MINISTERIET FOR BØRN, LIGESTILLING, INTEGRATION OG SOCIALE FORHOLD

Dato: 20. januar 2015

Statsrevisorernes Sekretariat
Christiansborg
1240 København K

Sagsnr. 2014-4002

**Ministeren for børn, ligestilling, integration og sociale forholds redegørelse til beretning nr. 01/2014 om statens behandling af fortrolige oplysninger om personer og virksomheder**

Som anmodet i brev af 20. november 2014 ref. 14-000917-16 fremsendes hermed min redegørelse for de foranstaltninger og overvejelser, som er afledt af statsrevisorernes beretning nr. 01/2014 om statens behandling af fortrolige oplysninger om personer og virksomheder.

Som borger i vores samfund og bruger af de offentlige myndigheders forskellige sociale tilbud har man krav på, at de personlige oplysninger, som registreres elektronisk, opbevares fortroligt og forsvarligt. Det er vigtigt for den sociale indsats, at man som borger eller virksomhed kan henvende sig til offentlige institutioner i tillid til, at informationssikkerheden lever op til gældende standard. Rigsrevisionen har derfor med denne beretning sat fokus på et vigtigt område.

Rigsrevisionen finder overordnet set ikke myndighedernes indsats overfor at beskytte fortrolige oplysninger om borgere og virksomheder tilfredsstillende. Rigsrevisionen har i den sammenhæng konstateret, at Socialstyrelsen i forhold til Stofmisbrugsdatabasen og projektstyringsværktøjet Project Flow ikke har levet op til en række af de krav, som er fastsat i Sikkerhedsbekendtgørelsen (BEK nr. 528 af 15.06.2000).

*Rigsrevisionsrapporten pkt. 13: Sikkerhedsbekendtgørelsen*
Rigsrevisionen har gennemgået de interne retningslinjer, instrukser, sikkerhedshåndbøger mv., som institutionerne har udarbejdet mhp at opfylde sikkerhedsbekendtgørelsens bestemmelser. Rigsrevisionen bemærker, at retningslinjerne for adgangsstyring ikke er opdateret, og Socialstyrelsen kritiseres specifikt for at mangle retningslinjer for distancearbejdspladser.

Et nyt sæt retningslinjer for distancearbejde (politik for mobil arbejdsplads og e-mail politik), er udarbejdet med afsæt i sikkerhedsbekendtgørelsen og er behandlet i Socialstyrelsens interne sikkerhedsstyregruppe d. 22. september 2014 og efterfølgende i Socialstyrelsens chefgruppe d. 4. november 2014. Politikkerne er under færdiggørelse med afsæt i den hidtidige sagsbehandling. Retningslinjerne bliver implementeret i Stofmisbrugsdatabasen, så snart Socialstyrelsens Informationssikkerhedsstyregruppe har godkendt den reviderede udgave i 1. kvartal 2015.

*Rigsrevisionsrapporten pkt. 15: Kontrol af medarbejdere*
Rigsrevisionen har gennemgået kontrollen af medarbejdernes adgang til fortrolige personoplysninger og konstaterer, at Socialstyrelsen har defineret,

hvilke brugere der må have adgang og har godkendt de pågældendes autorisationer. Det bemærkes, at Socialstyrelsen ikke har udført en halvårlig kontrol.

Socialstyrelsen har oplyst, at de i december 2014 har gennemført en brugergennemgang af medarbejdernes adgang til Stofmisbrugsdatabasen. En halvårlig revision af adgange og brugerrettigheder er fremadrettet blevet indarbejdet i det såkaldte Årshjul for Stofmisbrugsdatabasen, og der er lavet konkrete kalenderaftaler for relevante medarbejderes opfølgning på dette. Opfølgningen dokumenteres til senere revisionsbrug.
Årshjulet er den plan, som sikrer, at alle systemer løbende gennemgås mht. brugerrettigheder, adgangskontrol, kontrol af logning, backupsikring, opdatering af risikovurdering mv. Årshjulet er godkendt af Socialstyrelsens informationssikkerhedsstyregruppe d. 22. september 2014.

*Rigsrevisionsrapporten pkt. 16: Adgang til fortrolige data*
Rigsrevisionen har gennemgået Socialstyrelsens kontrol af afviste forsøg på at få adgang til fortrolige personoplysninger. Rigsrevisionen bemærker, at Socialstyrelsen ikke har registreret de afviste adgangsforsøg.

Socialstyrelsen har på baggrund af Rigsrevisionens bemærkning udarbejdet en ændringsanmodning til applikationsleverandøren for Stofmisbrugsdatabasen med henblik på at systemet tilrettes, således at afviste forsøg på adgang registreres. Tilrettelsen bliver udført og implementeret inden udgangen af 1. kvartal 2015. Herefter udføres halvårlig gennemgang af loggen mhp at undersøge om der er uregelmæssige hændelser, indbrudsforsøg mv.

*Rigsrevisionsrapporten pkt. 17: Logning af opslag*
Institutionerne skal kunne spore, hvilke medarbejdere der har søgt på oplysningerne i systemerne. Derfor skal institutionerne registrere medarbejdernes opslag på enkeltpersoner. Det fremgår af Sikkerhedsbekendtgørelsens § 19, stk 1, at loggen skal opbevares i 6 mdr. hvorefter den skal slettes. Rigsrevisionen konstaterer, at Socialstyrelsen ikke har slettet oplysningerne igen.

