INFORMATIONSSIKKERHEDSPOLITIK

for

M/S Museet for Søfart v. 25.05.2018

Indhold

Baggrund

1. Bestyrelsen og direktionen i M/S Museet for Søfart (herefter "ledelsen"), som opererer indenfor museumsområdet, beliggende Ny Kronborgvej 1, 3000 Helsingør, forpligter sig herved til at sikre, at M/S Museet for Søfarts informationsaktiver, herunder persondata, behandles med en passende grad af organisatorisk og teknisk sikkerhed med henblik på at sikre informationsaktivernes fortrolighed, integritet og tilgængelighed.

2. Derudover forpligter bestyrelsen og direktionen i M/S Museet for Søfart sig til at sikre, at M/S Museet for Søfarts persondata behandles lovligt, rimeligt og gennemsigtigt, herunder, men ikke udelukkende, ved at sikre at behandlingen af persondata sker på et gyldigt grundlag.

3. M/S Museet for Søfart overholder ovenstående under hensyntagen til M/S Museet for Søfarts konkurrenceevne, omkostningerne herved og de pågældende behandlingers karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder.

4. Ledelsen har besluttet sig for at udvikle og administrere informationssikkerhedsstrategier, som sikrer et informationssikkerhedsniveau, der følger principperne i de relevante dele af DS-/ISO-standarderne, og at dette dokumenteres i et ledelses- og styringssystem for informationssikkerhed.

5. M/S Museet for Søfarts ledelses- og styringssystem for informationssikkerhed består af informationssikkerhedspolitikken samt eventuel deraf afledt dokumentation (kontroller, bilag, politikker, instrukser, forretningsgange, standarder og vejledninger mv.) og benævnes samlet ledelses- og styringssystem for informationssikkerhed.

6. Ledelses- og styringssystemet for informationssikkerhed revideres og ajourføres mindst én gang om året eller efter behov.

7. Alt efter udviklingen i de eksterne omstændigheder og udviklingen i de interne behov vil M/S Museet for Søfart udvide eller ændre sigtet med ledelses- og styringssystemet for informationssikkerhed, ligesom det ikke på nuværende tidspunkt kan fastlægges hvilke dele af ledelses- og styringssystemet for informationssikkerhed, der udmønter sig i afledt dokumentation.

Indledning

8. Denne informationssikkerhedspolitik udgør den overordnede ramme for informationssikkerheden hos M/S Museet for Søfart.

9. Ledelses- og styringssystemet for informationssikkerhed udgør samtidig M/S Museet for Søfarts dokumentation for, at M/S Museet for Søfart overholder de til enhver tid gældende regler om behandling af persondata.

Lovgivning

10. M/S Museet for Søfart har identificeret de lovgivningsmæssige rammer, som M/S Museet for Søfarts styring af sine informationsaktiver under alle omstændigheder skal holde sig indenfor. M/S Museet for Søfarts aktiviteter kan dog i visse henseender være berørt af anden lovgivning:

10.1 databeskyttelsesloven (når denne får virkning) og

10.2 databeskyttelsesforordningen (Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016), når denne får virkning.

10.3 Cookie-bekendtgørelsen, sundhedslovgivningen, lov om indhentning af børneattester, revisionsstandarder, museale standarder, museumsloven, selskabsloven, regnskabsloven samt arkivloven.

Formål

11. Informationsaktiver, herunder persondata, og IT-systemer er nødvendige og livsvigtige for M/S Museet for Søfart, og informationssikkerheden, herunder persondatasikkerheden, har derfor vital betydning for M/S Museet for Søfarts troværdighed og funktionsdygtighed.

12. Formålet med informationssikkerhedspolitikken er at definere en ramme for beskyttelse af M/S Museet for Søfarts informationsaktiver, herunder persondata og særligt at sikre, at kritiske og følsomme informationsaktiver, herunder persondata og IT-systemer bevarer deres fortrolighed, integritet og tilgængelighed.

13. Formålet er derudover at sikre, at de persondata, som M/S Museet for Søfart er dataansvarlig for behandles lovligt, rimeligt og gennemsigtigt.

