Danske Havne

Bredgade 23, 2. tv
1260 København K

Telefon 7211 8100

efn@danskehavne.dk
Dir 61710706

www.danskehavne.dk

ORIENTERING OM PERSONDATAFORORDNINGEN

Baggrund

Havne indsamler, opbevarer eller behandler personoplysninger i forbindelse med personaleadministration, adgangskontrol, videoovervågning, cookies på havnens hjemmeside og i mange andre sammenhænge. Som det gælder for andre virksomheder, er det derfor vigtigt at havne er opmærksomme på overholdelse af reglerne vedrørende persondata.

Der er vedtaget en ny persondataforordning, som gælder i alle EU-lande og træder i kraft 25. maj 2018. Forordningen erstatter i udgangspunktet den danske lov om behandling af personoplysninger (Persondataloven) fra 2001.

Teksten i EU-forordningen ligger fast og gælder direkte, men Danmark har mulighed for at lave nationale særregler på en række områder. I august sendte Justitsministeriet et lovforslag i høring, som præciserer nogle af forordningens bestemmelser. Den endelige vedtagelse af det danske regelsæt forventes først at ske primo 2018. Men fordi de overordnede linjer ligger fast allerede nu, kan man med fordel gå i gang med at sikre sig, at man overholder forordningen, når den træder i kraft maj 2018.

Forordningen bygger på en række punkter videre på den eksisterende persondatalov. Der er dog introduceret nye bestemmelser, som havnene skal være opmærksomme på og tage højde for.

For at sikre overholdelse af forordningen kræver det, at havne, ligesom andre virksomheder, analyserer, hvilke personoplysninger de har, og hvordan de systemer de benytter til at behandle personoplysningerne er bygget op. Derfor varierer håndtering af personoplysninger fra havn til havn og den enkelte havn er nød til at finde sin individuelle løsning for leve op til forordningens krav.

Med forordningen indføres bl.a. skærpede sanktioner, hvis reglerne ikke overholdes og med den omfattende og detaljerede regulering øges fokus på cybersikkerheden betragteligt.

Denne orientering har til formål at give et overblik over hvordan forordningen er opbygget, og hvordan man går i gang med at kortlægge de personoplysninger, man håndterer, og hvordan man identificerer hvilke tiltag, der skal iværksættes for at overholde reglerne. Den er ikke en komplet facitliste, men giver et godt udgangspunkt for at gå i gang. Nedenfor følger en sammenfatning af de regler i persondataforordningen, som vi vurderer har særlig interesse for havnene.

Indhold

De grundlæggende principper

Al behandling, indsamling mv. skal være saglig, nødvendig og relevant. Det betyder at indsamlingen af personoplysninger skal have et udtrykkeligt angivet og legitimt formål, der dækker et sagligt behov i den konkrete situation. Der skal ikke registreres andre personoplysninger, end hvad der er nødvendigt og behandlingen af oplysningerne skal også begrænses til det, der er nødvendigt.

Havnen har pligt til at træffe de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger for at beskytte de personoplysninger, der indsamles og behandles. Forordningen foreskriver ikke de specifikke foranstaltninger, der skal træffes, og havnen skal derfor løbende sikre, at beskyttelsen af personoplysninger er tilstrækkelig ud fra de konkrete risici forbundet med havnens behandling af personoplysninger.

Nye tiltag med persondataforordningen

Blandt de nye tiltag i persondataforordningen skal især fremhæves:

- Dokumentation for at reglerne overholdes
  Der skal foreligge skriftlig dokumentation for, at havnen overholder de persondataretlige regler, og havnen skal løbende føre en fortegnelse over de kategorier af persondatabehandlinger, som havnen foretager.

- Nye rettigheder for de registrerede
  Ved indsamling af personoplysninger, skal der oplyses om grundlaget for indsamlingen, fx som led i en aftale eller via samtykke. De registrerede skal også orienteres om deres rettigheder efter forordningen.

- Rapportering af databrud
  Havnen har forpligtelse til at underrette Datatilsynet og berørte personer om eventuelle sikkerhedsbrud, hvis vedkommendes personoplysninger er blevet kompromitterede.

