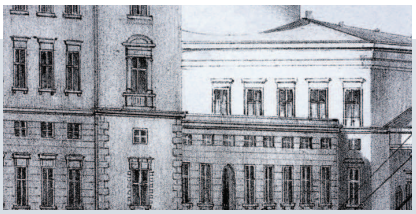
1/2014

STATSREVISORERNE

Beretning om statens behandling af fortrolige oplysninger om personer og virksomheder



1/2014

Beretning om statens behandling af fortrolige oplysninger om personer og virksomheder

Statsrevisorerne fremsender denne beretning med deres bemærkninger til Folketinget og vedkommende minister, jf. § 3 i lov om statsrevisorerne og § 18, stk. 1, i lov om revisionen af statens regnskaber m.m.

København 2014

Denne beretning til Folketinget skal behandles ifølge lov om revisionen af statens regnskaber, § 18:
Statsrevisorerne fremsender med deres eventuelle bemærkninger Rigsrevisionens beretning til Folketinget og vedkommende minister.
Udenrigsministeren, skatteministeren, økonomi- og indenrigsministeren, justitsministeren, forsvarsministeren, ministeren for børn, ligestilling, integration og sociale forhold, ministeren for sundhed og forebyggelse samt beskæftigelsesministeren afgiver en redegørelse til beretningen.
Rigsrevisor afgiver et notat med bemærkninger til ministrenes redegørelser.
På baggrund af ministrenes redegørelser og rigsrevisors notat tager Statsrevisorerne endelig stilling til beretningen, hvilket forventes at ske i marts 2015.
Ministrenes redegørelser, rigsrevisors bemærkninger og Statsrevisorernes eventuelle bemærkninger samles i Statsrevisorernes Endelig betænkning over statsregnskabet, som årligt afgives til Folketinget i februar måned – i dette tilfælde Endelig betænkning over statsregnskabet 2014, som afgives i februar 2016.

Henvendelse vedrørende
denne publikation rettes til:

Statsrevisorerne
Folketinget
Christiansborg
1240 København K
Telefon: 33 37 59 87
Fax: 33 37 59 95
E-mail: statsrevisorerne@ft.dk
Hjemmeside: www.ft.dk/statsrevisorerne

Yderligere eksemplarer kan
købes ved henvendelse til:

Rosendahls-Schultz Distribution
Herstedvang 10
2620 Albertslund
Telefon: 43 22 73 00
Fax: 43 63 19 69
E-mail: distribution@rosendahls.dk
Hjemmeside: www.rosendahls.dk

ISSN 2245-3008
ISBN 978-87-7434-447-6

Statsrevisorernes bemærkning

Statsrevisorerne,
den 12. november 2014

Peder Larsen
Henrik Thorup
Kristian Jensen
Klaus Frandsen
Lennart Damsbo-Andersen
Lars Barfoed

BERETNING OM STATENS BEHANDLING AF FORTROLIGE OPLYSNINGER OM PERSONER OG VIRKSOMHEDER

Digitalisering er en vigtig måde at forny og effektivisere den offentlige sektor på. Den øgede digitalisering af kommunikationen mellem borgere, private virksomheder og offentlige myndigheder forudsætter, at store mængder af data af fortrolig karakter beskyttes, så oplysningerne ikke falder i de forkerte hænder. Data beskyttes ved at kontrollere brugeradgange, registrere medarbejderes opslag, tjekke om interne retningslinjer og aftaler med eksterne databehandlere overholdes mv.

Rigsrevisionen har undersøgt, hvordan fortrolige oplysninger om personer og virksomheder behandles i 11 udvalgte it-systemer i 8 statslige institutioner: Arbejdsskadestyrelsen, Danmarks Statistik, Forsvarskommandoen, Institut for Menneskerettigheder, Rigspolitiet, SKAT, Socialstyrelsen og Sundhedsstyrelsen, hvoraf flere er vant til at håndtere store mængder fortrolige oplysninger.

Undersøgelsen viser, at ingen af de undersøgte institutioner efterlever alle de krav til behandling af fortrolige personoplysninger, som er fastsat i sikkerhedsbekendtgørelsen, der er udstedt i medfør af persondataloven.

Det bemærkes, at den manglende efterlevelse af sikkerhedsbekendtgørelsens krav kan gøre sig gældende for en større kreds af statslige institutioner.

Undersøgelsen viser endvidere, at sikkerheden ved behandling af fortrolige data fra private virksomheder bør styrkes – også selv om der ikke er fastsat særlig lovgivning for beskyttelse af fortrolige virksomhedsoplysninger.

Statsrevisorerne kritiserer skarpt, at en række statslige institutioner ikke i tilstrækkeligt omfang beskytter fortrolige oplysninger om personer og virksomheder. Det medfører 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 finder det særdeles relevant, at flere af institutionerne meget hurtigt har iværksat tiltag, der skal imødegå kritikpunkterne i undersøgelsen.

Statsrevisorerne bemærker særligt, at Rigsrevisionen allerede i 2011 gjorde Danmarks Statistik opmærksom på manglende opfyldelse af sikkerhedsbekendtgørelsens krav. Statsrevisorerne finder det utilfredsstillende, at Danmarks Statistik endnu ikke opfylder kravene.

Datatilsynet har bl.a. til opgave at føre tilsyn med, at statslige institutioner håndterer fortrolige personoplysninger i overensstemmelse med persondataloven og tilhørende regler. Statsrevisorerne har noteret sig, at Datatilsynet ikke har ført tilsyn med de 8 undersøgte it-systemer i de seneste 3 år.

Statsrevisorerne er opmærksomme på, at uklar ansvarsplacering mellem flere myndigheder kan svække tilsyn og datasikkerhed.

RIGSREVISIONEN

Beretning til Statsrevisorerne om statens behandling af fortrolige oplysninger om personer og virksomheder

Rigsrevisionen har selv taget initiativ til denne undersøgelse og afgiver derfor beretningen til Statsrevisorerne i henhold til § 17, stk. 2, i rigsrevisorloven, jf. lovbekendtgørelse nr. 101 af 19. januar 2012. Beretningen vedrører finanslovens § 6. Udenrigsministeriet, § 9. Skatteministeriet, § 10. Økonomi- og Indenrigsministeriet, § 11. Justitsministeriet, § 12. Forsvarsministeriet, § 15. Ministeriet for Børn, Ligestilling, Integration og Sociale Forhold, § 16. Ministeriet for Sundhed og Forebyggelse og § 17. Beskæftigelsesministeriet.

Indholdsfortegnelse

Beretningen vedrører finanslovens § 6. Udenrigsministeriet, § 9. Skatteministeriet, § 10. Økonomi- og Indenrigsministeriet, § 11. Justitsministeriet, § 12. Forsvarsministeriet, § 15. Ministeriet for Børn, Ligestilling, Integration og Sociale Forhold, § 16. Ministeriet for Sundhed og Forebyggelse og § 17. Beskæftigelsesministeriet.

I undersøgelsesperioden har der været følgende ministre:

Udenrigsministeriet:
Holger K. Nielsen: december 2013 - februar 2014
Martin Lidegaard: februar 2014 -

Skatteministeriet:
Jonas Dahl: december 2013 - februar 2014
Morten Østergaard: februar 2014 - september 2014
Benny Engelbrecht: september 2014 -

Økonomi- og Indenrigsministeriet:
Margrethe Vestager: oktober 2011 - september 2014
Morten Østergaard: september 2014 -

Justitsministeriet:
Karen Hækkerup: december 2013 - oktober 2014
Mette Frederiksen: oktober 2014 -

Forsvarsministeriet:
Nicolai Wammen: august 2013 -

Ministeriet for Børn, Ligestilling, Integration og Sociale Forhold:
Annette Vilhelmsen: august 2013 - februar 2014
Manu Sareen: februar 2014 -

Ministeriet for Sundhed og Forebyggelse:
Astrid Krag Kristensen: oktober 2011 - februar 2014
Nick Hækkerup: februar 2014 -

Beskæftigelsesministeriet:
Mette Frederiksen: oktober 2011 - oktober 2014
Henrik Dam Kristensen: oktober 2014 -

Beretningen har i udkast været forelagt de respektive ministerier og institutioner, hvis bemærkninger er afspejlet i beretningen.

1. Introduktion og konklusion

1.1. Formål og konklusion

1. Denne beretning handler om, hvordan en række statslige institutioner beskytter fortrolige oplysninger om personer og virksomheder. Beretningen er udarbejdet som en smal beretning, og undersøgelsen baserer sig på it-revisioner udført som led i årsrevisionen i foråret 2014. Formålet med revisionen har været at vurdere, om institutionerne beskytter fortrolige oplysninger om personer og virksomheder tilstrækkeligt. Rigsrevisionen har selv taget initiativ til undersøgelsen.

En **smal beretning** bygger på de samme revisionsprincipper og kvalitetskrav som Rigsrevisionens øvrige beretninger, men undersøgelsen er foretaget på et mere afgrænset område.

KONKLUSION

Rigsrevisionen har undersøgt, hvordan 8 statslige institutioner behandler fortrolige oplysninger om personer og virksomheder i 11 udvalgte it-systemer. Rigsrevisionen finder det utilfredsstillende, at institutionerne ikke beskytter fortrolige oplysninger om personer og virksomheder tilstrækkeligt.

