PERSONDATAPOLITIK
For Museum Sydfyn

Museum Sydfyn definerer sig selv som dataansvarlig som institution og dets medarbejdere og ansatte som databehandlere. Eksterne IT-platformssamarbejdspartnere anses ligeledes som værende databehandlere. Museets persondatapolitik er udarbejdet med baggrund i Databeskyttelsesforordningen[1] samt Datatilsynets officielle vejledninger i reglerne om databeskyttelse[2] og Lokalarkivers behandling af personoplysninger.[3]

Instruktion

Medarbejdere der skal håndtere personoplysninger, modtager ved ansættelse instruktion i museets persondatapolitik, og oplæring i hvad de må gøre med oplysningerne, og hvordan de skal beskytte oplysningerne.

Indsamling og opbevaring af personoplysninger

Der indsamles kun de nødvendige oplysninger i forbindelse med museets administration, forskning, indsamling og formidling. Skulle andre oplysninger blive kendt, destrueres de straks. Al indsamlet data bliver behandlet fortroligt, og opbevares sikkert. Borgerens personlige oplysninger opbevares på museets sikrede netværk og er underlagt vores IT-retningslinjer (se IT-sikkerhed), der sikrer borgerens rettigheder og overholdelse af gældende lovgivning på området. Elektroniske oplysninger beskyttes med firewall og password. Papirdokumenter og fotos opbevares aflåst i skab eller i lokaler med begrænset adgang. Kun personer, for hvem det er nødvendigt for udførelsen af deres arbejde, har eller kan få adgang til personfølsomme oplysninger. Vi deler aldrig indsamlede oplysninger med tredjepart, med mindre det på forhånd er aftalt med borgeren.

Ansøgninger til opslåede stillinger gemmes kun fra den person der ansættes. Alle andre ansøgninger slettes, med mindre andet aftales med ansøger. Ansatte, der deltager i ansættelsesudvalg / samtaler må ikke gemme ansøgninger eller bilag hertil efter ansættelse. Dette gælder også i elektronisk form. Ved uopfordrede ansøgninger sendes kvittering for modtagelsen, hvoraf det fremgår, at ansøgningen ikke gemmes, medmindre andet aftales skrifteligt.

Lønbehandling sker ved Danløn udelukkende med brugernavn og adgangskode. Alle bilag vedr. løn gemmes i 5 år, hvorefter de destrueres. Indeværende og foregående års materiale opbevares i aflåst skab på kontoret. Øvrige i aflåst rum på fjernarkivet. Lønrefusioner mm. behandles via de statslige systemer Nemrefusion og Fleksbarsel, der tilgås via NemID.

Bogføringen sker via det hostede system Economic. Kun regnskabsfører og personaleansvarlig

[1]https://eur-lex.europa.eu/legal-content/DA/TXT/PDF/?uri=CELEX:32016R0679&from=DA
[2]https://www.datatilsynet.dk/hvad-siger-reglerne/vejledning/vejledninger-i-pdf-format
[3]https://www.datatilsynet.dk/Media/638034275844404942/Retningslinjer%20for%20lokalarkivers%20behandling%20af%20personoplysninger.pdf

har adgang til dette, som er beskyttet via adgangskode. Bilag scannes til Economic. Fysiske bilag med personfølsomme oplysninger destrueres efter scanning. Indeværende og foregående års materiale opbevares i aflåst skab på regnskabskontoret, øvrige i aflåst rum på fjernarkivet.

Den online administrationsdatabase er sikret gennem udbyderen, som har erklæret sitet for GDPR kompatibelt jvf. email af 10/4/18. Se i øvrigt link: https://www.foreningsadministrator.dk/compliance Ved indmelding oplyses medlemmet skriftligt om Museets datasikkerhedspolitik, og dennes accept opbevares skriftligt under lås.

Personoplysninger indsamlet i forbindelse med museets forskning, indsamling og formidling (genstande/fotos/vidnesbyrd), vil indgå i museets arkivsystem. Ved genstandsregistreringer indsamler vi kun de personoplysninger, der er nødvendige for at sikre proveniens og efterfølgende kontakt med borgeren. Personoplysninger indsamlet i forbindelse med forskning og formidling, beror på informeret samtykke og opbevares så længe det er aftalt mellem parterne. Der er udarbejdet blanketter til informeret samtykke, der skal benyttes ved indsamling af vidnesbyrd mm. Vi sørger for at slette personoplysninger, når de ikke længere er relevante for det formål, vi har indsamlet dem til, eller når borgerens samtykke ophører. Alle kontaktoplysninger opbevares dog i minimum fem år, for at kunne sikre en efterfølgende kontakt ved tvivlsspørgsmål mm.