- Forøget bødeniveau
  Brydes forordningens regler, kan det udløse en bøde på op til €20 mio. eller 4% af en virksomheds globale omsætning.

Hvad er personoplysninger?

I forordningen anvendes betegnelsen "personoplysninger" om persondata, som omfatter enhver form for information om en identificeret eller identificerbar fysisk person. Krypterede oplysninger er også omfattet, så længe nogen kan gøre oplysningerne læsbare og dermed identificere de personer, som oplysningerne vedrører.

Personoplysninger opdeles i to kategorier:

- almindelige oplysninger
- følsomme oplysninger.

I forordningen defineres følsomme oplysninger således:
Følsomme oplysninger

- fagforeningsmæssige tilhørsforhold
- helbredsoplysninger samt genetisk og biometrisk data
- racemæssig eller etnisk baggrund
- politisk, religiøs eller filosofisk overbevisning
- oplysninger om seksuelle forhold eller seksuel orientering.

Behandling af følsomme oplysninger anses i udgangspunktet for, at medføre en større risiko for den registreredes grundlæggende rettigheder, og der er som følge heraf skærpede krav til behandlingen og hjemlen til behandlingen.

Karakteren af de såkaldte "almindelige personoplysninger" spænder meget vidt og udgør fx følgende:

Almindelige personoplysninger

- navn
- adresse
- telefonnummer
- e-mailadresse
- uddannelse/stilling/arbejdsområde
- anciennitet
- profilbillede
- initialer/login-navn/medarbejder ID
- nummerplade
- ansættelsesforhold
- økonomiske forhold fx skat, løn
- advarsler, fratrædelse, årsager hertil
- sygedage
- tjenestelige forhold
- familieforhold
- sociale forhold
- cpr-nummer

- strafbare forhold, fx straffeattester
- andre rent private forhold, der ikke hører under følsomme oplysninger.

Det er vigtigt at understrege, at det altid skal vurderes konkret om behandling af oplysninger er nødvendige, saglige og proportionale, samt om de sikkerhedskrav der er opstillet imødekommer de risici, der er forbundet med behandlingen af de pågældende data. Sagt med andre ord, så er behandlingen af "almindelige oplysninger" ikke nødvendigvis problemfri. Det er endvidere vigtigt at bemærke, at der er skærpede krav til behandling af fx straffeattester, ligesom at det forventes, at Folketinget vil vedtage skærpede krav i forhold til behandling af cpr-numre.

Mange personoplysninger indsamles i forbindelse med personale-administration, men kan også finde sted i forbindelse med:

- adgangskontrol
- videoovervågning
- logning i it-systemer, også hvis persondata gemmes fra SafeSeaNet
- maillister til udsendelse af fx nyhedsbrev
- cookies indsamlet på hjemmeside
- kundelister (kun privatpersoner eller enkeltmandsvirksomheder).

Personoplysninger opbevaret elektronisk og fysisk er omfattede

Forordningen gælder for al elektronisk behandling af personoplysninger. Enhver systematisk behandling af personoplysninger er også omfattet, selvom den ikke foregår elektronisk. Det betyder, at forordningen også gælder for manuelle behandlinger af personoplysninger, som er indeholdt i et register. Eksempler er f.eks. sagsmapper, ringbind m.v.

Andre centrale begreber

Dataansvarlig

Den dataansvarlige er den virksomhed, der overordnet bestemmer, hvilke personoplysninger der skal behandles, hvorfor og hvordan de behandles. Havnen vil blive betegnet som dataansvarlig.

Databehandler

Den dataansvarlige kan benytte en ekstern databehandler til at indsamle eller behandle personoplysninger på sine vegne. Eksempler på databehandlere er leverandører af hosting eller cloud-ydelser, eller en ekstern lønadministration.

