risiciene indtræffer.

Hvilke foranstaltninger der vil være mest hensigtsmæssige, afhænger af de aktuelle omstændigheder, herunder risici og omfang af databehandling i forbindelse med den konkrete databehandling.

3. Implementering af foranstaltninger

Når SOSU Esbjerg har identificeret de mulige sikkerhedsmæssige foranstaltninger, beslutter vi, hvilke der skal gennemføres for at etablere et sikkerhedsniveau, der passer til de identificerede risici.

Databeskyttelse gennem design

Ideen med databeskyttelsesforordningens artikel 25, stk. 1 er, at et højt sikkerhedsniveau bedst sikres ved at implementere databeskyttelse i it-systemer allerede i systemudviklingen.

Ved databeskyttelse gennem design forventes det, at SOSU Esbjerg tager højde for såvel de tekniske indretninger i systemet som vores organisatoriske arbejdsgange.

Kravet om databeskyttelse gennem design indebærer således, at SOSU Esbjerg har en generel overvejelses- og håndteringsforpligtelse, hvilket betyder, at vi allerede i forberedelsesfasen skal overveje, indtænke og håndtere databeskyttelse i vores it-løsninger, således databeskyttelsesforordningen overholdes.

Eksempler på foranstaltninger, der kan indbygges fra start:

- Minimering af persondatabehandlingen (artikel 5, stk. 1, litra c),
- Pseudonymisering af personoplysninger (artikel 4, nr. 5, jf. artikel 5, stk. 1, litra e),
- Transparens hvad angår personoplysningernes funktion og behandling (artikel 5, stk. 1, litra a),
- Kryptering af data i transit (artikel 5, stk.1, litra f jf. artikel 32, stk. 1, litra b)
- Sikring af infrastruktur mod uautoriseret indtrængen (artikel 5, stk.1, litra f jf. artikel 32, stk. 1, litra b)
- Organisatoriske kontroller til autorisation og styring af adgangsrettigheder (artikel 5, stk.1, litra f jf. artikel 32, stk. 1, litra b)
- Udladelse af visning af oplysninger i brugergrænseflader, når disse ikke er nødvendige for en given behandling (artikel 5, stk. 1, litra f)

Databeskyttelse gennem standardindstillinger

I henhold til databeskyttelsesforordningen er SOSU Esbjerg som dataansvarlig forpligtet til at sikre, at når fx softwareprogrammer, online-tjenester, it-systemer eller lignende anvendes til at behandle personoplysninger, skal de indstillingsmuligheder, som systemet m.v. indeholder, som standard indstilles på en måde, der understøtter forordningens krav i artikel 25, stk. 2 om databeskyttelse gennem standardindstillinger.

Hvis systemet m.v. giver mulighed for databeskyttelse, skal dette således indstilles som standard.

Kravet om databeskyttelse gennem standardindstillinger kan ses som et påkrævet supplement til kravet om databeskyttelse gennem design.

Eksisterende it-systemer hvor standardindstillingerne ikke kan ændres, vil ikke blive mødt af databeskyttelsesforordningens nye krav. Det forudsætter dog, at systemerne ikke forhindrer, at SOSU Esbjerg lever op til databeskyttelsesforordningens krav, herunder fx kravene til behandlingssikkerhed i artikel 32 og de grundlæggende principper i artikel 5.

Når et it-system ændres, skal standardindstillingerne opfylde forordningens krav.

Når et eksisterende it-systems standardindstillinger kan ændres, vil SOSU Esbjerg som dataansvarlig være forpligtet til at tilpasse systemets standardindstillinger således, at disse understøtter forordningens krav om bl.a. formålsspecifik behandling.

Kontrol og dokumentation

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

SOSU Esbjerg skal kunne dokumentere (påvise), at:

- Der er tilvejebragt et sikkerhedsniveau, der svarer til de identificerede risici, der er forbundet med en konkret databehandling
- Der er nedsat et beredskab for, hvordan adgangen til personoplysningerne genoprettes i tilfælde af fysiske eller tekniske hændelser, herunder fx brand, hacking, overgravede kabler m.v.
- Beredskabet afprøves regelmæssigt
- Der indtænkes databeskyttelse fra start ved implementering af nye it-systemer m.v.
- De it-systemer m.v. der giver mulighed for det, tilpasses sikkerhedsmæssigt, således databeskyttelse indstilles som standard.

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

Dokumentejer, godkender og versionering

Ejer: Claus Larsen

Godkender: Lisbeth Nørgaard

Dato	Version	Forfatter	Ændringsbeskrivelse
19. februar 2020	1.1	BEK	I afsnittet Kontrol og dokumentation, henvises der til "Procedure for intern GDPR-audit"
20. september 2018	1.0	BEK	-