Sletning og berigtigelse

Borgeren kan til enhver tid få oplyst, hvilke oplysninger vi har registreret om dem, og bede om at få slettet eller berigtiget sine data. Såfremt borgeren ønsker dette, bedes de kontakte museets administration. Hvis borgeren har spørgsmål eller kommentarer til vores datapolitik, eller til hvordan vi bruger deres personoplysninger, bedes de kontakte museets administration.

Efter fratrædelse af medarbejdere opbevares den underskrevne kontrakt i 20 år. Andet materiale, der kan være brugbart i forbindelse med evt. tvister, gemmes i 5 år, mens alt andet destrueres.

Alt papiraffald fra kontorerne makuleres ved afhentning af Svendborg Kommune, eller løbende på museets egen makuleringsmaskine.

Borgeren har ret til at indgive en klage til Datatilsynet, hvis de er utilfreds med den måde, vi behandler deres personoplysninger på. Datatilsynets kontaktoplysninger findes på www.datatilsynet.dk.

Databehandleraftaler

Der udarbejdes databehandleraftaler med eksterne databehandlere (hjemmesider etc.), og disse opbevares sammen med museets persondatapolitik. Databehandleraftaler udarbejdes med udgangspunkt i Datatilsynets skabelon.[4]

[4] https://www.datatilsynet.dk/hvad-siger-reglerne/vejledning

Nyhedsbreve

Til-og afmelding af nyhedsbrev er frivilligt, og håndteres af borgeren selv. Nyhedsbreve vil kun blive benyttet til det formål, som borgeren har givet samtykke til. Borgeren kan altid kontakte museets administration, hvis de ønsker at blive afmeldt igen.

IT-sikkerhed

Det er kun Museums Sydfyns faglige medarbejdere, der har adgang til de netværk, hvor data er arkiveret. Adgang hertil forudsætter personligt log-in. Computerne er indstillet til at låse efter et bestemt tidsrum, hvor tastaturet ikke er benyttet, og generelt anmodes medarbejderne om at låse computeren, når den forlades, således at uvedkommende ikke har adgang til digitale data

10 retningslinjer for museets medarbejdere

1. **IT-sikkerhed er dit ansvar!**

   Museum Sydfyn håndterer fortrolige oplysninger om både egne medarbejdere, borger og virksomheder. Derfor har du som medarbejder ansvaret for, at de oplysninger, du arbejder med, ikke ender som brud på IT-sikkerheden. Derfor er det vigtigt, at vi håndterer oplysninger forsvarligt og er ansvarlige i vores adfærd både på internettet, i mails og sågar når vi forlader vores skrivebord.

   2. Del ikke din adgangskode

   Dit brugernavn er din personlige identifikation og samtidig autorisation til rettigheder. Det samme gælder adgangskoder. Du har ansvaret for eventuelt misbrug, hvis du deler dit brugernavn og adgangskoder.

   3. Vælg stærke adgangskoder

   Det er vigtigt, at du vælger en stærk adgangskode, der er svær at gætte eller hacke. Derfor må du aldrig vælge adgangskoder, der for eksempel tager udgangspunkt i årstiden, dit barns eller kæledyrs navn eller fødselsdato.

   For at lave en stærk adgangskode, kan du gøre koden lang; jo længere, jo højere sikkerhed. Du bør kombinere tal, store og små bogstaver og undlade at bruge æ, ø eller å. Husk at bruge forskellige koder til forskellige systemer og at du ikke må genbruge dine koder.

   4. Brug din mobile enhed sikkert

   Det er dit ansvar, at sikkerheden på dine mobile enheder, så som smartphones og tablets, bliver overholdt. Derfor skal du sørge for, at der ikke andre end dig selv, der har adgang til enheden. Der skal være både skærmlås (pinkode) og simlås (pinkode) på enheden og den skal være låst, når den er udenfor dit opsyn. Du må aldrig opbevare følsomme og fortrolige oplysninger på dine mobile enheder.