Behandling
Begrebet indbefatter i hovedtræk enhver håndtering af en personoplysning, og altså også selve indsamlingen af oplysninger, videregivelse, opbevaring og sletning. Alle digitale behandlinger af personoplysninger er omfattede. Derudover gælder persondataforordningen også for fysiske manuelle behandlinger, hvis personoplysninger som nævnt ovenfor, er indeholdt i et register, fx sagsmapper eller ringbind.

Sådan kommer havnen godt i gang

Kortlægning af personoplysninger og datastrømme

Start med at få et overblik over havnens personoplysninger, for at finde ud af hvilke oplysninger havnen har og hvorfor.

Relevante spørgsmål at tage stilling til er:

- Hvilke kategorier af personoplysninger indsamles og behandles, og hvorfor?
- Hvor kommer personoplysningerne fra?
- Hvilke registrerede personer vedrører oplysningerne?
- Hvor behandles oplysningerne, og hvem har adgang?
- Hvilke systemer bruges til behandling af oplysningerne?

Eksempler på hvor personoplysninger opbevares er i fysiske personalemapper, et mail- og arkiveringssystem, lønadministration, havnens intranet eller på eksterne hjemmesider. Det er også vigtigt, at tage højde for både tredjepartssystemer som cloud-løsninger, og interne processer. Plejer havnens medarbejderne for eksempel at gemme oplysninger på computerens skrivebord eller i private mapper?

Datastrømme kortlægges ved at følge dataene i deres "levetid", dvs. fra indsamling til sletning. F.eks. i forhold til personoplysninger om medarbejdere, vil nogle oplysninger være indsamlet fra jobansøgninger, og nogle oplysninger vil først blive slettet efter ansættelsesforholdets ophør.

Resultatet af en datastrømsanalyse bør være en oversigt over havnens datastrømme, herunder de systemer havnen anvender, og indholdet af systemerne, både hvad angår de registrerede personer og de typer af oplysninger, der behandles. Oversigten kan derefter bruges som basis for det videre arbejde.

I samme forbindelse bør der også tages stilling til, om behandlingen af data lever op til de grundlæggende principper jf. side 3 i denne orientering. Hvis det ikke er tilfældet skal processerne ændres eller ophøre helt. Det bør

ligeledes overvejes, om der er hjemmel i forordningen til at foretage den konkrete behandling. Hvis man er i tvivl om, om behandlingerne lever op til disse krav, bør man søge nærmere rådgivning herom.

Udarbejdelse af risikovurdering

Det er et krav, at der udarbejdes en risikovurdering med fokus på behandlingen af personoplysninger, for at afdække om data håndteres korrekt og forsvarligt. Risikovurderingen har til formål at undersøge hvad risikoen er for, at personoplysningerne hændeligt eller ulovligt tilintetgøres, fortabes eller forringes, samt kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med loven.

Start med en overordnet vurdering af de risici, der er forbundet med havnens behandling af personoplysninger og brug af informationsteknologi.

En risikovurdering bør bl.a. indeholde følgende overvejelser:

- Hvilke risici er der ved behandlingen af personoplysningerne ud fra deres kategorisering (almindelige vs. følsomme), og hvad er de mulige konsekvenser, både fysisk og moralsk, samt hvor stor er sandsynligheden for, at et sikkerhedsbrud kan opstå?
- Hvordan kan disse risici overvåges og kontrolleres – hvilke foranstaltninger er nødvendige for at imødegå risici?
- Hvordan kan havnen løbende evaluere, om foranstaltningerne er effektive, og om der er nye risici, der skal tages i betragtning?

Eksempler på risicielementer kan være:

- tekniske fejl: fejl i udstyr, overbelastning, softwarefejl, manglende vedligeholdelse
- fysisk skade: brand, vandskade, ødelæggelse af udstyr, større ulykker
- naturkatastrofer: oversvømmelse, klimatiske fænomener
- forsyningssvigt: forsyningssvigt af el/internetforbindelse
- kompromittering af funktioner: brugerfejl pga. mangelfuld træning
- menneskelige handlinger: hackere, it-kriminelle, spionage – også fysisk ved uretmæssig adgang eller misbrug af adgang/rettigheder.