14. Formålet er endelig at sikre, at ovenstående kan dokumenteres.

Risikostyring

15. M/S Museet for Søfarts ledelse har besluttet sig for et sikkerheds- og efterlevelsesniveau, der er afstemt efter risiko og væsentlighed samt overholder lovkrav og indgåede aftaler, herunder licensbetingelser.

16. Risikovurderingen er sket efter følgende overordnede fremgangsmåde, hvorved risici skal:

16.1 identificeres og beskrives (risikoidentifikation)

16.2 analyseres og måles (risikoanalyse)

16.3 evalueres i forhold til risikotolerancen (risikoevaluering).

17. M/S Museet for Søfarts sikkerheds- og efterlevelsesniveau ændrer sig efter omstændighederne på baggrund af en fornyet risikovurdering, der især tager hensyn til hvilke brud på persondatasikkerheden, der kan konstateres, herunder de faktiske omstændigheder ved bruddet på persondatasikkerheden, dets virkninger og de trufne afhjælpende foranstaltninger.

18. Der gennemføres under alle omstændigheder en risikovurdering hvert 5. år, så ledelsen kan holde sig informeret om det aktuelle risikobillede forbundet med det gældende sikkerheds- og efterlevelsesniveau.

19. Der foretages ligeledes en risikovurdering ved større forandringer i M/S Museet for Søfart, herunder ved væsentlig ændring eller udskiftning af IT-systemer, som M/S Museet for Søfart anvender til at behandle persondata.

20. M/S Museet for Søfart gennemfører en afbalanceret risikovurdering under hensyntagen til konkurrenceevne og de økonomiske omkostninger.

21. Til brug for ovenstående dokumenterer den IT-ansvarlige brud på informationssikkerheden, herunder brud på persondatasikkerheden, ikke mindst på baggrund af underretninger fra M/S Museet for Søfarts databehandlere.

22. Til brug for ovenstående fører M/S Museet for Søfart en fortegnelse over behandlingsaktiviteterne, som den HR-ansvarlige løbende opdaterer.

Kommunikation

23. For at realisere formålene for informationssikkerhedspolitikken

23.1 oplyser M/S Museet for Søfart medarbejderne om ansvarlighed i relation til M/S Museet for Søfarts informationsaktiver, herunder persondata. Hver medarbejder meddeles således indholdet af de overordnede formål med informationssikkerhedspolitikken samt de dele af ledelses- og styringssystemet for informationssikkerhed, der er relevant for den enkelte medarbejder alt efter, hvad der er udmøntet i dokumentation.

23.2 oplyser M/S Museet for Søfart alle eksterne samarbejdspartnere, handelsrelationer mv., som har en relation til M/S Museet for Søfart, om indholdet af denne informationssikkerhedspolitik.

24. Hensigten er, at sikkerhedsproblemer, herunder brud på informations- og persondatasikkerheden, forebygges, eventuelle skader kan begrænses, og retablering af informationssikkerhedsaktiver, herunder persondata kan sikres.

Omfang og ansvar

25. Informationssikkerhedspolitikken omfatter alle M/S Museet for Søfarts informationsaktiver, herunder persondata, uanset hvilken form de opbevares og formidles på, herunder informationsaktiver, herunder persondata, som ikke tilhører M/S Museet for Søfart, men som M/S Museet for Søfart kan gøres ansvarlig for.

26. Dette inkluderer fx alle data om personale, data om finansielle forhold, alle data, som bidrager til administrationen af M/S Museet for Søfart, produktionsdata og anlægsdata samt informationsaktiver, herunder persondata, som er overladt M/S Museet for Søfart af andre. Disse data kan være faktuelle oplysninger, optegnelser, registreringer, rapporter, forudsætninger for planlægning eller enhver anden information, som kun er til intern brug.

27. Denne politik gælder for alle ansatte uden undtagelse, både fastansatte og personer, som midlertidigt arbejder for M/S Museet for Søfart. Alle disse personer bliver her betegnet som ”medarbejderne”.

IT-drift

28. Ved udlicitering af dele af eller hele IT-driften skal det sikres i samarbejdet med IT-leverandøren, i museets tilfælde ekstern IT-konsulent Jens W. Skov, at M/S Museet for Søfarts sikkerheds- og efterlevelsesniveau fastholdes, således at IT-leverandøren, dennes faciliteter og de medarbejdere, som har adgang til M/S Museet for Søfart, mindst lever op til M/S Museet for Søfarts sikkerheds- og efterlevelsesniveau.

