JUSTITSMINISTERIET
Justitsministeren

Statsrevisorernes Sekretariat
Christiansborg
1240 København K

Dato: 20 JAN. 2015

Sagsnr.: 2014-024-0220
Dok.: 1441327

Kære statsrevisorer

Ved brev af 20. november 2014 har Statsrevisorernes Sekretariat fremsendt Rigsrevisionens beretning nr. 1/2014 om statens behandling af fortrolige oplysninger om personer og virksomheder med anmodning om, at jeg redegør for, hvilke initiativer beretningen giver anledning til.

Indledningsvist vil jeg gerne kvittere for beretningen.

Jeg vil gerne understrege, at Justitsministeriet har et særligt ansvar for at sikre en høj grad af datasikkerhed. Ministeriet har en række kritiske it-systemer på ministerområdet, herunder i Rigspolitiet, og ministeriet håndterer dagligt fortrolige personoplysninger. Jeg ser derfor med stor alvor på Rigsrevisionens konklusioner i forhold til it-sikkerhed i Rigspolitiet og Statsrevisorernes efterfølgende bemærkninger omkring it-sikkerhed.

Jeg kan imidlertid konstatere, at Rigspolitiet har oplyst, at der er gennemført en række aktiviteter, således at Rigspolitiet nu efterlever sikkerhedsbekendtgørelsens krav for Det Centrale Kriminalregister.

For så vidt angår Statsrevisorernes og Rigsrevisionens konkrete bemærkninger, skal jeg bemærke følgende:

Ad punkt 12 & 13 om sikkerhedsbekendtgørelsens krav om retningslinjer
Af sikkerhedsbekendtgørelsens § 5, stk. 1 og 2, fremgår det, at den dataansvarlige myndighed skal fastsætte nærmere interne bestemmelser om sikkerhedsforanstaltninger i myndigheden til uddybning af de regler, der

Slotsholmsgade 10
1216 København K.

Telefon 7226 8400
Telefax 3393 3510

www.justitsministeriet.dk
jm@jm.dk

fremgår af bekendtgørelsen, samt at bestemmelserne skal gennemgås mindst én gang hvert år.

Jeg noterer med tilfredshed, at det fremgår af beretningen, at Rigspolitiet efterlever sikkerhedsbekendtgørelsens krav om fastlæggelse af retningslinjer for beskyttelse af fortrolige personoplysninger.

For så vidt angår opdateringen af retningslinjerne, har Rigspolitiet oplyst, at politiets it-sikkerhedspolitik er opdateret og godkendt af direktionen med virkning fra september 2014. Den underliggende sikkerhedshåndbog, der fastsætter de nærmere interne bestemmelser om sikkerhedsforanstaltninger i politiet, er ligeledes opdateret og forventes endelig godkendt i politiets it-sikkerhedsudvalg primo 2015.

Ad punkt 15 om sikkerhedsbekendtgørelsens krav om brugeradgange og kontrol heraf

Af sikkerhedsbekendtgørelsens § 17, stk. 1 og 2, fremgår det bl.a., at det skal sikres, at autoriserede personer fortsat opfylder betingelserne om brugeradgang, samt at der skal foretages kontrol heraf halvårligt.

Af beretningen fremgår det, at Rigspolitiet ikke efterlever kravet, idet kontrollen hidtil alene har været udført helårligt.

Rigspolitiet har oplyst, at årsagen til, at kontrollen hidtil har været udført helårligt, er det afledte ressourceforbrug i politikredsene. Det oplyses endvidere, at Rigspolitiet har været i dialog med Datatilsynet vedrørende problemstillingen. På den baggrund er der nu implementeret rollebaseret adgangstildeling, der dokumenteres i et centralt brugeradministrationssystem. Løsningen muliggør, at kontrollen af brugeradgange kan foretages halvårligt.

Kontrollen af brugeradgange i politikredsene vil således fremadrettet foregå halvårligt og vil blive dokumenteret i det centrale brugeradministrationssystem.

Det bemærkes, at systemet ikke omfatter brugeradgange i Rigspolitiet, hvorfor kontrol af disse fortsat vil blive foretaget manuelt. Rigspolitiet vil fremadrettet foretage disse kontroller halvårligt, for så vidt angår politiets centrale registre, herunder Det Centrale Kriminalregister. Førstkommende kontrol er planlagt til februar 2015.

