Retningslinjer om brud på persondatasikkerheden

Indhold

Anvendelsesområde

Retningslinje om brud på persondatasikkerheden 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, samt for samarbejdspartnere (databehandlere), der udfører opgaver på vegne af SOSU Esbjerg.

Formål

Formålet med denne retningslinje er at sikre, at SOSU Esbjerg håndterer eventuelle brud på persondatasikkerheden korrekt og i overensstemmelse med forordningens krav. Dette indebærer bl.a., at der sker anmeldelse til Datatilsynet, og at den registrerede underrettes i de tilfælde, hvor det er påkrævet.

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 ansat ved ITCenterFyn og via kontrakt tilknyttet SOSU Esbjerg.

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.

Hvordan håndterer vi et brud på persondatasikkerheden?

Det kan have omfattende konsekvenser for den registrerede, hvis et brud på persondatasikkerheden ikke håndteres på en passende og rettidig måde. Konsekvenserne kan fx være tab af kontrol over den registreredes personoplysninger, forskelsbehandling, identitetstyveri, finansielle tab, tab af omdømme eller andre betydelige økonomiske eller sociale konsekvenser for den berørte fysiske person.

Det skal derfor sikres, at SOSU Esbjerg har en klar procedure for håndtering af brud på persondatasikkerheden, når vi er henholdsvis dataansvarlig og databehandler.

Når SOSU Esbjerg er dataansvarlig

Hvis der sker et brud på persondatasikkerheden, skal SOSU Esbjerg, som hovedregel og senest inden for 72 timer fra vi er blevet bekendt med bruddet, anmelde det til Datatilsynet.

Såfremt SOSU Esbjerg kan dokumentere, at det er *usandsynligt*, at bruddet på persondatasikkerheden indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder, skal der ikke ske anmeldelse til Datatilsynet.

Vi skal således foretage en risikovurdering af, hvad bruddet har haft af betydning for den registrerede.

I vurderingen af risikoen skal der tages udgangspunkt i de konsekvenser, sikkerhedsbruddet kan have for den registrerede, samt hvad sandsynligheden for disse konsekvenser er.

Afhængigt af hvilken grad af risici vores risikovurdering kommer frem til, skal følgende procedurer følges:

Risici	Procedure
Bruddet indebærer ingen risiko for den registrerede	Ej anmeldelsespligt til Datatilsynet
Bruddet indebærer en risiko for den registrerede	Anmeldelsespligt til Datatilsynet
Bruddet indebærer en *høj* risiko for den registrerede	Anmeldelsespligt til Datatilsynet samt underretningspligt over for den registrerede.

Bruddet indebærer ingen risiko for den registrerede:

I de tilfælde hvor den udførte risikovurdering viser, at det er usandsynligt, at bruddet på persondatasikkerheden har indebåret en risiko for den registreredes rettigheder, er bruddet ikke anmeldelsespligtigt til Datatilsynet.

Bruddet indebærer en risiko for den registrerede

Hvis risikovurderingen viser, at sikkerhedsbruddet indebærer en risiko for den registrerede, er SOSU Esbjerg forpligtet til at anmelde bruddet til Datatilsynet. Anmeldelsen skal ske hurtigst muligt, og senest 72 timer fra SOSU Esbjerg er blevet bekendt med bruddet.

Anmeldelsen til Datatilsynet skal som minimum indeholde:

1. Beskrivelse af karakteren af bruddet samt hvor det er muligt:
    a. Kategorier af registrerede
    b. Antal af berørte registrerede
    c. Kategorier af personoplysninger
    d. Antal af berørte registreringer af personoplysninger
2. Navn og kontaktoplysninger på SOSU Esbjergs databeskyttelsesrådgiver
3. Beskrivelse af mulige konsekvenser af sikkerhedsbruddet
4. Beskrivelse af de tekniske og organisatoriske foranstaltninger, som SOSU Esbjerg har truffet eller foreslår truffet for at mindske skaden.

Se desuden bilag 1, som indeholder en skabelon til brug for anmeldelse.

Bruddet indebærer en høj risiko for den registrerede

I de tilfælde hvor den udførte risikovurdering viser, at bruddet på persondatasikkerheden har indebåret en *høj* risiko for den registreredes rettigheder, skal bruddet anmeldes til Datatilsynet, og de registrerede skal desuden, som hovedregel, underrettes – se dog undtagelser for underretning nedenfor.

Hvis det skulle ske, at vi i vores risikovurdering er nået frem til, at bruddet ikke indebærer en høj risiko for den registrerede, kan vi i visse tilfælde alligevel blive pålagt at underrette den registrerede, såfremt Datatilsynet i deres undersøgelse af bruddet vurderer, at der har været tale om en høj risiko.