Når en institution ikke beskytter fortrolige oplysninger tilstrækkeligt, øger det risikoen for, at uvedkommende får kendskab til fortrolige oplysninger, og at oplysningerne kan misbruges. Manglende beskyttelse af fortrolige oplysninger kan desuden svække borgeres og virksomheders tillid til it-sikkerheden i den statslige forvaltning, hvilket kan blive en barriere for fortsat at digitalisere og effektivisere i staten.

Undersøgelsen viser, at ingen af de undersøgte institutioner efterlever alle de krav til behandling af fortrolige personoplysninger, som fremgår af sikkerhedsbekendtgørelsen, og som er en uddybning af persondatalovens bestemmelser. De undersøgte institutioner mangler i vidt omfang at opdatere interne retningslinjer, at kontrollere brugeradgange, at registrere medarbejdernes opslag og slette dem igen, at følge op på, om indgåede aftaler med eksterne databehandlere overholdes, og at føre tilsyn med, at interne sikkerhedsforanstaltninger overholdes. Selv institutioner som Danmarks Statistik, Rigspolitiet og SKAT, der er vant til at håndtere store mængder fortrolige oplysninger, har i de undersøgte systemer ikke efterlevet sikkerhedsbekendtgørelsens krav på flere punkter.

*Om en **oplysning er fortrolig** afhænger af, om oplysningen er af en sådan karakter, at den efter den almindelige opfattelse i samfundet bør kunne forlanges unddraget offentlighedens kendskab.*

*Oplysninger om racemæssig eller etnisk baggrund, politisk, religiøs eller filosofisk overbevisning, fagforeningsmæssige tilhørsforhold, helbredsforhold, seksuelle forhold, strafbare forhold og væsentlige sociale problemer vil utvivlsomt være fortrolige oplysninger. Disse oplysninger er nævnt i lov om behandling af personoplysninger, § 7, stk. 1, og § 8, stk. 1. De kaldes også for **følsomme personoplysninger**.*

Oplysninger om interne familieforhold, fx stridigheder, og oplysninger om selvmordsforsøg og ulykkestilfælde er også fortrolige oplysninger. Herudover vil fx oplysninger om indtægts- og formueforhold samt arbejds-, uddannelses- og ansættelsesmæssige forhold efter omstændighederne også være fortrolige.

Danmarks Statistik behandler mange oplysninger om alle danskere, men registrerer ikke medarbejdernes opslag i overensstemmelse med sikkerhedsbekendtgørelsens krav. I praksis betyder det, at Danmarks Statistik ikke kan spore, om en medarbejder har foretaget et uberettiget opslag, hvis der fx er lækket oplysninger om en persons tidligere domme. Rigsrevisionen konstaterede allerede i 2011, at Danmarks Statistik ikke umiddelbart registrerede medarbejdernes opslag efter sikkerhedsbekendtgørelsen. Datatilsynet vurderede i juli 2014, at kravet om at logge gælder for Danmarks Statistik. Datatilsynet henstillede, at Danmarks Statistik tog skridt til at indrette sin behandling af personoplysninger, så sikkerhedsbekendtgørelsens krav blev opfyldt. Datatilsynet og Danmarks Statistik er fortsat i dialog om sagen. Rigsrevisionen finder det ikke tilfredsstillende, at Danmarks Statistik ikke har sørget for en hurtigere afklaring af så vigtig en sag.

Rigsrevisionen har desuden undersøgt, om 3 af institutionerne også beskytter private virksomheders fortrolige oplysninger tilstrækkeligt. Der er ikke fastsat særlig lovgivning for at beskytte fortrolige virksomhedsoplysninger, som det gør sig gældende for fortrolige personoplysninger. Rigsrevisionen finder, at institutionerne bør forbedre sikkerheden for de oplysninger, de behandler om private virksomheder, fordi læk af disse oplysninger fx kan skade virksomhedernes konkurrenceevne.

1.2. Baggrund

2. En stadig større del af kommunikationen mellem borgere, private virksomheder og offentlige institutioner foregår digitalt. Den øgede digitalisering bevirker, at der behandles store mængder oplysninger af fortrolig karakter. Det kan fx være oplysninger om en persons helbred, skatteforhold eller strafbare forhold.

Den øgede digitalisering stiller krav til institutionernes behandling af fortrolige oplysninger og til selve it-sikkerheden, så det fx kun er de relevante medarbejdere i institutionen, der har adgang til oplysningerne. Hvis en offentlig institution ikke beskytter oplysningerne tilstrækkeligt, er der en øget risiko for, at personer, private virksomheder og offentlige institutioner får adgang til oplysninger, som de ikke er berettigede til.

Brud på datasikkerheden kan have vidtrækkende konsekvenser for de personer og virksomheder, det går ud over, hvis oplysninger falder i de forkerte hænder. Personer kan få krænket deres privatliv, hvis fx oplysninger om deres helbred eller strafbare forhold pludselig bliver omtalt i medierne. Private virksomheder kan fx miste konkurrencefordele, hvis en konkurrent får uberettiget kendskab til fortrolige oplysninger om virksomhedens produkter.

Problemstillingen er især aktuel, efter at det i april 2014 kom frem, at en medarbejder med adgang til fortrolige personoplysninger angiveligt skulle have overvåget oplysninger om kendte danskere og solgt oplysningerne videre. Episoden har bl.a. ført til debat om, hvordan personoplysninger skal håndteres. I forlængelse heraf har Folketingets Kulturudvalg og Folketingets Retsudvalg i juni 2014 i fællesskab afgivet en beretning om nedsættelse af en parlamentarisk arbejdsgruppe, der skal undersøge mulighederne for en bedre beskyttelse af personfølsomme oplysninger og et effektivt tilsyn med såvel offentlige institutioners som private virksomheders behandling af disse oplysninger.

3. Det er de statslige institutioners ansvar at sikre, at fortrolige oplysninger om personer og virksomheder bliver behandlet korrekt. Finansministeriet har ressortansvaret for it-sikkerhedspolitikken i staten og fastlægger rammevilkårene for digitalisering af den offentlige sektor. Datatilsynet er den statslige myndighed, der fører tilsyn med, at institutionerne behandler oplysninger om personer i overensstemmelse med persondataloven og regler udstedt i medfør af loven.

4. En statslig institution kan sikre oplysninger ved at gennemføre forskellige tiltag, der forbedrer it-sikkerheden. Det kan være gennem organisatoriske eller administrative tiltag som fx at udarbejde risikovurderinger og instrukser, som fastlægger forretningsgange og ansvar for it-sikkerheden og for kontrol og tilsyn. Det kan også være tekniske løsninger, der medvirker til at sikre, at kun medarbejdere med et arbejdsbetinget behov får adgang til oplysningerne. Desuden kan det være at sikre den fysiske bygning, hvor oplysninger behandles, mod uautoriseret adgang.

5. Behandling af oplysninger om personer er omfattet af lov om behandling af personoplysninger (persondataloven). Persondatalovens bestemmelser er uddybet i bekendtgørelse om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for den offentlige forvaltning (sikkerhedsbekendtgørelsen).

Regler for personoplysninger
Lov nr. 429 af 31. maj 2000 om behandling af personoplysninger (persondataloven).

Bekendtgørelse nr. 528 af 15. juni 2000 om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for den offentlige forvaltning (sikkerhedsbekendtgørelsen).

Persondataloven bygger på et EU-direktiv fra oktober 1995. I lyset af den teknologiske udvikling, globaliseringen og den stigende anvendelse af personoplysninger arbejdes der i EU-regi på at regulere databeskyttelsesområdet, bl.a. i en generel forordning (bindende retsakt).

Ud over personoplysninger indsamler de statslige institutioner også en række fortrolige oplysninger om virksomheder. Der eksisterer ingen lovgivning for behandling af oplysninger om virksomheder i Danmark på samme måde som for personoplysninger.

Der findes flere vejledninger, standarder mv., som handler om it-sikkerhed, bl.a. den danske informationssikkerhedsstandard DS 484 og den internationale informationssikkerhedsstandard ISO 27001. De statslige institutioner har fra januar 2014 skullet følge ISO 27001. Digitaliseringsstyrelsen har også udarbejdet en række guider, vejledninger og paradigmer til brug for de statslige institutioners arbejde med informationssikkerhed.

Standarder for informationssikkerhed
DS 484 og ISO 27001 er begge informationssikkerhedsstandarder. Der er forskel på indholdet i sikkerhedsstandarderne, men for dem begge gælder det, at efterlevelse af standarden er en metode til at sikre virksomhedernes informationer.

1.3. Revisionskriterier, metode og afgrænsning

Revisionskriterier
6. Undersøgelsens revisionskriterier er baseret på persondataloven og sikkerhedsbekendtgørelsen for så vidt angår institutionernes beskyttelse af fortrolige personoplysninger. Da der ikke eksisterer lovgivning for at beskytte oplysninger om fortrolige virksomhedsoplysninger, har vi baseret vores revisionskriterier på informationssikkerhedsstandarden ISO 27001.