Ad punkt 16 om sikkerhedsbekendtgørelsens krav om kontrol med afviste adgangsforsøg

Jeg konstaterer med tilfredshed, at det fremgår af beretningen, at Rigspolitiet registrerer afviste forsøg på at få adgang til Det Centrale Kriminalregister, samt at Rigspolitiet regelmæssigt følger op på, om der har været afviste forsøg på at få adgang til registret.

Ad punkt 17 om sikkerhedsbekendtgørelsens krav om registrering af opslag på enkeltpersoner

Af sikkerhedsbekendtgørelsens § 19, stk. 1, fremgår det bl.a., at der skal foretages en maskinel registrering (logning) af alle anvendelser af personoplysninger, samt at loggen skal opbevares i 6 måneder, hvorefter den slettes. Det fremgår endvidere, at myndigheder med særlige behov kan opbevare loggen i op til 5 år.

Jeg konstaterer med tilfredshed, at Rigspolitiet har dokumenteret baggrunden for udvidelsen af logningsperioden overfor Rigsrevisionen.

Af beretningen fremgår det imidlertid, at Rigspolitiet samlet set efter Rigsrevisionens vurdering ikke efterlever kravet om registrering af opslag på enkeltpersoner, idet Rigspolitiet ikke har slettet registreringerne efter den udvidede periodes afslutning.

Rigspolitiet har i den forbindelse oplyst, at Rigsrevisionen ikke har anmodet om dokumentation for sletning af logregistreringerne men alene anmodet om formel dokumentation vedrørende beslutningen om forlængelse af perioden for opbevaring af loggen. Det kan i den forbindelse oplyses, at sletning af logregistreringer foretages maskinelt ved udløbet af den udvidede periodes afslutning, samt at der føres løbende kontrol med logregistreringerne i forbindelse med tilsyn af mulig uberettiget anvendelse af oplysninger i overensstemmelse med sikkerhedsbekendtgørelsens bestemmelser.

Under henvisning til det ovenstående finder Justitsministeriet således ikke, at Rigsrevisionens bemærkning om, at Rigspolitiet ikke har foretaget sletning af logregistreringer efter den udvidede periodes afslutning, er dækkende for de faktiske forhold.

Ad punkt 19 om sikkerhedsbekendtgørelsens krav om aftaler med databehandlere

Af sikkerhedsbekendtgørelsens § 7, stk. 1, fremgår det bl.a., at hvis behandling af personoplysninger foretages af en databehandler på den dataansvarliges vegne, skal der foreligge en skriftlig aftale, hvoraf det fremgår, at reglerne i bekendtgørelsen ligeledes gælder for behandlingen ved databehandleren. Af persondatalovens § 42 følger det endvidere, at der skal følges op på databehandleraftalen.

Jeg konstaterer med tilfredshed, at Rigspolitiet indgår aftaler med de databehandlerne, Rigspolitiet benytter sig af.

Rigsrevisionen vurderer imidlertid, at Rigspolitiet ikke samlet efterlever kravet om opfølgning, idet Rigspolitiet kun indhenter generelle revisionserklæringer fra databehandlerne. Rigsrevisionen vurderer således, at erklæringerne ikke har til formål at kontrollere om persondataloven overholdes.

Rigspolitiet har oplyst, at Rigspolitiet, som opfølgning på de indhentede revisionserklæringer, løbende afholder sikkerhedsmøder og driftsstatusmøder med databehandlerne, ligesom databehandlerne månedligt afrapporterer på sikkerhedsemner ved indsendelse af rapporter herom.

Rigspolitiet har endvidere oplyst, at Rigsrevisionens vurdering af manglende opfølgning på sikkerhedsforanstaltningerne hos databehandlerne tages til efterretning, hvorfor Rigspolitiet fremadrettet vil indhente en yderligere revisionserklæring, der forholder sig specifikt til, om der er truffet de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger mod, at oplysninger kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med persondataloven.

Jeg konstaterer med tilfredshed, at Rigspolitiet allerede har foretaget opfølgning på Rigsrevisionens anbefaling i 2014.