29. Ved outsourcing i museets tilfælde Danløn og Foreningsadministration, skal det sikres, at der indgås databehandleraftaler, der som minimum indeholder de krav, som M/S Museet for Søfart skal stille som dataansvarlig til en IT-leverandør, der behandler data for M/S Museet for Søfart.

Sikkerhedsniveau

30. Det er M/S Museet for Søfarts politik at beskytte sine informationsaktiver, herunder persondata og udelukkende tillade brug, adgang og offentliggørelse af informationsaktiver, herunder persondata, i overensstemmelse med M/S Museet for Søfarts retningslinjer og under hensyntagen til den til enhver tid gældende lovgivning.

31. M/S Museet for Søfart fastlægger på baggrund af en risikovurdering et sikkerheds- og efterlevelsesniveau, som svarer til betydningen af de pågældende informationsaktiver, herunder persondata.

32. Det operationelle ansvar for den daglige styring af informationssikkerhedsindsatsen, er placeret hos den IT-ansvarlige.

33. Økonomichefen sikrer, at de aktiviteter, standarder, retningslinjer, kontroller og foranstaltninger, der er beskrevet i ledelses- og styringssystemet for informationssikkerhed, gennemføres og efterleves.

34. Økonomichefen og den IT-ansvarlige sikrer ligeledes, at informationssikkerheden integreres i alle forretningsgange, driftsopgaver og projekter samt i forhold til samarbejdet med aktuelle eller fremtidige IT-leverandører.

Beredskab

35. Beredskabets formål er at sikre M/S Museet for Søfarts robusthed overfor følgerne af brud på informationssikkerheden, herunder brud på persondatasikkerheden.

36. Den IT-ansvarlige sikrer, at M/S Museet for Søfart kan

36.1 samarbejde efter anmodning med Datatilsynet

36.2 anmelde brud på persondatasikkerheden til Datatilsynet uden unødig forsinkelse og om muligt senest 72 timer, efter at M/S Museet for Søfart er blevet bekendt med bruddet på persondatasikkerheden, hvis der efter en konkret vurdering er krav herom

36.3 give underretning til den eller de registrerede om bruddet uden unødig forsinkelse, hvis bruddet på persondatasikkerheden sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder og frihedsrettigheder.

36.4 træffe passende foranstaltninger for at begrænse den skade, som den registrerede har lidt ved brud på persondatasikkerheden.

Sikkerhedsbevidsthed (awareness)

37. Informationssikkerhed, herunder persondatasikkerhed, vedrører M/S Museet for Søfarts samlede informationsflow, og gennemførelse af en informationssikkerhedspolitik kan ikke foretages af ledelsen alene.

38. Alle medarbejdere har et ansvar for at bidrage til at beskytte M/S Museet for Søfarts informationsaktiver, herunder persondata, mod uautoriseret eller ulovlig behandling og mod hændeligt tab, tilintetgørelse eller beskadigelse.

39. Alle medarbejdere skal derfor løbende uddannes i informationssikkerhed, herunder persondatasikkerhed, i relevant omfang.

40. Som brugere af M/S Museet for Søfarts informationsaktiver, herunder persondata, må alle medarbejdere følge informationssikkerhedspolitikken og de dokumenter, der er afledt heraf.

41. Medarbejderne skal beskytte informationsaktiver, herunder persondata, på en måde, som er i overensstemmelse med informationsaktivernes, herunder persondataenes, karakter, følsomhed, behandlingsgrundlag, beskyttelsesniveau (IT-sikkerhed), fortrolighed og forretningskritiske betydning.

42. Medarbejderne må kun anvende M/S Museet for Søfarts informationsaktiver, herunder persondata, i overensstemmelse med den arbejdsfunktion, de udfører i M/S Museet for Søfart.

Brud på informations- og persondatasikkerheden

43. Såfremt en medarbejder opdager trusler mod informations- eller persondatasikkerheden eller brud herpå, skal dette straks meddeles til den ansvarlige for den daglige ledelse af informationssikkerhedsindsatsen.