Metode
7. Undersøgelsen er baseret på it-revisioner udført som led i årsrevisionen. Undersøgelsen omfatter 8 statslige institutioner, som er udvalgt, fordi de alle behandler fortrolige oplysninger om personer og/eller virksomheder. Vi har udvalgt 1-2 it-systemer hos hver institution. I forbindelse med årsrevisionen udvælger vi primært it-systemer til revision efter væsentlighed og risiko, men vi prioriterer også at udvælge mindre it-systemer for at kunne vurdere systemerne bredt. Vi har derfor udvalgt både små og store institutioner, der behandler fortrolige person- og virksomhedsoplysninger i it-systemer. Vi har også udvalgt it-systemer, der både har få og mange brugere af systemerne, og it-systemer, der har registreret få og mange personer/virksomheder. Undersøgelsens resultater kan endvidere underbygges af erfaringer fra tidligere it-revisioner. Se bilag 1 om metode.

Brugere af et it-system *er interne brugere, fx medarbejdere i en statslig institution, og eksterne brugere, fx medarbejdere i kommuner, der har adgang til at behandle oplysninger om de personer/virksomheder, der er registreret i systemet. Brugerne kan fx have adgang til at læse og/eller redigere i oplysningerne.*

Antal ***registrerede i et it-system*** *er antallet af personer (eller virksomheder), som der findes oplysninger om i systemet. Når en person fx betaler skat, registreres oplysninger om personens skatteforhold i et it-system. Antal registrerede personer er alle de personer, hvis oplysninger er registreret i systemet.*

I afsnit 2.1 undersøger vi, hvordan institutionerne beskytter oplysninger om personer i 8 it-systemer. I afsnit 2.2 undersøger vi, hvordan institutionerne beskytter oplysninger om virksomheder i 3 it-systemer.

Tabel 1 viser, hvilke oplysninger de undersøgte systemer indeholder, hvad systemerne anvendes til, hvor mange personer og virksomheder der er registreret i systemerne, og hvor mange brugere der har adgang til oplysningerne.

Tabel 1. De undersøgte systemer

Institution og system	Indhold af oplysninger	Systemet anvendes af	Antal registrerede i systemet	Antal brugere af systemet
Systemer med fortrolige oplysninger om personer:				
Arbejdsskadestyrelsen Scan Jour P (SJP) understøtter behandlingen af sager om, hvorvidt skader eller sygdomme kan anerkendes som arbejdsskader.	Skader, ulykker, sygdomme mv.	Arbejdsskadestyrelsen, Ankestyrelsen, Arbejdstilsynet, forsikringsselskaber og kommuner.	1.003.013 personer	349 interne og eksterne brugere.
Danmarks Statistik Oracle Database er opdelt i adskilte projekter. Bruges til statistiske analyser mv. Systemet indeholder alle de oplysninger, som Danmarks Statistik modtager.	Kriminalitet, domme, sociale ydelser, folke- og førtidspension, lægebesøg, opholdstilladelser, trafikuheld, fødsel og adoption mv.	Danmarks Statistik.	Alle personer med et cpr-nr., herunder også afdøde.	Typisk 3-8 interne brugere pr. projekt. En bruger har typisk adgang til flere projekter. Kun et fåtal har adgang til mere end 20 forskellige projekter. I alt 450 interne brugere.
Forsvarskommandoen Lønmodulet i Dansk Forsvars Management- og Ressourcestyringssystem (DeMars), der er et koncernfælles styringssystem.	Modulet indeholder bl.a. oplysninger om cpr-nr., helbred, militære straffe, løn og fravær.	Forsvarskommandoen og Moderniseringsstyrelsen.	282.599 personer	12.272 brugere, heraf 10.512 interne brugere og 1.760 eksterne brugere.
Institut for Menneskerettigheder Et almindeligt fildrev (G-drevet), der understøtter behandlingen af sager om menneskerettigheder og ligebehandling. På drevet gemmes vedhæftede filer fra den indgående post.	Navn, adresse, etnicitet, politisk anskuelse, virksomheders politikker, procedurer, planer mv.	Institut for Menneskerettigheder.	1.695 personer	30 interne brugere.
Rigspolitiet Det Centrale Kriminalregister (Kriminalregisteret) indeholder afgørelser mv. i kriminalsager. Registeret bruges bl.a. til at udskrive straffeattester til brug for strafferetsplejen og til at udarbejde kriminalstatistik.	Lovovertrædelser, rejste sigtelser og afgørelser truffet i straffesager.	Politiet, anklagemyndigheden, Den Uafhængige Politiklagemyndighed, Udlændingestyrelsen, Auditørkorpset, Justitsministeriet og Kriminalforsorgens anstalter og arresthuse.	Antallet af registrerede personer er fortroligt, men der er tale om et betydeligt antal.	14.700 interne og eksterne brugere.
SKAT Faglige kontingenter og A-Kassebidrag (AKFA) indeholder indberetninger om faglige kontingenter og a-kassebidrag.	Medlemskab af fagforening og a-kasse.	SKAT, fagforeninger, a-kasser og private foreninger.	2.639.752 personer	1.341 brugere, heraf 2 interne brugere.
Socialstyrelsen Stofmisbrugerdatabasen (SMDB) bruges til lovovervågning, forskning og formidling.	Sociale og økonomiske forhold for stofmisbrugere i behandling, helbred, stofforbrug og behandlingsintensitet og -formål.	Socialstyrelsen, Sundhedsstyrelsen, Statens Serum Institut og Center for Rusmiddelforskning.	40.848 personer	750 brugere, heraf 12 interne brugere.
Sundhedsstyrelsen Udleveringstilladelser (ULS) understøtter behandlingen af ansøgninger fra læger, dyrlæger og tandlæger om at udlevere lægemidler, der ikke markedsføres i Danmark.	Ansøgte lægemidler, ansøgers data, patientnavn, cpr-nr., eventuel adresse og virksomhedsnavn og -adresse.	Sundhedsstyrelsen.	4.253 personer	27 brugere, heraf 24 interne brugere[1)] og 3 eksterne brugere.

Institution og system	Indhold af oplysninger	Systemet anvendes af	Antal registrerede i systemet	Antal brugere af systemet
Systemer med fortrolige oplysninger om virksomheder:				
SKAT Selskabsskattesystemet (3S) anvendes til at indtaste og beregne skat for selskaber, fonde og foreninger, ændringer af indkomster, administration af udbytte til selskaber og personer i både Danmark og i udlandet samt registrering af diverse oplysninger til statistisk brug.	Selskabers stamoplysninger, hovedaktionærforhold, sambeskatning, ligningsoplysninger, skatteberegning, udbytte mv.	SKAT, kommuner, Danmarks Statistik, Økonomi- og Indenrigsministeriet, visse banker og Statens Arkiver.	407.303 virksomheder	2.290 brugere, heraf 6 eksterne og alle kommuner.[2)]
Socialstyrelsen Project Flow bruges til at styre projekter internt i styrelsen.	Oplysninger om interne projekter og satspuljeprojekter med relevante projektdokumenter.	Socialstyrelsen.	543 aktive projekter[3)]	398 brugere, heraf 4 eksterne brugere.
Sundhedsstyrelsen Kategorisering Af Total-oplysninger (KAT) anvendes primært til at godkende lægemidler. Det er sundhedsproduktområdets centrale database.	Oplysninger om et givent lægemiddel, substitution, virksomhedstilladelser, kliniske forsøg, laboratoriekontrol, apoteksregnskab mv.	Sundhedsstyrelsen og Statens Serum Institut.	19.838 virksomheder	532 brugere, heraf 522 interne brugere[1)] og 10 eksterne brugere.

1) Sundhedsstyrelsen har oplyst, at test- og systembrugere er medregnet i opgørelsen over interne brugere.

2) SKAT har oplyst, at kommunerne selv administrerer brugeradgange til de ansatte, som skal have læseadgang til 3S. Derfor kender SKAT ikke antallet af brugere i kommunerne.

3) Opgjort pr. 26. august 2014.

Note: Oplysninger om antal brugere og registrerede i systemet er opgjort i juni 2014.

Kilde: Rigsrevisionen på baggrund af oplysninger fra de undersøgte institutioner.

Det fremgår af tabel 1, at alle undersøgte systemer indeholder fortrolige oplysninger om personer og/eller virksomheder. Der er registreret oplysninger lige fra tidligere straffe i Kriminalregisteret over behandling for misbrug i Stofmisbrugerdatabasen til oplysninger om medlemskab af fagforening i SKATs register.

Danmarks Statistik har registreret oplysninger om alle personer med et cpr-nr. Arbejdsskadestyrelsen har registreret oplysninger om ca. 1 mio. personer i sit system. Omfanget af registrerede i et system kan give et billede af, hvor mange personer og virksomheder det kan berøre, hvis oplysninger i systemet skulle komme uvedkommende personer/virksomheder til kendskab. Antallet af brugere af et system fortæller, hvor mange personer der har adgang til oplysningerne. Systemerne i Rigspolitiet og Forsvarskommandoen har henholdsvis ca. 15.000 og ca. 12.000 brugere.