Risikovurderingen danner grundlaget for at sikre, at der er iværksat passende tekniske og organisatoriske sikkerhedstiltag for at beskytte personoplysninger.

Havnen bør gennemgå risikovurderingen regelmæssigt for at sikre, at foranstaltningerne afspejler de personoplysninger havnen ligger inde med og behandler, samt det aktuelle trusselsbillede.

Formen minder om den risikovurdering, havnen har lavet i forbindelse med ISPS godkendelse.

Hvis risikovurderingen viser, at behandlingen har (eller sandsynligvis har) en høj risiko i forhold til de registreredes rettigheder, skal der udarbejdes en såkaldt DPIA (på dansk "konsekvensanalyse vedrørende databeskyttelse"). Det vil efter vores vurdering sjældent være relevant for havne.

Udarbejdelse af sikkerhedsbeskrivelse

Når havnen kender sine risici, er næste skridt at indføre de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger. Der er ikke fastlagt specifikke bestemmelser for hvilke foranstaltninger, der skal tages i anvendelse, fordi trusselsbilledet og mulige teknologiske foranstaltninger konstant forandrer sig.

Udgangspunktet for etablering af foranstaltninger er i stedet, hvad risikovurderingen har afdækket og dermed hvad der på det grundlag skal til, for i passende omfang at sikre beskyttelse af personoplysninger.

Sikkerhedsbeskrivelsen skal omfatte både tekniske, fysiske og organisatoriske beskyttelseselementer.

Tekniske beskyttelseselementer

Beskyttelse mod ulovlig adgang og misbrug af data

Følgende kan anvendes til at beskytte havnens it-systemer mod ulovlig adgang eller misbrug af data:

- adgangskontrol (login og passwords) til it-systemer hvor personoplysninger opbevares eller behandles, fx lønsystem, e-mail på computer og smartphone. Adgang blokeres efter et antal mislykkede forsøg på login
- sikring af internetadgang via fx passwords til Wi-Fi eller intranet
- etablering og vedligeholdelse af en firewall, som f.eks. spærrer for adgang til suspekte hjemmesider
- ajourføring af servere og pc-arbejdspladser (også hjemmearbejdspladser) med sikkerhedsopdateringer, som sikrer mod ondsindet udnyttelse af sårbarheder i de anvendte programmer
- etablering af virusværn, som løbende holdes ajourført
- opsætning af sikkerhedsindstillingerne i browseren og evt. e-mailprogram på de enkelte pc-arbejdspladser sådan, at der opnås den ønskede sikkerhed omkring websteder, cookies og plug-ins m.v.
- logning af adgang til personoplysninger – hvem tilgår oplysningerne og hvornår

- kryptering - hvis der behandles følsomme personoplysninger.

Beskyttelse mod tab eller beskadigelse af data
Havnen bør sikre, at personoplysninger ikke fortabes, beskadiges eller ændres utilsigtet. Et tiltag kan være at sikre, at der tages nødvendig backup af personoplysninger.

Fysiske beskyttelseselementer

Uretmæssig adgang til havnekontor/administration
Havnen bør sikre, at der er værn mod ulovlig indtrængen til kontoret, så både computere og fysiske papirversioner er opbevaret aflåst.

Makulering eller destruktion
Når fysiske dokumenter med personoplysninger skal bortskaffes, anbefales det at makulere eller foretage en anden form for destruktion.

Eksterne medier
Havnen bør begrænse opbevaring af personoplysninger på eksterne medier – fx USB-stik.

Organisatoriske beskyttelseselementer

Begrænset adgang
Adgang til personoplysninger begrænses, så der kun er adgang for dem der har et sagligt behov (så få som muligt).

Instruktion og uddannelse
Medarbejdere med adgang til persondata skal instrueres i korrekt håndtering af persondata. Der bør udarbejdes skriftlige instrukser til de forskellige personaletyper. For nogle havne vil det være tilstrækkeligt at lade instruksen indgå som en del af den interne persondatapolitik – se nærmere nedenfor under "Orientering af de registrerede". På den ene eller anden måde bør det sikres, at de medarbejdere der behandler personoplysninger, er uddannet korrekt i deres ansvar i forhold til at sikre overholdelse af havnens persondatapolitik.

