Statsrevisorerne 2014-15 (1. samling)
Beretning nr. 1 Rigsrevisionens notat af 17. februar 2015
Offentligt

RIGSREVISIONEN

Notat til Statsrevisorerne om beretning om statens behandling af fortrolige oplysninger om personer og virksomheder

Februar 2015

Vedrører:
Statsrevisorernes beretning nr. 1/2014 om statens behandling af fortrolige oplysninger om personer og virksomheder

17. februar 2015

RN 1402/15

Forsvarsministerens redegørelse af 9. januar 2015
Beskæftigelsesministerens redegørelse af 13. januar 2015
Udenrigsministerens redegørelse af 15. januar 2015
Skatteministerens redegørelse af 20. januar 2015
Justitsministerens redegørelse af 20. januar 2015
Økonomi- og indenrigsministerens redegørelse af 20. januar 2015
Ministeren for sundhed og forebyggelses redegørelse af 20. januar 2015
Ministeren for børn, ligestilling, integration og sociale forholds redegørelse af 20. januar 2015

1. Dette notat handler om de initiativer, som ministrene har iværksat og vil iværksætte som følge af Statsrevisorernes bemærkninger og beretningens indhold og konklusioner.

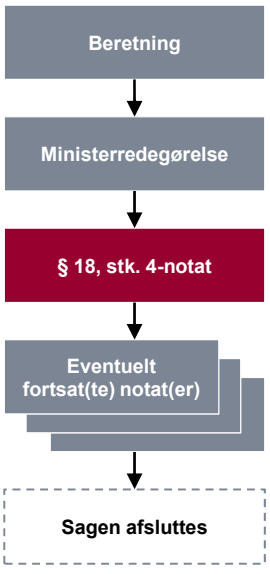
KONKLUSION

Ministrene har oplyst, at institutionerne har taget en række initiativer til at sikre, at sikkerhedsbekendtgørelsen efterleves, og til at styrke sikkerheden omkring behandling af fortrolige oplysninger om personer og virksomheder. Rigsrevisionen finder initiativerne tilfredsstillende og vurderer, at sagen kan afsluttes. Rigsrevisionen vil i forbindelse med it-revisionen fortsat følge, at initiativerne bliver implementeret og fungerer i praksis.

Rigsrevisionen baserer konklusionen på følgende:

- Institutionerne har udarbejdet retningslinjer om sikkerhedsforanstaltninger, og de har tilkendegivet, at retningslinjerne fremover vil blive opdateret.
- Institutionerne har igangsat eller vil igangsætte initiativer til at udføre en halvårlig kontrol af brugernes adgange i de undersøgte systemer.
- Institutionerne har taget initiativ til at registrere afviste forsøg på at få adgang til systemerne og til, at der efterfølgende følges op på de afviste forsøg.
- Institutionerne har taget initiativ til at registrere medarbejdernes opslag på enkeltpersoner og til at slette registreringerne igen efter ½ år eller efter en eventuel udvidet periodes afslutning.

Sagsforløb for en større undersøgelse



Du kan læse mere om forløbet og de enkelte step på www.rigsrevisionen.dk

- Institutionerne har indgået skriftlige aftaler med databehandlerne og har iværksat eller vil iværksætte initiativer til at følge op på de indgåede aftaler.
- Institutionerne har udarbejdet eller er i gang med at udarbejde retningslinjer for eget tilsyn med sikkerhedsforanstaltninger.
- Institutionerne har opdateret risikovurderingen for de undersøgte systemer, der indeholder fortrolige virksomhedsoplysninger.

I. Baggrund

2. Rigsrevisionen afgav i november 2014 en beretning om statens behandling af fortrolige oplysninger om personer og virksomheder. Beretningen handlede om, hvordan 8 udvalgte institutioner behandlede fortrolige oplysninger om personer og virksomheder i 11 udvalgte it-systemer. Beretningen viste, at institutionerne ikke beskyttede fortrolige oplysninger tilstrækkeligt. Ingen af de undersøgte institutioner efterlevede alle de krav til behandling af fortrolige personoplysninger, som fremgår af sikkerhedsbekendtgørelsen, og som er en uddybning af persondatalovens bestemmelser. Endvidere burde institutionerne forbedre sikkerheden for fortrolige virksomhedsoplysninger.

3. Da Statsrevisorerne behandlede beretningen, kritiserede de skarpt, at en række statslige institutioner ikke i tilstrækkeligt omfang beskytter fortrolige oplysninger om personer og virksomheder. Det kan medføre risiko for, at personer kan få krænket deres privatliv, og at virksomheder kan miste konkurrencefordele, fordi personer, private virksomheder og offentlige myndigheder kan få adgang til fortrolige oplysninger, som de ikke er berettigede til.