Ad punkt 21 om sikkerhedsbekendtgørelsens krav om institutionernes eget tilsyn med sikkerhedsforanstaltningerne

Af sikkerhedsbekendtgørelsens § 5, stk. 1, fremgår det, at den dataansvarlige myndighed skal fastsætte retningslinjer for myndighedernes tilsyn med overholdelsen af de sikkerhedsforanstaltninger, der er fastsat for myndigheden.

Af beretningen fremgår det, at bestemmelsen i sikkerhedsbekendtgørelsen ikke er uddybet, og at det således er op til institutionerne at fastlægge det nærmere indhold af tilsynet.

Rigspolitiet har bl.a. oplyst til Rigsrevisionen, at der foreligger retningslinjer for Rigspolitiets tilsyn med, at sikkerhedsforanstaltningerne overholdes. Derudover har Rigspolitiet redegjort for, at der gennemføres regelmæssigt tilsyn med overholdelsen af sikkerhedsforanstaltningerne.

Rigsrevisionen har imidlertid vurderet, at retningslinjerne ikke er tilstrækkeligt udbygget, samt at det faktum, at Rigspolitiet deltager i andre myndigheders tilsyn/revisioner ikke kan erstatte Rigspolitiets eget tilsyn med, at sikkerhedsforanstaltningerne overholdes i forhold til Det Centrale Kriminalregister. Ovenstående medfører, at Rigsrevisionen vurderer, at Rigspolitiet samlet set ikke efterlever kravet.

Jeg kan i forlængelse heraf oplyse, at Rigspolitiet har planlagt at udvide det eksisterende tilsyn med overholdelse af sikkerhedsforanstaltningerne i løbet af 2015 således, at det også omfatter Rigspolitiets eget tilsyn med, at der er truffet de fornødne sikkerhedsforanstaltninger i forhold til Det Centrale Kriminalregister, samt at den nye tilsynspraksis forventes påbegyndt i 2. halvår 2015.

Ad punkt 23 om Datatilsynets tilsyn med de statslige myndigheder
Af beretningen samt Statsrevisorernes efterfølgende bemærkninger fremgår det, at Datatilsynet ikke har inspiceret de otte it-systemer med personoplysninger, som Rigsrevisionens beretning omfatter, inden for de sidste 3 år.

Datatilsynet oplyser imidlertid, at der er gennemført andre tilsynsaktiviteter over for flere af de myndigheder, som er ansvarlige for de otte systemer. Inden for de seneste tre år har Datatilsynet bl.a. foretaget inspektioner hos SKAT, Sundhedsstyrelsen og Rigspolitiet.

Tilsynet har endvidere taget sager op af egen drift over for en række myndigheder, herunder Danmarks Statistik, Rigspolitiet, SKAT og Sundhedsstyrelsen, ligesom Datatilsynet har behandlet klage- og anmeldelsessager vedrørende flere af myndighederne.

Siden persondatalovens ikrafttræden i 2000 har Datatilsynet gennemført ca. 160 inspektionsbesøg hos statslige myndigheder. Inspektionerne har

fordelt sig på besøg hos mange forskellige statslige myndigheder, herunder Rigspolitiet, politikredse, statsadvokaturer, fængsler, statsforvaltninger, enheder inden for SKAT samt forskellige ministeriers departementer og underliggende styrelser. Af Datatilsynets årsberetninger, som afgives til Folketinget, jf. persondatalovens § 65, og offentliggøres, fremgår en oversigt over udførte inspektioner i det pågældende år.

Datatilsynets oplyser endvidere, at inspektionerne har karakter af et legalitetstilsyn – dvs. fokus er på, at behandlingen af personoplysninger er i overensstemmelse med reglerne i persondataloven og evt. anden relevant lovgivning, og at reglerne om registreredes rettigheder overholdes.

I forhold til datasikkerhed stiller Datatilsynet typisk spørgsmål inden for de emner, som fremgår af sikkerhedsbekendtgørelsen. Spørgsmålene vedrører typisk myndighedernes uddybende sikkerhedsregler eller mere specifikke sikkerhedsforanstaltninger, herunder f.eks. procedurer for autorisation af brugere og/eller logning. Tilsynet foretager derimod ikke en mere omfattende it-revision eller fuldstændig gennemgang af de etablerede sikkerhedsforanstaltninger.

Kopi af denne skrivelse er samtidigt fremsendt elektronisk til Rigsrevisionens orientering.

Med venlig hilsen

Mette Frederiksen