Anmeldelsen til Datatilsynet skal som minimum indeholde:

1. Beskrivelse af karakteren af bruddet, samt hvor det er muligt:
    a. Kategorier af registrerede
    b. Antal af berørte registrerede
    c. Kategorier af personoplysninger
    d. Antal af berørte registreringer af personoplysninger
2. Navn og kontaktoplysninger på SOSU Esbjergs databeskyttelsesrådgiver
3. Beskrivelse af mulige konsekvenser af sikkerhedsbruddet
4. Beskrivelse af de tekniske og organisatoriske foranstaltninger, som SOSU Esbjerg har truffet eller foreslår truffet for at mindske skaden.

Anmeldelsen kan sendes til dt@datatilsynet.dk eller via Datatilsynets hjemmeside.

Se endvidere bilag 1, som indeholder en skabelon til brug for anmeldelse.

Underretningen til den registrerede skal som minimum indeholde:

1. Beskrivelse af karakteren af bruddet
2. Navn og kontaktoplysninger på SOSU Esbjergs databeskyttelsesrådgiver
3. Beskrivelse af mulige konsekvenser af sikkerhedsbruddet
4. Beskrivelse af de tekniske og organisatoriske foranstaltninger, som SOSU Esbjerg har truffet eller foreslår truffet for at mindske skaden.

Se endvidere bilag 2, som indeholder en skabelon til brug for underretning af den registrerede.

Situationer hvor SOSU Esbjerg, på trods af høj risiko, ikke er forpligtet til at underrette den registrerede.

Én af følgende betingelser skal være opfyldt:

1. SOSU Esbjerg har gennemført passende tekniske og organisatoriske beskyttelsesforanstaltninger, og disse foranstaltninger er blevet anvendt på de personoplysninger, som er berørt af bruddet på persondatasikkerheden, navnlig foranstaltninger der gør personoplysningerne uforståelige for enhver, der ikke har autoriseret adgang hertil, som fx kryptering
2. SOSU Esbjerg har efter bruddet truffet foranstaltninger, der sikrer, at den høje risiko for den registreredes rettigheder sandsynligvis ikke længere er reel

3. Det vil kræve en uforholdsmæssig indsats. I et sådant tilfælde skal der i stedet foretages en offentlig meddelelse eller tilsvarende foranstaltning, hvorved den registrerede underrettes på en tilsvarende effektiv måde.

Databeskyttelsesrådgiveren

SOSU Esbjergs databeskyttelsesrådgiver inddrages altid, når der sker et brud på persondatasikkerheden.

Når SOSU Esbjerg er databehandler

I de tilfælde hvor SOSU Esbjerg er databehandler for en anden dataansvarlig, underretter vi uden unødig forsinkelse den dataansvarlige efter at være blevet opmærksom på, at der er sket et brud på persondatasikkerheden.

Det er vigtigt, at SOSU Esbjerg ligeledes instruerer vores databehandlere i, at underrette SOSU Esbjerg, såfremt der skulle ske et brud på persondatasikkerheden.

Fortegnelse over sikkerhedsbrud

SOSU Esbjerg er forpligtet til at dokumentere alle brud på persondatasikkerheden. Efter anmodning fra Datatilsynet, skal vi udlevere denne dokumentation.

Dokumentationen skal som minimum indeholde følgende:

1. Beskrivelse af karakteren af bruddet, samt hvor det er muligt:
    a. Kategorier af registrerede
    b. Antal af berørte registrerede
    c. Kategorier af personoplysninger
    d. Antal af berørte registreringer af personoplysninger
2. Navn og kontaktoplysninger på SOSU Esbjergs databeskyttelsesrådgiver
3. Beskrivelse af mulige konsekvenser af sikkerhedsbruddet
4. Beskrivelse af de tekniske og organisatoriske foranstaltninger, som SOSU Esbjerg har truffet eller foreslår truffet for at mindske skaden.
5. Dokumentation for anmeldelse til Datatilsynet og evt. underretning til den registrerede.

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:

- Vi foretager den nødvendige risikovurdering i forhold til den registreredes rettigheder
- Vi anmelder brud på persondatasikkerheden i de tilfælde, hvor det er påkrævet
- Anmeldelsen indeholder de minimumskrav, som forordningen stiller
- Vi underretter den registrerede om brud persondatasikkerheden i de tilfælde, hvor bruddet har indebåret en høj risiko for den registrerede

- Vi har instrueret vores databehandlere i at underrette os, hvis der sker et brud
- Vi overholder den løbende kontrol.

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

Dokumentejer, godkender og versionering

Ejer: Claus Larsen

Godkender: Lisbeth Nørgaard

Dato	**Version**	**Forfat-ter**	**Ændringsbeskrivelse**
19. februar 2020	1.1	BEK	I afsnittet kontrol og dokumentation henvises der til "Procedure for intern GDPR- audit"
28. maj 2018	1.0	CLL	-