Statsrevisorerne fandt det særdeles relevant, at flere af institutionerne meget hurtigt havde iværksat tiltag, der skulle imødegå kritikpunkterne i undersøgelsen.

4. Dette notat indeholder Rigsrevisionens vurdering af de initiativer, som ministrene har iværksat og vil iværksætte som følge af beretningen.

Hele sagen og dens dokumenter kan følges på www.rigsrevisionen.dk og på www.ft.dk/Statsrevisorerne.

II. Gennemgang af ministrenes redegørelser

Retningslinjer for at sikre fortrolige oplysninger

5. Beretningen viste, at Institut for Menneskerettigheder ikke havde nogen retningslinjer, der var dækkende. Socialstyrelsen og Sundhedsstyrelsen manglede enkelte specifikke retningslinjer, fx for distancearbejdsplads. Ingen af de 7 institutioner, der havde retningslinjer, havde opdateret alle retningslinjer inden for det seneste år, som de skal ifølge sikkerhedsbekendtgørelsen.

Beretningen viste i øvrigt, at SKAT, Socialstyrelsen og Sundhedsstyrelsen ikke havde opdaterede retningslinjer for at sikre fortrolige virksomhedsoplysninger.

6. Det fremgår af redegørelserne fra de ansvarlige ministre, at Institut for Menneskerettigheder, Socialstyrelsen og Sundhedsstyrelsen har udarbejdet de manglende retningslinjer. Alle 8 ministre bemærker i deres redegørelser, at retningslinjerne er eller vil blive opdateret. Det gælder også retningslinjer for de undersøgte systemer, der indeholder fortrolige oplysninger om virksomheder.

Kontrol af brugernes adgang i de undersøgte systemer
7. Beretningen viste, at Arbejdsskadestyrelsen, Institut for Menneskerettigheder, Rigspolitiet, SKAT, Socialstyrelsen og Sundhedsstyrelsen ikke har udført en halvårlig kontrol i de undersøgte systemer, som de skal ifølge sikkerhedsbekendtgørelsen.

Beretningen viste endvidere, at SKAT, Socialstyrelsen og Sundhedsstyrelsen ikke har gennemgået brugernes rettigheder med et passende interval, hvad angår de undersøgte systemer, der indeholder fortrolige virksomhedsoplysninger.

8. De ansvarlige ministre har alle bemærket, at institutionerne har igangsat eller vil igangsætte initiativer til at udføre en halvårlig kontrol af brugernes adgange i de undersøgte systemer.

Kontrol af afviste forsøg på at få adgang til de undersøgte systemer
9. Beretningen viste, at Socialstyrelsen ikke har registreret afviste forsøg på at få adgang til det undersøgte system. Arbejdsskadestyrelsen, SKAT og Sundhedsstyrelsen har ikke fulgt op på de afviste forsøg. Systemerne er dog sat op til, at adgangen låses efter 3-5 forgæves forsøg.

10. Det fremgår af ministeren for børn, ligestilling, integration og sociale forholds redegørelse, at Socialstyrelsen har taget initiativ til at rette it-systemet, så afviste forsøg på adgang registreres. Vedrørende de 3 institutioner, som ikke fulgte op på de afviste forsøg, bemærker ministrene, at institutionerne har igangsat initiativer, så de kan følge op på gentagne afviste adgangsforsøg.

Registrering af medarbejdernes opslag på enkeltpersoner i de undersøgte systemer
11. Beretningen viste, at Institut for Menneskerettigheder og Danmarks Statistik ikke har registreret medarbejdernes opslag på enkeltpersoner i de undersøgte systemer. Forsvarskommandoen, Rigspolitiet, SKAT, Socialstyrelsen og Sundhedsstyrelsen har ikke slettet registreringerne efter ½ år eller efter en eventuel udvidet periodes afslutning, som de skal ifølge sikkerhedsbekendtgørelsen.

12. Statsrevisorerne bemærkede særligt, at Rigsrevisionen allerede i 2011 gjorde Danmarks Statistik opmærksom på manglende opfyldelse af sikkerhedsbekendtgørelsens krav. Statsrevisorerne fandt det utilfredsstillende, at Danmarks Statistik endnu ikke opfyldte kravene.

Det fremgår af økonomi- og indenrigsministerens redegørelse, at ministeren beklager, at man ikke tilstrækkeligt hurtigt tog kontakt til Datatilsynet og forelagde dem spørgsmålet, som blev endeligt afklaret med Datatilsynets afgørelse den 4. juli 2014. Danmarks Statistik har efter afgørelsen udarbejdet en plan for at logge den statistiske behandling af personoplysninger efter sikkerhedsbekendtgørelsens § 19, stk. 1. Løsningen omfatter også, at logfiler vil blive slettet igen.

Det fremgår ligeledes af udenrigsministerens redegørelse, at Institut for Menneskerettigheder vil registrere logfiler på enkeltpersoner, og at de efter senest 6 måneder vil blive slettet, efter oplysningerne er kontrolleret.