Orientering af de registrerede

IT- og e-mailpolitik til medarbejdere som de registrerede
Hvis havnen sikkerhedskopierer medarbejdernes e-mail for at sikre drift og mulighed for genetablering, eller på anden måde udfører kontrol af medarbejdernes brug af e-mail, skal medarbejderne orienteres om det. Det samme gælder, hvis havnen logger eller kontrollerer medarbejdernes brug af internettet. Også i det tilfælde skal det klart og utvetydigt fremgå, at oplysningerne eventuelt vil blive gennemset ved mistanke om misbrug af

internet eller e-mail. Bemærk at i en sådan situation må havnen ikke læse private e-mails. Orientering kan finde sted ved, at udarbejde en IT- og e-mailpolitik målrettet medarbejderne.

Intern persondatapolitik
Havnen bør ligeledes udarbejde en intern persondatapolitik hvori medarbejderne, orienteres om hvilke personoplysninger der behandles og hvorfor, hvem der har afgang (så få som muligt), procedurer for sletning samt en beskrivelse af medarbejderenes rettigheder, ret til indsigelse, berigtigelse, sletning osv.

Andre orienteringer
Havne vil også kunne behandle persondata om andre end sine ansatte. Det gælder fx hvor havnen udfører adgangskontrol, eller hvis havnen indgår aftaler med enkeltmandsvirksomheder. Disse personer skal ligeledes orienteres om behandlingen og de rettigheder de har mv. Orienteringen bør ske skriftligt – fx i forbindelse med udlevering af adgangskort, eller ved fremsendelse af ordrebekræftelse eller lignende.

Orienteringspligten gælder også i forhold til fx ansøgere til en stilling i havnen – både ansøgninger der indgives på baggrund af stillingsopslag og uopfordrede ansøgninger. For nogle havne vil det være relevant at lave et standardsvar, der kan bruges i forbindelse med rekrutteringsprocesser, således at alle ansøgere får klar besked, om hvilken behandling havnen foretager mv.

Andre væsentlige regler

Pligt til rapportering af brud på datasikkerheden

Hvis havnen oplever et brud på datasikkerheden, hvor der er risiko for, at personoplysninger er blevet kompromitterede, skal havnen underrette Datatilsynet og de personer, hvis oplysninger er blevet kompromitterede om bruddet.

Konkret vil underretningen skulle foretages senest 72 timer efter, at havnen er blevet bekendt med, at personoplysningerne er blevet kompromitterede, og de berørte personer skal underrettes uden ugrundet ophold.

I praksis vil havnen derfor med fordel kunne udarbejde en plan for, hvordan man skal håndtere et brud på datasikkerheden, sådan at der er klare retningslinjer for, hvordan havnens medarbejdere skal agere i situationen.

Indgåelse af it-, outsourcing- og cloudaftaler

Hvis havnen har valgt at lade dele af it-driften outsource, vil det ofte også betyde, at personoplysninger behandles af en ekstern it-leverandør. Det kan eksempelvis være ved anvendelse af mailtjenester, webhosting eller ved helt eller delvis outsourcing af havnens it-drift.

Havnen er forpligtet til at sikre, at den behandling af personoplysninger, der foretages af eksterne it-leverandører, er i overensstemmelse med forordningens regler og kun sker efter instruks fra havnen. Det betyder i praksis, at der skal indgås en databehandleraftale mellem havnen og it-leverandøren. Det kan enten ske i form af en selvstændig aftale eller indeholdt som et afsnit i serviceaftalen/leveranceaftalen mellem havnen og it-leverandøren.

Databehandleraftale ved it-, outsourcing- og cloud-aftaler
Ofte vil databehandleraftaler skulle opdateres for at leve op til de nye krav. Det skal af databehandleraftalen bl.a. tydeligt fremgå, at it-leverandøren er underlagt samme regelsæt for behandling af personoplysninger som havnen, og at it-leverandøren kun foretager behandling af personoplysningerne på instruks fra havnen.