Forsvarsministeriet blev omorganiseret pr. 1. oktober 2014. Det betød bl.a., at Forsvarskommandoen blev nedlagt.

8. Undersøgelsen er baseret på skriftligt materiale, som er indhentet fra de 8 undersøgte institutioner. Det drejer sig bl.a. om informationssikkerhedspolitikker, retningslinjer for beskyttelse af oplysninger, oversigter over systemer med oplysninger om personoplysninger og virksomhedsoplysninger, databehandleraftaler og serviceaftaler med it-driftsleverandørerne. Vi har endvidere besøgt de 8 institutioner. Hver enkelt institution har modtaget en særskilt rapport om resultater, som institutionen har haft mulighed for at kommentere på. Institutionerne har endvidere haft et udkast til beretning i høring.

9. Som tidligere nævnt fører Datatilsynet tilsyn med, at institutionernes praksis i forhold til fortrolige personoplysninger lever op til persondataloven. Vi har derfor været i dialog med Datatilsynet for at sikre en ensartet udlægning af kravene i lovgivningen, som vi har lagt til grund, når vi har vurderet institutionernes måde at behandle fortrolige personoplysninger på. Datatilsynet er kort omtalt i denne undersøgelse i forhold til Datatilsynets tilsyn med de undersøgte systemer. Datatilsynet har ligeledes haft et udkast til beretning i høring.

Revisionen er udført i overensstemmelse med god offentlig revisionsskik, jf. boks 1.

BOKS 1. GOD OFFENTLIG REVISIONSSKIK

God offentlig revisionsskik er baseret på de grundlæggende revisionsprincipper i rigsrevisionernes internationale standarder (ISSAI 100-999).

Afgrænsning

10. It-revisionen er udført i perioden januar 2014 - maj 2014. Undersøgelsen giver derfor et billede af, hvordan institutionerne sikrede fortrolige oplysninger om personer og virksomheder i de undersøgte systemer i den pågældende periode.

Undersøgelsen omfatter udvalgte statslige institutioner og fokuserer på institutionernes ansvar for at beskytte fortrolige oplysninger om personer og virksomheder. Undersøgelsens resultater vedrører kun de undersøgte systemer. Baseret på erfaring fra andre it-revisioner er det dog Rigsrevisionens vurdering, at den manglende efterlevelse af sikkerhedsbekendtgørelsen kan gøre sig gældende for en større kreds af statslige institutioner.

Vejledning nr. 125 af 10. juli 2000 om anmeldelse i henhold til kapitel 12 i lov om behandling af personoplysninger (til den offentlige forvaltning)
Det fremgår bl.a. af pkt. 2.1.3 i vejledningen, hvilke oplysninger der anses for fortrolige, og hvilke oplysninger som utvivlsomt vil være fortrolige.

Alle de undersøgte systemer indeholder fortrolige oplysninger. Det afgørende for, om en oplysning skal anses for fortrolig, vil være en vurdering af, om oplysningen er af en sådan karakter, at den efter den almindelige opfattelse i samfundet bør kunne forlanges unddraget offentlighedens kendskab, jf. vejledning om anmeldelse. Oplysninger om personer i de undersøgte systemer er omfattet af de almindelige og generelle krav til beskyttelse i sikkerhedsbekendtgørelsens kap. 1 og 2 og de supplerende krav til sikkerhedsforanstaltninger i kap. 3. Vi har undersøgt institutionernes efterlevelse af udvalgte bestemmelser, og disse fremgår af hvert enkelt afsnit.

I forbindelse med høringssvarene har flere institutioner gjort opmærksom på, at de har planlagt eller allerede har iværksat flere initiativer, der imødekommer vores kritikpunkter. De fremadrettede initiativer fremgår af bilag 2, som også viser en oversigt over undersøgelsens resultater. Bilag 3 indeholder en ordliste, der forklarer udvalgte ord og begreber.

2. Institutionernes beskyttelse af fortrolige oplysninger

2.1. Institutionernes beskyttelse af fortrolige oplysninger om personer

11. Dette afsnit handler om, hvordan de statslige institutioner har beskyttet de fortrolige personoplysninger, der indgår i de undersøgte systemer.

Institutionernes retningslinjer for at sikre fortrolige personoplysninger
12. Det er vigtigt, at institutionerne har klarlagt, hvordan fortrolige oplysninger skal håndteres, og at retningslinjerne afspejler de faktiske forhold i institutionen. Vi har derfor undersøgt, om institutionerne har opdaterede retningslinjer for, hvordan institutionerne skal beskytte fortrolige oplysninger om personer. Boks 2 viser sikkerhedsbekendtgørelsens krav om retningslinjer.

BOKS 2. SIKKERHEDSBEKENDTGØRELSENS KRAV OM RETNINGSLINJER

Sikkerhedsbekendtgørelsens § 5, stk. 1 og 2:

- Den dataansvarlige myndighed skal fastsætte nærmere interne bestemmelser om sikkerhedsforanstaltninger i myndigheden til uddybning af de regler, der fremgår af bekendtgørelsen. Bestemmelserne skal navnlig omfatte organisatoriske forhold og fysisk sikring, herunder sikkerhedsorganisation, administration af adgangskontrolordninger og autorisationsordninger samt kontrol med autorisationer. Der skal endvidere fastsættes instrukser, som fastlægger ansvaret for og beskriver behandling og destruktion af ind- og uddatamateriale samt anvendelse af edb-udstyr.
- De interne bestemmelser skal gennemgås mindst én gang hvert år med henblik på at sikre, at de er fyldestgørende og afspejler de faktiske forhold i myndigheden.

13. Vi har gennemgået de interne retningslinjer, instrukser, sikkerhedshåndbøger mv., som institutionerne har udarbejdet, for nærmere at uddybe sikkerhedsbekendtgørelsens bestemmelser.

Tabel 2 viser, hvilke institutioner der har udarbejdet retningslinjer for at sikre fortrolige personoplysninger, og om retningslinjerne er opdaterede.

Tabel 2. Retningslinjer for at sikre fortrolige personoplysninger i de undersøgte institutioner

	Arbejdsskadestyrelsen	Institut for Menneskerettigheder	Danmarks Statistik	Forsvarskommandoen	Rigspolitiet	SKAT	Socialstyrelsen	Sundhedsstyrelsen
Er der retningslinjer for at sikre personoplysninger?	●	●	●	●	●	●	●	●
Er retningslinjerne opdateret årligt?	●	●	●	●	●	●	●	●

● Ikke tilfredsstillende, da der forekommer væsentlige mangler.
● Delvist tilfredsstillende.
● Tilfredsstillende, men mindre mangler kan forekomme.

Kilde: Rigsrevisionen.

Det fremgår af tabel 2, at 5 ud af 8 institutioner (Arbejdsskadestyrelsen, Danmarks Statistik, Forsvarskommandoen, Rigspolitiet og SKAT) havde retningslinjer for at sikre grundlaget for at beskytte fortrolige oplysninger om personer. Institut for Menneskerettigheder havde ikke 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. Det gjaldt fx retningslinjer for adgangsstyring, logning og overvågning. Gennemgangen viser, at der fx var retningslinjer, der senest var opdateret i 2009. Da der ofte forekommer tekniske og organisatoriske ændringer, medfører den manglende opdatering, at sikkerheden kan være utilstrækkelig, da retningslinjerne ikke nødvendigvis afspejler de faktiske forhold i institutionen.

Institutionernes sikring af fortrolige personoplysninger i praksis

14. Vi har undersøgt, hvordan institutionerne beskytter fortrolige personoplysninger i praksis, så risikoen for, at fortrolige oplysninger kommer uvedkommende til kendskab, mindskes. Konkret har vi undersøgt, om institutionerne kontrollerer medarbejdernes adgang til fortrolige personoplysninger, om institutionerne kontrollerer afviste adgangsforsøg, om institutionerne registrerer medarbejdernes opslag i systemerne, om institutionerne har indgået aftaler med eksterne databehandlere om behandling af fortrolige oplysninger, og om institutionerne fører tilsyn med deres sikkerhedsforanstaltninger. De undersøgte punkter fremgår alle af sikkerhedsbekendtgørelsen.

Persondatalovens kap. 11 indeholder en række bestemmelser om, hvilke sikkerhedsforanstaltninger der skal træffes i forbindelse med behandling af personoplysninger.

Det følger bl.a. af disse regler (§ 41, stk. 3), at den dataansvarlige skal træffe de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger mod, at oplysninger hændeligt eller ulovligt tilintetgøres, fortabes eller forringes, og mod, at de kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med loven. Det samme gælder for de såkaldte databehandlere. Reglerne er nærmere fastsat i sikkerhedsbekendtgørelsen.

Institutionernes kontrol af medarbejdernes adgang til fortrolige personoplysninger
15. Institutionerne må kun give medarbejdere adgang til fortrolige personoplysninger, hvis de skal bruge oplysningerne til at løse deres arbejdsopgaver. Samtidig skal institutionerne løbende kontrollere, at medarbejdernes adgange fortsat er relevante. Boks 3 viser sikkerhedsbekendtgørelsens krav om brugeradgange og kontrol heraf.