På baggrund af Rigsrevisionens bemærkning har Socialstyrelsen rettet henvendelse til applikationsleverandøren for Stofmisbrugsdatabasen med henblik på, at systemet tilrettes, således at der foretages en automatiseret sletning af logfiler efter 6 måneder. Rettelsen bliver udført og implementeret inden udgangen af 1. kvartal 2015.

*Rigsrevisionsrapporten pkt. 19: Databehandleraftale*
Institutionerne skal som dataansvarlige indgå en skriftlig aftale om sikker behandling af fortrolige personoplysninger, hvis der er eksterne virksomheder, der behandler oplysningerne på vegne af institutionen. Rigsrevisionen påpeger, at Socialstyrelsen ikke har indgået en skriftlig aftale med databehandlerne på Stofmisbrugsdatabasen. Fraværet af en sådan aftale betyder, at Socialstyrelsen

ikke har pålagt databehandleren instruktioner i forhold til at behandle fortrolige personoplysninger.

Endvidere påpeger Rigsrevisionen, at Socialstyrelsen på undersøgelsestidspunktet ikke havde indgået en skriftlig aftale med databehandlerne og dermed ikke har kunnet følge op på aftalens indhold. Socialstyrelsen har indhentet en generel revisorerklæring, som ikke er specifikt rettet mod sikkerhedsforanstaltninger i det undersøgte system. Rigsrevisionen har dog ikke vurderet dette som værende tilstrækkeligt.

Socialstyrelsen har oplyst, at der nu er indgået databehandleraftale med de relevante virksomheder.

*Rigsrevisionsrapporten pkt. 21: Tilsyn med sikkerhedsforanstaltningerne*
Institutionerne skal føre tilsyn med, at institutionens sikkerhedsforanstaltninger efterleves. Rigsrevisionen konstaterer, at Socialstyrelsen ikke har retningslinjer for, hvordan eget tilsyn skal udføres, og derfor heller ikke har kunnet udføre et tilsyn i overensstemmelse med retningslinjerne.

Socialstyrelsen har oplyst, at en procesbeskrivelse for tilsyn er under udarbejdelse i forbindelse med Socialstyrelsens implementering af informationssikkerhedsstandarden ISO 27001, som omfatter Stofmisbrugsdatabasen. Processen for tilsynet er beskrevet i Årshjulet, jf tidligere omtale. I forbindelse med de løbende kontroller dokumenteres hvert enkelt tilsyn således, at der bliver fuld gennemsigtighed med Socialstyrelsens tilsyn og de tiltag, som løbende iværksættes for at sikre et forsvarligt højt sikkerhedsniveau.

*Rigsrevisionsrapporten pkt. 25: Virksomhedsoplysninger*
Socialstyrelsen har en forpligtelse til at beskytte fortrolige oplysninger om virksomheder, der indgår i de undersøgte systemer. Rigsrevisionen bemærker, at Socialstyrelsen ikke har opdaterede retningslinjer på det undersøgte område inden for det seneste år. Socialstyrelsen modtager en revisorerklæring[1], selv om styrelsen ikke har fastlagt detaljerne for revisorerklæringens indhold. Socialstyrelsen har ikke en opdateret risikovurdering for de undersøgte systemer.

Socialstyrelsen har oplyst, at de er ved at lægge sidste hånd på at opdatere retningslinjerne jf. ISO 27001 informationssikkerhedsstandarden. Disse retningslinjer gælder også det af Rigsrevisionen undersøgte projektstyringsværktøj og vil blive revideret årligt af Socialstyrelsens Informationssikkerhedsstyregruppe. Det er samme styregruppes ansvar at sørge for, at ændringer i Socialstyrelsens informationssikkerhedsstandard bliver efterlevet af de relevante systemer.

[1] Ledelsen i Dokumentation og Metode har indhentet en uvildig revisorerklæring for at sikre sikkerheden hos driftsleverandøren på tværs af alle de hostede løsninger. Rigsrevisionen mener ikke, at en generel erklæring er tilstrækkelig.

Der er i øvrigt siden Rigsrevisionens gennemgang i Socialstyrelsen indgået databehandleraftale med koncernens nye IT-drift leverandør, KMD/Itavis.

Yderligere kan jeg informere om, at Socialstyrelsen i september 2014 har udarbejdet en opdateret risikoprofil for dette projektstyringsværktøj, som er godkendt af Socialstyrelsens Informationssikkerhedsstyregruppe. Projektstyringsværktøjet indeholder ikke datafelter til at registrere kontaktoplysninger på medarbejdere i virksomhederne. Der registreres ingen fortrolige oplysninger om virksomhederne i systemet.

Ministeriet, og herunder Socialstyrelsen, har taget Rigsrevisionens konklusioner og anbefalinger til efterretning og vil arbejde videre med styrkelse af informationssikkerhedsniveauet i forhold til disse både for Stofmisbrugsdatabasen og projektstyringsværktøjet, men også for de øvrige systemer i Socialstyrelsen.

Jeg har ikke yderligere bemærkninger til statsrevisorernes beretning.

Der er ved fremsendelsen af dette brev sendt en kopi til rigsrevisor, St. Kongensgade 45, 4. sal, 1264 København K.

Med venlig hilsen

*Manu Sareen*