44. Medarbejdere, som bryder informationssikkerhedspolitikken eller deraf afledte retningslinjer, vil blive udsat for disciplinære forholdsregler i overensstemmelse med den pågældendes ansættelseskontrakt, gældende ret og M/S Museet for Søfarts medarbejderinstruks, jf. nedenfor under dokumentation.

Dokumentation

45. Som angivet indledningsvis udgøres ledelses- og styringssystemet for informationssikkerhed af nærværende informationssikkerhedspolitik samt eventuel deraf afledt dokumentation, herunder fortegnelse over behandlingsaktiviteter, kontroller, bilag, politikker, instrukser, forretningsgange, standarder og vejledninger mv. alt efter hvad M/S Museet for Søfart løbende finder relevant.

46. Ledelses- og styringssystemet for informationssikkerhed kan, hvis ønsket, indgå som en blandt flere kontroller til dokumentation af, at kontrolmålene i Anneks A i ISO27001 er opfyldt helt eller delvist.

47. Ledelses- og styringssystemet for informationssikkerhed samt den tilhørende dokumentation nedenfor, skal suppleres af andre, relevante kontroller i henhold til eksempelvis ISO27002 alt efter M/S Museet for Søfarts behov og aktiviteter, hvis M/S Museet for Søfart ønsker at blive certificeret. En certificeringsproces må forventes at indebære ændringer af nærværende ledelses- og styringssystemet for informationssikkerhed samt tilhørende dokumentation.

48. De dokumenter, der efter lovgivningen skal udarbejdes og kunne fremvises for de relevante myndigheder, herunder især Datatilsynet, fremgår nedenfor.

48.1 Ledelses- og styringssystem for informationssikkerhed samt tilhørende dokumentation (art. 5 og art. 24).

48.2 Fortegnelse over behandlingsaktiviteter (art. 30 i databeskyttelsesforordningen).

48.3 Dokumentation for brud / logbog (art. 33 i databeskyttelsesforordningen

48.4 Instruks til medarbejderne hos den dataansvarlige og databehandleren med anvisning om, at enhver fysisk person, der udfører arbejde for den dataansvarlige eller databehandleren, og som får adgang til personoplysninger, kun behandler disse efter instruks fra den dataansvarlige, medmindre behandling kræves i henhold til EU-retten eller medlemsstaternes nationale ret (art. 32 databeskyttelsesforordningen)

48.5 Databehandleraftaler vedlægges, efter de er tjekket igennem for, om de lever op til kravene (art. 28 i databeskyttelsesforordningen)

48.6 Oplysning til de registrerede (art. 13 og art. 14 i databeskyttelsesforordningen)

48.7 Samtykkeerklæring til ansatte, kunder mv. (art. 6. art. 9 og art. 10 i databeskyttelsesforordningen)

49. M/S Museet for Søfart har som led i udmøntningen af det IT-sikkerhedsniveau, der på baggrund af en løbende risikovurdering er fastlagt, udarbejdet følgende politikker, der gemmes på server + i fysisk kopi:

49.1 Sikkerhedspolitik i forbindelse med personaleadministration

49.2 Fortegnelse over behandling ved personaleadministration

49.3 Fortegnelse over behandling ved klubadministration

49.4 Fortegnelse over behandling ved administration af booking og arrangementer

49.5 Fortegnelse over behandling ved arkiv- & museumsadministration

49.6 IT-sikkerhedspolitik

49.7 Datasikkerhed MS

49.8 Backuprutine MS

49.9 Konsekvensanalyse og risikovurdering incl. beredskabsplan (på vej)

49.10 Persondatapolitik for vores medarbejdere

49.11 Procedure ved anmodning om indsigt og sletning af persondata (på vej)

49.12 Standardsvar ved ansættelsesopgaver i M/S Museet for Søfart

49.13 Samtykkeerklæring vedrørende brug af medarbejderbilleder på internettet

49.14 Politik om TV-overvågning (afventer udkast fra Dansk Erhverv)

49.15 Notat om, hvorfor organisationen ikke skal have en DPO

Ikrafttræden

50. Denne informationssikkerhedspolitik træder i kraft den 25.05.2018.