BOKS 3. SIKKERHEDSBEKENDTGØRELSENS KRAV OM BRUGERADGANGE OG KONTROL HERAF

Sikkerhedsbekendtgørelsens § 11, stk. 2, og § 17, stk. 1 og 2:

- Der må kun autoriseres personer, der er beskæftiget med de formål, hvortil personoplysningerne behandles. De enkelte brugere må ikke autoriseres til anvendelser, som de ikke har behov for.
- Det skal sikres, at de autoriserede personer fortsat opfylder betingelserne.
- Kontrol heraf skal foretages mindst én gang hvert halve år.

Vi har bl.a. gennemgået institutionernes retningslinjer for at autorisere medarbejderne, ledelsernes godkendelser af de oprettede brugere og dokumentation for institutionernes senest udførte kontroller af brugernes rettigheder til adgang i systemerne.

Vores gennemgang viser, at alle 8 undersøgte institutioner har defineret, hvilke brugere der må have adgang, og har godkendt de pågældendes autorisationer. Institutionerne ved altså, hvilke systemer og dermed hvilke oplysninger de har givet medarbejderne adgang til. Arbejdsskadestyrelsen og Danmarks Statistik manglede dog dokumentation for, at de oprindelige autorisationer til systemerne var godkendt. Danmarks Statistik har oplyst, at der ikke er dokumentation for, at de oprettede brugeradgange før 2011 er godkendt. Efter 2011 er oprettelser dokumenteret i en digital løsning. Tabel 3 viser institutionernes kontrol af brugernes adgang i de undersøgte systemer.

Tabel 3. Kontrol af brugernes adgang i de undersøgte systemer

	Arbejds-skade-styrelsen	Institut for Menneske-rettigheder	Danmarks Statistik	Forsvars-kommando-en	Rigspolitiet	SKAT	Social-styrelsen	Sundheds-styrelsen
Kontrolleres brugeradgange halvårligt?	●	●	●	●	●	●	●	●

● Ikke tilfredsstillende, da der forekommer væsentlige mangler.
● Delvist tilfredsstillende.
● Tilfredsstillende, men mindre mangler kan forekomme.

Kilde: Rigsrevisionen.

Det fremgår af tabel 3, at 2 ud af de 8 institutioner (Danmarks Statistik og Forsvarskommandoen) har kontrolleret, at brugerne stadig havde et arbejdsbetinget behov for at have adgang til systemerne. Kontrollen var udført halvårligt, som de skal ifølge sikkerhedsbekendtgørelsen.

6 institutioner (Arbejdsskadestyrelsen, Institut for Menneskerettigheder, Rigspolitiet, SKAT, Socialstyrelsen og Sundhedsstyrelsen) har ikke udført en halvårlig kontrol. Rigspolitiet har udført kontrollen årligt. SKAT har udført en halvårlig kontrol, men vores gennemgang viser, at kontrollen ikke var effektiv, da flere medarbejdere havde adgang til oplysninger, som de ikke havde et arbejdsbetinget behov for.

Institutionernes kontrol af afviste forsøg på at få adgang til fortrolige personoplysninger

16. Institutionerne skal følge op på, om der er gentagne forsøg på at få adgang til systemer, der indeholder fortrolige personoplysninger. Hvis der er det, kan det tyde på, at der er nogle, der prøver at skaffe sig uretmæssig adgang til systemets oplysninger. Boks 4 viser sikkerhedsbekendtgørelsens krav om kontrol af afviste adgangsforsøg.

BOKS 4. SIKKERHEDSBEKENDTGØRELSENS KRAV OM KONTROL AF AFVISTE ADGANGSFORSØG

Sikkerhedsbekendtgørelsens § 18:

- Der skal foretages registrering af alle afviste adgangsforsøg. Hvis der inden for en fastsat periode er registreret et nærmere fastsat antal på hinanden følgende afviste adgangsforsøg fra samme arbejdsstation eller med samme brugeridentifikation, skal der blokeres for yderligere forsøg. Der skal løbende ske opfølgning i myndigheden.

Vi har gennemgået institutionernes logfiler. Tabel 4 viser, om institutionerne har registreret afviste forsøg på at få adgang til systemerne, og om de har ført kontrol med de afviste forsøg.

Tabel 4. Kontrol af afviste forsøg på at få adgang til de undersøgte systemer

	Arbejdsskadestyrelsen	Institut for Menneskerettigheder	Danmarks Statistik	Forsvarskommandoen	Rigspolitiet	SKAT	Socialstyrelsen	Sundhedsstyrelsen
Registreres afviste adgangsforsøg?	🟢	🟢	🟢	🟢	🟢	🟢	🔴	🟢
Følges der op på afviste adgangsforsøg?	🟡	🟢	🟢	🟢	🟢	🟡	🔴	🟡

🔴 Ikke tilfredsstillende, da der forekommer væsentlige mangler.
🟡 Delvist tilfredsstillende.
🟢 Tilfredsstillende, men mindre mangler kan forekomme.

Kilde: Rigsrevisionen.

Det fremgår af tabel 4, at 7 ud af 8 institutioner har registreret afviste forsøg på at få adgang til de undersøgte systemer. Socialstyrelsen har ikke registreret de afviste forsøg.

4 ud af de 7 institutioner (Institut for Menneskerettigheder, Danmarks Statistik, Forsvarskommandoen og Rigspolitiet), der har registreret afviste forsøg, har regelmæssigt fulgt op på, om der har været afviste forsøg på at få adgang til de undersøgte systemer. 3 institutioner (Arbejdsskadestyrelsen, SKAT og Sundhedsstyrelsen) har ikke har fulgt op på de afviste forsøg. Systemerne er dog sat op til, at adgangen låses efter 3-5 forgæves forsøg (afhængigt af institution).

Institutionernes registrering af medarbejdernes opslag i systemerne
17. Institutionerne skal kunne spore, hvilke medarbejdere der har søgt på oplysningerne i systemerne. Derfor skal institutionerne registrere medarbejdernes opslag på enkeltpersoner. Boks 5 viser sikkerhedsbekendtgørelsens krav om registrering af opslag på enkeltpersoner.

BOKS 5. SIKKERHEDSBEKENDTGØRELSENS KRAV OM REGISTRERING AF OPSLAG PÅ ENKELTPERSONER

Sikkerhedsbekendtgørelsens § 19, stk. 1:

- Der skal foretages maskinel registrering (logning) af alle anvendelser af personoplysninger. Registreringen skal mindst indeholde oplysning om tidspunkt, bruger, type af anvendelse og angivelse af den person, de anvendte oplysninger vedrørte, eller det anvendte søgekriterium. Loggen skal opbevares i 6 måneder, hvorefter den skal slettes. Myndigheder med et særligt behov kan opbevare loggen i op til 5 år.

Vi har gennemgået institutionernes logfiler og dokumentation for, at de har registreret medarbejdernes opslag på enkeltpersoner. Tabel 5 viser, om institutionerne har registreret medarbejdernes opslag på enkeltpersoner i de undersøgte systemer, og om de sletter dem igen.

Tabel 5. Registrering af medarbejdernes opslag på enkeltpersoner i de undersøgte systemer

	Arbejdsskadestyrelsen	Institut for Menneskerettigheder	Danmarks Statistik	Forsvarskommandoen	Rigspolitiet	SKAT	Socialstyrelsen	Sundhedsstyrelsen
Registreres medarbejdernes opslag på enkeltpersoner?	●	●	●	●	●	●	●	●
Slettes logregistreringerne?	●	●	●	●	●	●	●	●

● Ikke tilfredsstillende, da der forekommer væsentlige mangler.
● Delvist tilfredsstillende.
● Tilfredsstillende, men mindre mangler kan forekomme.

Kilde: Rigsrevisionen.

Det fremgår af tabel 5, at 6 ud af 8 institutioner har registreret medarbejdernes opslag på enkeltpersoner, som de skal ifølge sikkerhedsbekendtgørelsen, fx oplysninger om, hvordan og hvornår medarbejderen har anvendt hvilke oplysninger. Institut for Menneskerettigheder og Danmarks Statistik har ikke registreret disse oplysninger.

Ud af de 6 institutioner, der har registreret opslag på enkeltpersoner i en log, er det kun Arbejdsskadestyrelsen, som har slettet registreringerne efter ½ år, som de skal ifølge sikkerhedsbekendtgørelsen, medmindre der er et særligt behov for at forlænge perioden. 5 af de 6 institutioner har ikke slettet registreringerne igen. Heraf har Rigspolitiet og SKAT udvidet perioden for at opbevare registreringerne, men de har ikke slettet registreringerne efter den udvidede periodes afslutning.

***Danmarks Statistik** har en koordinerende funktion med at indsamle og bearbejde statistiske oplysninger hos andre offentlige myndigheder. For at samle den officielle statistikproduktion i Danmarks Statistik har styrelsen løbende overtaget ansvaret for statistikker, der tidligere blev udarbejdet af andre myndigheder, fx forsknings-, udviklings-, innovations-, valg-, kirke- og kulturstatistikkerne.*

18. Én af de institutioner, der ikke har registreret medarbejdernes opslag på enkeltpersoner, er Danmarks Statistik. Boks 6 viser eksempler på, hvilke personoplysninger Danmarks Statistik er i besiddelse af.

