THE DANISH INSTITUTE FOR HUMAN RIGHTS

REDEGØRELSEN VEDR. BERETNING NR. 1/2014 OM STATENS BEHANDLING AF FORTROLIGE OPLYSNINGER OM PERSONER OG VIRKSOMHEDER

12 JANUARY 2015

1) Indledning

Institut for Menneskerettigheder (IMR) har i det følgende kort sammenfattet de overvejelser og sikkerhedsforanstaltninger, som beretning nr. 1/2014 har givet anledning til.

IT har i november og december 2014 udarbejdet en handlingsplan, som skal sikre, at IMR følger de gældende retningslinjer for statens behandling af fortrolige personoplysninger[1]. Handlingsplanen er sammen med en ny politik for informationssikkerhed blevet forelagt for direktionen i december. Direktionen godkendte handlingsplanen i december, mendens den nye politik for informationssikkerhed er blevet godkendt d. 12 januar 2015. De planlagte sikkerhedsforanstaltninger vil blive gennemført inden udgangen af 1. kvartal 2015.

Ved udarbejdelsen af politikken for informationssikkerhed har IT taget udgangspunkt i de gældende ISO-standarder og de aktuelle vejledninger og værktøjer, som Digitaliseringsstyrelsen har udarbejdet og publiceret på deres hjemmeside[2].

2) Overvejelser

Med den nye ISO-standard indføres et ISMS[3] (Information Security Management System). ISMS er en metode som omfatter de relevante politikker, procedurer og kontroller for Informationssikkerhedsstyring m.v. Med udgangspunkt i en grundig risikovurdering udpeges de nødvendige og relevante sikringsforanstaltninger for Instituttet. Som en del af risikohåndtering vil Instituttet udarbejde et Statement of Applicability (SoA), som beskriver hvordan retningslinjerne fra ISO-standarden er implementeret ud fra princippet "*Comply or Explain*".

Instituttet vil etablere et IT-sikkerhedsudvalg med repræsentanter fra ledelsen, IT og de udvalgte afdelinger, som anvender personfølsomme oplysninger i

[1] De gældende retningslinjer fremgår af sikkerhedsbekendtgørelsen BEK 528, som er udarbejdet i tilknytning til Lov om behandling af personoplysninger – (LOV nr. 429).
[2] Link til Digitaliseringsstyrelsens hjemmeside: http://www.digst.dk/Arkitektur-og-standarder/Styring-af-informations-sikkerhed-efter-ISO-27001.aspx
[3] ISO27001 stiller krav om, at en række styringsaktiviteter er til stede for at kunne lykkes med styringen af informationssikkerhed. Når der i en organisation er skabt et samspil mellem styringsaktiviteterne, er det i realiteten udtryk for, at der er implementeret et ISMS. Reference til Digitaliseringsstyrelsens vejledning i informationssikkerhedsstyring (ISMS), som er udgivet i marts måned 2013.

deres daglige arbejde med forskning, konsulentopgaver m.v. Der vil blive udarbejdet en årsplan for IT-sikkerhedsudvalgets arbejde, der skal sikre et fagligt kvalificeret og kontinuert tilsyn med, at de gældende regler i persondataloven og sikkerheds bekendtgørelsen vil blive overholdt.
ekendtgørelsen vil blive overholdt.

3) Foranstaltninger

Handlingsplanen indeholder en komplet beskrivelse af de sikkerhedsforanstaltninger, som IMR har valgt at implementere på baggrund af resultaterne fra den gennemførte IT-revision i foråret 2014. Ved udarbejdelsen af handlingsplanen har IT foretaget en systematisk vurdering af de specifikke resultater, som fremgår af beretningen og det revisonsnotat, som Rigsrevisionen har udarbejdet til IMR.

Der er i nedenstående tabel 1 foretaget en opsummering af de sikkerhedsforanstaltninger, som Instituttet har besluttet at iværksætte i relation til de udvalgte spørgsmål fra bilag 2 i beretningen fra Rigsrevisionen.

Tabel 1: Undersøgelsens resultater og de planlagte initiativer i Institut for Menneskerettigheder:

Nr.	**De udvalgte spørgsmål fra bilag 2**	**Resultat**	**Planlagte sikkerhedsforanstaltninger i IMR**
1)	Er der retningslinjer for at sikre person-oplysninger?	●	Institut for Menneskerettigheder har vedlagt en ny politik for informationssikkerhed, som er blevet godkendt af direktionen
2)	Er retningslinjerne opdateret årligt?	●	IT-sikkerhedsudvalget vil mindst en gang årligt foretage en kontrol og eventuel opdatering af retningslinjerne, så de er fyldestgørende.
3)	Kontrolleres brugeradgange halvårligt?	●	I forbindelse med implementeringen af den nye politik vil der blive indført en ny procedure for kontrol af brugerrettigheder hvert halve år.
4)	Registreres afviste adgangsforsøg?	●	*Ikke yderligere sikkerhedsforanstaltninger*
5)	Følges der op på afviste adgangsforsøg?	●	*Ikke yderligere sikkerhedsforanstaltninger*

6)	Registreres medarbejdernes opslag på enkeltpersoner?	●	Der vil fremover blive foretaget en logning af opslag på enkeltpersoner i de anvendte fagsystemer og ESDH m.v.
7)	Slettes logregistreringerne?	●	IMR vil senest efter 6 måneder foretage en sletning af logfilerne efter der er foretaget den foreskrevne kontrol af oplysningerne.
8)	Er der en aftale med databehandleren?	IR	*Ikke relevant (IR)*
9)	Følges der op på databehandleraftalen?	IR	*Ikke relevant (IR)*
10)	Er der retningslinjer for tilsyn?	●	Retningslinjerne for kontrol og tilsyn med informationssikkerheden er udarbejdet i henhold til de gældende anbefalinger i ISO-standarden.
11)	Føres der tilsyn med sikkerheds-foranstaltningerne?	●	IMR vil fremadrettet foretage en regelmæssig kontrol og tilsyn i henhold til de vedtagne sikkerheds-foranstaltninger for Instituttet.