5. Adskil privat og arbejdsmæssig brug af mail

Bruger du din arbejdsmail privat, kan der være situationer, hvor modtageren kan komme i tvivl om, hvem du er som afsender – myndighed eller privatperson. Det er ikke forbudt at bruge din arbejdsmail til private anliggender i begrænset omfang – blot du husker at fjerne din signatur. Men som udgangspunkt bør du have en privat mail til korrespondancer, hvor der kan opstå tvivl. Mangler du en alternativ mailadresse, kan du oprette en gratis på hotmail.com eller gmail.com.

6. Lås din computer, når du forlader den

Med tasterne ”Windows”+”L” kan du hurtigt låse din computer. Som medarbejdere sidder vi mange forskellige steder i organisationen. Nogle steder er der nemmere adgang for uvedkommende end andre. Din computer låser først af sig selv efter 20 min. Gør det derfor til en vane at låse den, når du forlader kontoret. Tryk ”Windows” tasten (den med det lille flag) og ”L” samtidig.

Efterlader du den ulåst, har du åbnet op for misbrug i dit navn. Du bærer også ansvaret her.

7. Ryd op på dit skrivebord og brug fortroligt print

Vær opmærksom på ikke at efterlade dokumenter personfølsomme eller fortrolige oplysninger.

Du risikerer, oplysningerne kan havne i de forkerte hænder eller bliver læst af uvedkommende. Det er også dit ansvar. Sørg derfor altid for at have et ryddet skrivebord, når du forlader det.

Du kender det sikkert; du har hentet dine dokumenter ved printeren, og når du så gennemgår dem, har du også fået din kollegas dokumenter med. Også selvom du lavede en hurtig sortering, inden du forlod printeren. Derfor er fortroligt print en god ting. Du er nemlig ansvarlig for, hvad du printer og at dette ikke kommer i andres hænder. Du kan gøre fortroligt print til standard via printerindstillingerne eller bruge det fra gang til gang ved at vælge det i udskriftsfeltet.

8. Gem og send fortrolige dokumenter sikkert

Vi kan dele og lagre informationer på mange måder i dag. Både på nettet, netværksdrev og usb-lagerenheder. Problemet er, at mange af disse gratis tjenester ikke lever op til Datatilsynets strenge krav til datasikkerhed.

Alle personfølsomme og fortrolige oplysninger skal både opbevares og sendes sikkert. Det betyder, at disse oplysninger som udgangspunkt skal opbevares i ESDH-systemet SBSYS med begrænsning på hvem der kan tilgå sagen og sendes via Digital Post. Dette gælder også CPR numre, som aldrig må sendes via almindelig ubeskyttede mail eller opbevares usikkert.

Hvis du bruger netværksdrev må oplysningerne kun være tilgængelige for relevante medarbejdere. Du må ikke opbevare personfølsomme eller fortrolige oplysninger på din private computer eller på en flytbar lagringsenhed.

9. Vær forsigtig på internettet og i mails

Du er beskyttet til en vis grænse af vores it-sikkerhedsforanstaltninger, men meget afhænger af din adfærd.

Spørger hjemmesider, om de skal gemme dit brugernavn og password, så vurder altid nøje, om det er nødvendigt. Der er altid en sikkerhedsrisiko ved at gemme personlige oplysninger på hjemmesider.

Hvis du får en uopfordret mail fra en afsender, du normalt ikke mailer med, skal du være på vagt og vær forsigtig med at trykke på links til hjemmesider. Overvej grundigt afsenderens troværdighed, læs indholdet med kritiske øjne og vurder så, om du bør trykke på linket.

10. Overvej, hvad du skriver på sociale medier

Vær opmærksom på brug af sociale medier, og de signaler du sender her. Grænserne mellem privatsfæren og arbejdslivet bliver mere flydende, jo mere vi færdes på sociale medier - specielt i situationer, hvor du nogle gange repræsenterer Museum Sydfyn og andre gange er privatperson.

Procedure ved brud

I tilfælde af brud på nærværende persondatapolitik og -procedure vil en undersøgelse af hændelsesforløbet finde sted og en analytisk rapport blive udarbejdet. Rapportens konklusion vil ligge til grund for en øjeblikkelig afhjælpning og afgrænsning af bruddet samt udarbejdelse af forholdsregler fremover. Inden for 72 timer vil bruddet blive anmeldt til Datatilsynet, hvor der oplyses om følgende:

1. Sikkerhedsbruddets karakter
2. Konsekvenser
3. Begrænsning af bruddet
4. Dataansvarliges kontaktinformationer
5. Dataproceduredokumenter

En formular til udfyldelse af hændelsesforløbet er udarbejdet.