BOKS 6. DANMARKS STATISTIKS OPLYSNINGER OM PERSONER

Danmarks Statistik er oprettet ved lov og er den centrale danske myndighed, der indsamler, bearbejder og offentliggør statistiske oplysninger om samfundsforhold. Danmarks Statistik er i besiddelse af en række personoplysninger, fx oplysninger om fødsel og adoption, fertilitet, familieoplysninger (husstand, indkomst, skilsmisser mv.), boligforhold, trafikuheld, kriminalitet, domme, fængselsophold, sociale ydelser, folke- og førtidspension, sygehusbenyttelse, lægebesøg, indvandrere og deres efterkommere samt asylansøgninger og opholdstilladelser. Registreringen omfatter alle personer i Danmark, inkl. afdøde, tilbage til indførelsen af cpr-nr.

Kilde: Rigsrevisionen på baggrund af tidligere it-revisioner og Danmarks Statistiks hjemmeside.

Rigsrevisionen har ved en tidligere revision i 2011 konstateret, at Danmarks Statistik ikke umiddelbart registrerede medarbejdernes opslag efter sikkerhedsbekendtgørelsens § 19, stk. 1. I praksis kunne det betyde, at Danmarks Statistik ikke ville kunne spore, om der var foretaget et opslag, eller hvem der eventuelt havde foretaget opslaget, i tilfælde af lækkede fortrolige personoplysninger.

Rigsrevisionen vurderede, at det kunne være meget problematisk, hvis personoplysninger blev lækket, og Danmarks Statistik ikke efterfølgende kunne redegøre for, om en medarbejder var involveret. Ifølge Danmarks Statistik var de imidlertid omfattet af en undtagelsesbestemmelse i sikkerhedsbekendtgørelsen. Rigsrevisionen anbefalede Danmarks Statistik at forelægge sagen for Datatilsynet.

Rigsrevisionen fremsendte revisionsrapporten til Danmarks Statistik i juni 2011. På et møde mellem Danmarks Statistik og Datatilsynet blev Datatilsynet gjort bekendt med, at der forelå en it-revisionsrapport fra Rigsrevisionen, som satte spørgsmålstegn ved, om sikkerhedsbekendtgørelsen var opfyldt. Danmarks Statistik sendte ikke rapporten til Datatilsynet. Rigsrevisionen rykkede i juli 2012 Danmarks Statistik for status i sagen. Danmarks Statistik oplyste, at sagen var afklaret med Datatilsynet, som ikke havde bemærkninger til Danmarks Statistiks praksis. Rigsrevisionen rettede henvendelse til Datatilsynet i november 2012 for at få uddybet begrundelsen for Datatilsynets konklusion. Datatilsynet oplyste, at Datatilsynet ikke havde fået forelagt problemstillingen, som den var omtalt i revisionsrapporten. Datatilsynet havde derfor ikke taget stilling til, om Danmarks Statistik loggede i overensstemmelse med sikkerhedsbekendtgørelsens bestemmelse.

Danmarks Statistik forelagde herefter sagen for Datatilsynet primo 2013. Datatilsynet har herefter holdt møde med Danmarks Statistik og har indhentet Danmarks Statistiks udtalelse i sagen. Datatilsynet har endvidere indhentet oplysninger fra datatilsynene i Norge, Sverige og Finland, Den Europæiske Tilsynsførende for Databeskyttelse og flere offentlige forskningsinstitutioner i Danmark.

Efter behandling af sagen i Datarådet vurderede Datatilsynet i juli 2014, at kravet i sikkerhedsbekendtgørelsens § 19, stk. 1, om logning gælder for Danmarks Statistik, der således ikke er omfattet af undtagelsesbestemmelser i sikkerhedsbekendtgørelsen. Efter Datatilsynets opfattelse anses logning for vigtig for at undgå uberettiget brug af persondata – både præventivt, men også bagudrettet, så det kan spores, hvem der måtte have foretaget et uberettiget opslag. Ifølge Datatilsynet gør det sig også gældende for Danmarks Statistik, hvor det som følge af institutionens særlige rolle vil være muligt at fremsøge oplysninger – herunder fortrolige oplysninger – om enhver person i Danmark.

Datatilsynet henstillede, at Danmarks Statistik tog skridt til at indrette sin behandling af personoplysninger, så sikkerhedsbekendtgørelsens krav blev opfyldt. Datatilsynet og Danmarks Statistik er fortsat i dialog om sagen.

Institutionernes aftaler med databehandlerne

19. 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. Boks 7 viser persondatalovens og sikkerhedsbekendtgørelsens krav om aftaler med databehandlere.

Databehandleraftale
Når en dataansvarlig overlader en behandling af oplysninger til en databehandler, kræver det, at der indgås en skriftlig aftale mellem den dataansvarlige og databehandleren – en såkaldt databehandleraftale. Det skal fremgå af aftalen, at databehandleren kun handler efter instruks fra den dataansvarlige, og at databehandleren skal træffe forskellige tekniske og organisatoriske sikkerhedsforanstaltninger.

BOKS 7. PERSONDATALOVENS OG SIKKERHEDSBEKENDTGØRELSENS KRAV OM AFTALER MED DATABEHANDLERE

Persondatalovens § 42:

- Når en dataansvarlig overlader en behandling af oplysninger til en databehandler, skal den dataansvarlige sikre sig, at databehandleren kan træffe de i § 41, stk. 3-5, nævnte tekniske og organisatoriske sikkerhedsforanstaltninger, og påse, at dette sker.

Sikkerhedsbekendtgørelsens § 7:

- 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.

Vi har gennemgået institutionernes aftaler med databehandlerne vedrørende de undersøgte systemer, revisorerklæringer samt referater fra møder med de eksterne databehandlere. Institut for Menneskerettigheder har egen it-drift og er derfor ikke omfattet af dette punkt.

Tabel 6 viser, hvilke institutioner der har en skriftlig aftale med databehandlerne om de undersøgte systemer, og om institutionerne følger op på aftalerne.

Tabel 6. Databehandleraftaler om de undersøgte systemer

	Arbejdsskadestyrelsen	Danmarks Statistik	Forsvarskommandoen	Rigspolitiet	SKAT	Socialstyrelsen	Sundhedsstyrelsen
Er der en aftale med databehandleren?	●	●	●	●	●	●	●
Følges der op på databehandleraftalen?	●	●	●	●	●	●	●

● Ikke tilfredsstillende, da der forekommer væsentlige mangler.
● Delvist tilfredsstillende.
● Tilfredsstillende, men mindre mangler kan forekomme.

Kilde: Rigsrevisionen.

Det fremgår af tabel 6, at 5 ud af 7 institutioner (Arbejdsskadestyrelsen, Danmarks Statistik, Forsvarskommandoen, Rigspolitiet og Sundhedsstyrelsen) har indgået en skriftlig aftale med databehandlerne, der indeholder aftale om organisatoriske og tekniske sikkerhedsforanstaltninger vedrørende behandling af fortrolige personoplysninger.

SKAT og Socialstyrelsen har ikke indgået en skriftlig aftale med databehandlerne. Fraværet af en sådan aftale betyder, at institutionerne ikke har pålagt databehandleren instruktioner i forhold til at behandle fortrolige personoplysninger. SKAT har oplyst, at SKAT i juni 2014 har indgået en aftale med databehandleren.

Institutionen skal følge op på aftalen med databehandleren. Hvis institutionen ikke indhenter en specifik revisorerklæring, skal institutionen selv efterprøve, om databehandlerens sikkerhedsforanstaltninger lever op til de aftalte niveauer.

20. Institutionerne skal følge op på, om de indgåede aftaler overholdes. Institutionerne kan vælge at lade en ekstern revisor følge op på, om databehandlerne har overholdt de aftalte sikkerhedsforanstaltninger. I givet fald bør revisorerklæringen udformes, så det specifikt fremgår, at erklæringen omfatter de fortrolige personoplysninger, som databehandleren behandler for den dataansvarlige.

Det er kun Forsvarskommandoen, der har fulgt op på den indgåede aftale, idet institutionen har indhentet en specifik revisorerklæring, som omfatter fortrolige personoplysninger i det undersøgte system.

4 ud af de 5 institutioner, der har indgået en aftale med databehandleren, har ikke fulgt op på aftalen, som de skal ifølge persondataloven. Når en institution ikke følger op på, om aftalen overholdes, så ved institutionen ikke, hvordan de fortrolige personoplysninger beskyttes, hvem der læser dem, om de kopieres, eller om de videreføres til andre.

Arbejdsskadestyrelsen og Danmarks Statistik har hverken indhentet en revisorerklæring eller selv fulgt op på, om databehandlerne har efterlevet de aftalte sikkerhedsforanstaltninger. Rigspolitiet og Sundhedsstyrelsen har hver indhentet en revisorerklæring, der handler om institutionernes regnskabsførelse generelt. De indhentede erklæringer er ikke specifikt rettet mod sikkerhedsforanstaltninger i de pågældende systemer og omfatter ikke fortrolige personoplysninger. Rigsrevisionen finder derfor, at erklæringerne hos Rigspolitiet og Sundhedsstyrelsen ikke kan opfylde persondatalovens krav om opfølgning, da erklæringerne ikke har til formål at kontrollere, om persondataloven overholdes.