13. Ud af de 5 institutioner, der ikke slettede registreringerne igen efter ½ år, bemærker forsvarsministeren, skatteministeren, ministeren for børn, ligestilling, integration og sociale forhold og ministeren for sundhed og forebyggelse, at institutionerne har indført eller vil indføre tiltag, der kan sikre, at registreringerne slettes igen efter ½ år eller efter den udvidede periodes afslutning.

14. Det fremgår af justitsministerens redegørelse, at Rigspolitiet oplyser, at Rigsrevisionen ikke har anmodet om dokumentation for sletning af logregistreringerne, men kun har anmodet om formel dokumentation vedrørende beslutningen om at forlænge perioden for at opbevare loggen. Rigspolitiet oplyser, at logregistreringer slettes maskinelt ved udløbet af den udvidede periodes afslutning, og at der føres løbende kontrol med logregistreringer i forbindelse med tilsyn af mulig uberettiget anvendelse af oplysninger i overensstemmelse med sikkerhedsbekendtgørelsens bestemmelser. Justitsministeriet finder således ikke, at Rigsrevisionens bemærkning om, at Rigspolitiet ikke har slettet logregistreringerne efter den udvidede periodes afslutning, er dækkende for de faktiske forhold.

Det er fortsat Rigsrevisionens opfattelse, at Rigsrevisionen har anmodet om relevant dokumentation, og at beretningen afspejler de oplysninger og den dokumentation, som er fremkommet i løbet af undersøgelsesperioden. Rigsrevisionen vil i forbindelse med it-revisionen følge op på dette punkt.

Databehandleraftaler om de undersøgte systemer

15. Beretningen viste, at SKAT og Socialstyrelsen ikke havde indgået en skriftlig aftale med databehandlerne for de undersøgte systemer. Det gjaldt både de systemer, der indeholdt fortrolige personoplysninger, og de systemer, der indeholdt fortrolige virksomhedsoplysninger. SKAT oplyste, at SKAT i juni 2014 indgik en aftale med databehandleren. Arbejdsskadestyrelsen, Danmarks Statistik, Rigspolitiet og Sundhedsstyrelsen har ikke fulgt op på den indgåede aftale, som de skal ifølge persondataloven.

16. Ministeren for børn, ligestilling, integration og sociale forhold oplyser, at Socialstyrelsen nu har indgået en databehandleraftale med de relevante virksomheder på de undersøgte systemer. Ligeledes bemærker skatteministeren, at SKAT – ud over at have indgået databehandleraftale på de undersøgte systemer – også har indgået databehandleraftaler med 6 andre leverandører og er i gang med at indgå aftale med den sidste leverandør, hvor databehandleraftale er relevant. SKAT vil på baggrund af de indgåede aftaler fastlægge omfang og form for at følge op på aftalerne.

De ansvarlige ministre oplyser videre, at Arbejdsskadestyrelsen, Danmarks Statistik, Rigspolitiet og Sundhedsstyrelsen nu har iværksat eller vil iværksætte initiativer til at følge op på de indgåede aftaler.

Institutionernes eget tilsyn med sikkerhedsforanstaltningerne

17. Beretningen viste, at Arbejdsskadestyrelsen, Institut for Menneskerettigheder, Danmarks Statistik, Rigspolitiet, SKAT, Socialstyrelsen og Sundhedsstyrelsen ikke havde retningslinjer for, hvordan eget tilsyn skal udføres, og institutionerne har derfor heller ikke kunnet udføre et tilsyn i overensstemmelse med retningslinjerne. SKAT og Sundhedsstyrelsen har dog udført en delvis kontrol.

18. De ansvarlige ministre for de 7 institutioner, der ikke havde retningslinjer for eget tilsyn med sikkerhedsforanstaltningerne, bemærker, at institutionerne har udarbejdet eller er i gang med at udarbejde retningslinjer for eget tilsyn med sikkerhedsforanstaltninger.

Institutionernes risikovurderinger for de undersøgte systemer

19. Beretningen viste, at Socialstyrelsen og Sundhedsstyrelsen ikke havde en opdateret risikovurdering for de undersøgte systemer, der indeholder fortrolige virksomhedsoplysninger.

20. Ministeren for børn, ligestilling, integration og sociale forhold og ministeren for sundhed og forebyggelse bemærker, at Socialstyrelsen og Sundhedsstyrelsen har opdateret deres risikovurderinger.

III. Afslutning

21. Rigsrevisionen finder ministrenes initiativer tilfredsstillende og vurderer, at sagen kan afsluttes. Rigsrevisionen vil i forbindelse med it-revisionen fortsat følge, at initiativerne bliver implementeret og fungerer i praksis.

Lone Strøm