Det er havnens ansvar som dataansvarlig, at databehandleraftalerne lever op til forordningens krav. Det vil derfor for mange være en god ide at søge nærmere rådgivning herom.

Indsamling af cookies på havnens hjemmeside

Cookies indgår som en integreret del af de fleste hjemmesideløsninger. En cookie er en lille tekstfil, som lagres på brugerens elektroniske udstyr og som muliggør genkendelse af brugeren og indsamling af data om vedkommendes adfærd på hjemmesiden. Data indsamlet fra cookies vil derfor også som udgangspunkt være personoplysninger. Hvis der indsamles cookies på havnens hjemmeside kræves det, at brugeren af hjemmesiden skal acceptere, at der placeres cookies på brugerens computer, smartphone mv. Udover at cookies skal behandles som personoplysninger ifølge persondata-forordningen, er området også reguleret af cookiebekendtgørelsen. Erhvervsstyrelsen har udarbejdet en vejledning om cookies med eksempler på tekst til indhentning af samtykke[1].

[1] Link til Erhvervsstyrelsens vejledning til cookiebekendtgørelsen:
https://erhvervsstyrelsen.dk/lovgivning-og-vejledning-til-cookiebekendtgoerelsen

Tv-overvågning på havnens område

Tv-overvågning af havnen finder ofte sted i forbindelse med havnesikring eller havnefacilitetssikring. Ifølge lov om tv-overvågning skal havnen tydeligt skilte med, at der foretages tv-overvågning. Persondataforordningens regler gælder i forhold til behandlingen af de personoplysninger, der indsamles som følge af tv-overvågningen. Med mindre havnen er forpligtet til at videregive optagelser i henhold til anden lovgivning, er det kun lovligt at videregive optagelser, hvis:

- den person, der optræder på optagelserne, har givet sit samtykke til videregivelsen
- videregivelsen sker til politiet i kriminalitetsopklarende øjemed.

Hvis ikke andet er angivet i havnens havnesikringsplan (PSP) eller havnefacilitetssikringsplan (PFSP) skal optagelser som udgangspunkt slettes senest 30 dage efter, at de er foretaget. Optagelserne kan opbevares længere, hvis det er nødvendigt for behandlingen af en konkret tvist. I så fald skal havnen som udgangspunkt underrette den, som tvisten vedrører, og på anmodning udlevere en kopi af optagelsen.

Hvor længe må personoplysninger gemmes?

De personoplysninger havnen indsamler, må ikke opbevares længere end det der er nødvendigt til de formål som personoplysningerne er indsamlet til. Bortset fra tv-overvågning, er der ingen absolut tidsafgrænsning af, hvor længe oplysningerne må opbevares. Men det gælder for opbevaring af alle typer af personoplysninger, at de aldrig må opbevares i længere tid, end hvad der er nødvendigt i forhold til det formål oplysningerne oprindeligt blev indsamlet til. Havnen kan i medfør af havnesikringsplan eller havnefacilitetssikringsplan have særlige forpligtelser til at opbevare personoplysningerne i en længere periode, eller under særlige vilkår, som i så fald skal følges.

Den videre proces

Danske Havne opfordrer til, at arbejdet med at kortlægge datastrømme og udarbejde behandlingsoversigter påbegyndes snarest, navnlig i de havne der hidtil kun i begrænset omfang har beskæftiget sig med persondatabeskyttelse og de tilknyttede regler.

Datatilsynet udsteder i løbet af de næste par måneder vejledninger, der vil præcisere og uddybe lovgivningen. Danske Havne opretter i den forbindelse et persondatanetværk med henblik på at understøtte det videre arbejde med

persondatalovgivningen. I netværket vil der løbende komme opdateringer om persondataforordningen og den danske fortolkning af reglerne.

For at tilmelde sig persondatanetværket, kontakt da Eva Fiil Nielsen, PA/Policy Advisor i Danske Havne på efn@danskehavne.dk eller tlf. 6171 0706.