SKAT og Socialstyrelsen, der på undersøgelsestidspunktet ikke havde indgået en skriftlig aftale med databehandlerne, har i sagens natur ikke kunnet følge op på aftalens indhold. Socialstyrelsen har indhentet en generel revisorerklæring, som ikke er specifikt rettet mod sikkerhedsforanstaltninger i det undersøgte system.

Institutionernes eget tilsyn med sikkerhedsforanstaltninger

21. Institutionerne skal føre tilsyn med, at de sikkerhedsforanstaltninger, som de har fastlagt internt i institutionen, rent faktisk efterleves. Boks 8 viser sikkerhedsbekendtgørelsens krav om institutionernes eget tilsyn med sikkerhedsforanstaltninger.

BOKS 8. SIKKERHEDSBEKENDTGØRELSENS KRAV OM INSTITUTIONERNES EGET TILSYN MED SIKKERHEDSFORANSTALTNINGER

Sikkerhedsbekendtgørelsens § 5, stk. 1:

- Den dataansvarlige myndighed skal fastsætte retningslinjer for myndighedens tilsyn med overholdelsen af de sikkerhedsforanstaltninger, der er fastsat for myndigheden.

Bestemmelsen i sikkerhedsbekendtgørelsen er ikke uddybet, og det er således op til institutionerne at fastlægge det nærmere indhold af tilsynet, dvs. at de skal have taget stilling til, hvordan kontrollen skal tilrettelægges, fx omfanget og hyppigheden, samt dokumentation for kontrollen. Vi har gennemgået institutionernes retningslinjer for tilsyn og dokumentation for, om tilsynet blev udført. Resultatet er vist i tabel 7.

Tabel 7. Institutionernes eget tilsyn med sikkerhedsforanstaltninger

	Arbejdsskadestyrelsen	Institut for Menneskerettigheder	Danmarks Statistik	Forsvarskommandoen	Rigspolitiet	SKAT	Socialstyrelsen	Sundhedsstyrelsen
Er der retningslinjer for tilsyn?	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴
Føres der tilsyn med sikkerhedsforanstaltningerne?	🔴	🔴	🔴	🟢	🔴	🟡	🔴	🟡

🔴 Ikke tilfredsstillende, da der forekommer væsentlige mangler.
🟡 Delvist tilfredsstillende.
🟢 Tilfredsstillende, men mindre mangler kan forekomme.

Kilde: Rigsrevisionen.

Det fremgår af tabel 7, at det kun er Forsvarskommandoen, som har udarbejdet retningslinjer for eget tilsyn med at overholde sikkerhedsforanstaltningerne, og som har udført et regelmæssigt tilsyn med, at retningslinjerne blev overholdt.

7 ud af de 8 institutioner har ingen retningslinjer for, hvordan eget tilsyn skal udføres, og institutionerne har derfor heller ikke kunnet udføre et tilsyn i overensstemmelse med retningslinjerne. Vores gennemgang viser dog, at SKAT og Sundhedsstyrelsen har udført en delvis kontrol af sikkerhedsforanstaltningerne. SKAT udfører bl.a. intern revision af udvalgte sikkerhedsforanstaltninger. Sundhedsstyrelsen har udført en kontrol af udvalgte punkter i sikkerhedsbekendtgørelsen i forbindelse med styrelsens akkrediteringsordning.

Resultater

22. Undersøgelsen viser, at ingen af de undersøgte institutioner inden for det seneste år har gennemgået og vurderet deres retningslinjer for sikkerhedsforanstaltninger. Da der ofte forekommer tekniske og organisatoriske ændringer, medfører den manglende opdatering, at sikkerheden kan være utilstrækkelig, da retningslinjerne ikke nødvendigvis afspejler de faktiske forhold i institutionen.

6 af de undersøgte institutioner har ikke sikret, at medarbejdernes adgange er opdaterede. Det betyder, at en medarbejders adgang til fortrolige personoplysninger ikke nødvendigvis bliver lukket, hvis medarbejderen skifter arbejdsområde og ikke længere har brug for adgangen. Dermed er der ikke sikkerhed for, at det kun er personer med et arbejdsbetinget behov, som har adgang til fortrolige oplysninger om personer.

Socialstyrelsen har ikke registreret afviste adgangsforsøg i det undersøgte system.

Institut for Menneskerettigheder og Danmarks Statistik har ikke registreret medarbejdernes opslag på enkeltpersoner og kan således ikke spore, hvilken medarbejder der i givet fald uberettiget har læst de fortrolige personoplysninger. Rigsrevisionen konstaterede allerede i 2011, at Danmarks Statistik ikke umiddelbart registrerede medarbejdernes opslag efter sikkerhedsbekendtgørelsens bestemmelser. Datatilsynet vurderede i juli 2014, at kravet om at logge gælder for Danmarks Statistik. Datatilsynet henstillede, at Danmarks Statistik tog skridt til at indrette sin behandling af personoplysninger, så sikkerhedsbekendtgørelsens krav blev opfyldt. Datatilsynet og Danmarks Statistik er fortsat i dialog om sagen. Rigsrevisionen finder det ikke tilfredsstillende, at Danmarks Statistik ikke har sørget for, at så vigtig en sag blev afklaret hurtigere.

5 ud af de 6 undersøgte institutioner, der registrerer opslag på enkeltpersoner, har ikke slettet registreringerne igen efter en nærmere fastsat periode, som sikkerhedsbekendtgørelsen foreskriver.

SKAT og Socialstyrelsen har overladt behandlingen af fortrolige personoplysninger til eksterne databehandlere uden at indgå en aftale om sikkerhedsniveauet hos databehandleren, som de skal ifølge sikkerhedsbekendtgørelsen.

7 ud af de 8 undersøgte institutioner har ikke tilrettelagt og udført et tilsyn med, at sikkerhedsforanstaltningerne bliver overholdt.

Samlet set er der ingen af de undersøgte institutioner, der efterlever alle de krav til behandling af fortrolige personoplysninger, som fremgår af sikkerhedsbekendtgørelsen, og som er en uddybning af persondatalovens bestemmelser. Danmarks Statistik, Rigspolitiet og SKAT, der er vant til at håndtere store mængder fortrolige personoplysninger, efterlever på flere punkter ikke de krav, som fremgår af sikkerhedsbekendtgørelsen. Forsvarskommandoen er den af de undersøgte institutioner, der bedst beskytter de fortrolige oplysninger.

Datatilsynets tilsyn med statslige institutioner
23. Datatilsynet fører som en af sine opgaver tilsyn med, at offentlige myndigheder og private virksomheder behandler fortrolige oplysninger om personer i overensstemmelse med persondataloven og regler udstedt i medfør af loven. Datatilsynet er finanslovsmæssigt og personalemæssigt tilknyttet Justitsministeriet, men udøver sine funktioner i fuld uafhængighed.

Der er i alt 175 statslige institutioner at føre tilsyn med. Det er Rigsrevisionens erfaring, at de fleste statslige institutioner har en berøringsflade til persondataloven – enten som dataansvarlig eller som databehandler. Datatilsynet fører tilsyn med, at persondatalovens regler overholdes. Datatilsynet udfører tilsynet ved at tage på inspektioner, behandle klager og tage sager op af egen drift. Datatilsynet behandler endvidere anmeldelser fra statslige institutioner, som gerne vil behandle fortrolige oplysninger om personer. Datatilsynet behandler konkrete klager fra borgere, yder rådgivning og vejledning og udtaler sig i forbindelse med høringer af love, bekendtgørelser mv.

Datatilsynets tilsyn med institutioners behandling af personoplysninger har karakter af et legalitetstilsyn, jf. svar på spørgsmål nr. 957 til Folketingets Retsudvalg af 6. januar 2014. Det betyder, at Datatilsynet har fokus på, at behandlingen af personoplysninger er i overensstemmelse med reglerne i persondataloven og eventuelt anden relevant lovgivning, og at reglerne om registreredes rettigheder overholdes. I forhold til datasikkerhed stiller Datatilsynet spørgsmål inden for de emner, som fremgår af sikkerhedsbekendtgørelsen. Det kan vedrøre institutionernes uddybende sikkerhedsregler eller mere specifikke sikkerhedsforanstaltninger. Datatilsynet foretager ikke en mere omfattende it-revision eller en fuldstændig gennemgang af de etablerede sikkerhedsforanstaltninger.

Som led i Datatilsynets inspektionsstrategi for 2013-2015 har Datatilsynet udvalgt 6 kategorier, hvor der er særligt behov for regelmæssigt tilsyn. Inspektionerne vil primært ske inden for disse kategorier, men valget udelukker ikke, at Datatilsynet også kan inspicere andre institutioner og virksomheder. De 6 kategorier er lokale politiembeder og Rigspolitiet, kommuner, sygehuse og sundhedsdatabaser, kreditoplysningsbureauer og advarselsregistre, privat og offentlig forskning samt tv-overvågning.

Det fremgår af svar på spørgsmål nr. 957 til Folketingets Retsudvalg af 6. januar 2014, at Datatilsynet bl.a. har gennemført ca. 160 inspektioner i statslige institutioner siden 2000. Det fremgår af Datatilsynets oversigt over udførte inspektioner i 2013, at Datatilsynet i 2013 udførte 7 inspektioner i statslige institutioner. Det fremgår endvidere af svar på spørgsmål nr. 361 til Folketingets Retsudvalg af 18. marts 2014, at der ud fra Datatilsynets skøn er brugt ca. 2 årsværk pr. år på inspektionsbesøg og andre inspektioner.

Datatilsynet har på Rigsrevisionens forespørgsel oplyst, at Datatilsynet ikke har udført inspektioner vedrørende de 8 undersøgte systemer de seneste 3 år.

2.2. Institutionernes beskyttelse af fortrolige oplysninger om virksomheder

24. Dette afsnit handler om, hvordan de statslige institutioner har beskyttet de fortrolige oplysninger om virksomheder, der indgår i de undersøgte systemer.

Der findes ikke en tilsvarende lov, der beskytter fortrolige oplysninger om private virksomheder, som det gør sig gældende for fortrolige personoplysninger, men krav til beskyttelse af oplysninger kan i nogle tilfælde være omfattet af særlovgivning. Det betyder ikke, at fortrolige oplysninger om virksomheder ikke bør beskyttes.

Private virksomheder har ikke noget valg i forhold til, om de vil aflevere oplysninger til statslige institutioner, da indsamlingen sker som led i en myndighedsopgave. Ofte er oplysningerne væsentlige for virksomhedens konkurrencesituation og måske endda for virksomhedens fortsatte overlevelse. Derfor har virksomhederne en rimelig forventning om, at de statslige institutioner beskytter de indsamlede oplysninger tilstrækkeligt.

Statslige institutioner har fra januar 2014 skullet tilrettelægge deres styring af informationssikkerheden efter sikkerhedsstandarden ISO 27001 som erstatning for sikkerhedsstandarden DS 484. Institutionerne skal etablere sikkerhedsforanstaltninger vedrørende private virksomheders fortrolige oplysninger på en måde, som er tilstrækkelig og dækkende i forhold til oplysningernes følsomhed og betydning. Der er stort sammenfald mellem kravene i persondataloven og bedste praksis for beskyttelse af visse virksomhedsoplysninger i standarderne.

25. Vi har gennemgået 3 systemer, der indeholder fortrolige oplysninger om virksomheder. Vi har undersøgt institutionernes praksis ud fra kriterier i informationssikkerhedsstandarden ISO 27001. Resultaterne er vist i tabel 8.

Tabel 8. Institutionernes beskyttelse af fortrolige oplysninger om virksomheder i de undersøgte systemer

	SKAT	Socialstyrelsen	Sundhedsstyrelsen
Er der opdaterede retningslinjer på de undersøgte områder?	●	●	●
Er der godkendte brugeradgange?	●	●	●
Vurderes brugeradgange løbende med afsæt i arbejdsbetingede behov?	●	●	●
Registreres medarbejdernes opslag og ændringer i data?	●	●	●
Er der en aftale med databehandleren?	●	●	●
Følges der op på aftalen med databehandleren?	●	●[1)]	●
Er der en opdateret risikovurdering?	●	●	●

● Ikke tilfredsstillende, da der forekommer væsentlige mangler.
● Delvist tilfredsstillende.
● Tilfredsstillende, men mindre mangler kan forekomme.

[1)] Socialstyrelsen modtager en revisorerklæring.

Kilde: Rigsrevisionen.

Det fremgår af tabel 8, at ingen af de 3 institutioner har opdaterede retningslinjer på de undersøgte områder. Det skyldes, at ingen af de interne retningslinjer var blevet opdateret inden for det seneste år. Rigsrevisionen anser det for god praksis, at institutionerne årligt opdaterer deres retningslinjer for at sikre fortrolige virksomhedsoplysninger.

Alle 3 institutioner har fulgt en procedure for at oprette brugere, som sikrer, at det kun er de brugere, som har et arbejdsbetinget behov til systemet, der får adgang til fortrolige virksomhedsoplysninger. Ingen af institutionerne har dog gennemgået rettighederne med et passende interval. Det betyder, at der er risiko for, at medarbejdere, som én gang har fået en rettighed, ikke fratages den igen, når det arbejdsbetingede behov eventuelt ophører.

Medarbejdernes opslag og ændringer i oplysninger registreres i tilstrækkeligt omfang i alle 3 systemer.

Kun Sundhedsstyrelsen har indgået en aftale med databehandleren om sikkerhed mv., selv om alle 3 institutioner benytter en databehandler. Sundhedsstyrelsen følger også op på aftalen ved at indhente en revisorerklæring. Socialstyrelsen modtager en revisorerklæring, selv om styrelsen ikke har en aftale om sikkerhedsniveau mv. SKAT har efterfølgende oplyst, at SKAT har indgået en aftale med databehandleren.

Socialstyrelsen og Sundhedsstyrelsen har ikke en opdateret risikovurdering for de undersøgte systemer. En risikoanalyse er et centralt redskab, når institutionen skal vurdere, hvilket sikkerhedsniveau institutionen skal etablere i forhold til et it-system.

Resultater

26. Undersøgelsen viser, at ingen af institutionerne kontrollerer, om medarbejdernes adgange til de undersøgte systemer stadig er relevante for at kunne løse deres arbejdsopgaver. Kun Sundhedsstyrelsen har indgået en aftale med den eksterne databehandler om sikker behandling af fortrolige virksomhedsoplysninger. Socialstyrelsen og Sundhedsstyrelsen har ikke en opdateret risikoanalyse.

Det er Rigsrevisionens vurdering, at de undersøgte institutioner ikke i tilstrækkeligt omfang beskytter fortrolige oplysninger om virksomheder. Alle 3 institutioner bør derfor forbedre sikkerheden omkring de fortrolige oplysninger, som de behandler om private virksomheder.

Rigsrevisionen, den 5. november 2014

Lone Strøm

/Peder Juhl Madsen

Bilag 1. Metode

Udvælgelse af institutioner og systemer
Undersøgelsen er baseret på it-revisioner udført som led i årsrevisionen. I forbindelse med årsrevisionen udvælger vi primært it-systemer til revision efter væsentlighed og risiko. Vi prioriterer også at udvælge mindre it-systemer for at kunne vurdere systemerne bredt. Vi har derfor udvalgt både små og store institutioner, der behandler fortrolige person- og virksomhedsoplysninger i it-systemer. Vi har også udvalgt it-systemer, der både har få og mange brugere af systemerne, og it-systemer, der har registreret få og mange personer/virksomheder.

Undersøgelsen omfatter 8 statslige institutioner, som er udvalgt, fordi de alle behandler fortrolige oplysninger om personer og/eller virksomheder. Vi har undersøgt 8 systemer, som indeholder fortrolige oplysninger om personer, og 3 systemer, som indeholder fortrolige oplysninger om virksomheder.

Undersøgelsens revisionskriterier
Undersøgelsens revisionskriterier er baseret på persondataloven og sikkerhedsbekendtgørelsen for så vidt angår institutionernes beskyttelse af fortrolige personoplysninger. Da der ikke eksisterer lovgivning for at beskytte fortrolige oplysninger om virksomheder, har vi baseret vores revisionskriterier på informationssikkerhedsstandarden ISO 27001, som de statslige institutioner har skullet følge siden januar 2014 som erstatning for informationssikkerhedsstandarden DS 484. Rigsrevisionen kunne dog konstatere, at flere virksomheder endnu ikke havde tilrettelagt styringen af informationssikkerheden efter ISO 27001, men at de var i en overgangsperiode. Det er Rigsrevisionens vurdering, at det praktiske sikkerhedsarbejde med de 2 standarder næsten er identisk for så vidt angår beskyttelsen af fortrolige oplysninger. Vi har derfor holdt institutionerne op imod den af de 2 sikkerhedsstandarder, som institutionerne selv har oplyst, at de fulgte og styrede informationssikkerheden efter.

Indsamling af materiale
Undersøgelsen er baseret på skriftligt materiale, som er indhentet fra de 8 institutioner. Det drejer sig bl.a. om informationssikkerhedspolitikker, retningslinjer for beskyttelse af oplysninger, oversigter over systemer med oplysninger om personer og virksomheder, databehandleraftaler samt serviceaftaler med it-driftsleverandørerne. Ved gennemgangen af materialet har vi ved tilfældig udvælgelse stikprøvevist efterprøvet den modtagne information. Vi har endvidere besøgt de 8 institutioner.

Undersøgelsens forløb og resultater
It-revisionen er udført fra januar 2014, hvor vi anmeldte undersøgelsen til institutionerne, til maj 2014, hvor vi sendte revisionsrapporter ud. Det betyder, at vi har undersøgt institutionernes praksis i denne periode. It-revisionen omfattede flere områder end dem, der er afrapporteret i beretningen. Vi har revideret institutionernes behandling af fortrolige oplysninger ud fra 60 revisionskriterier, som blev opstillet på baggrund af persondataloven, sikkerhedsbekendtgørelsen, informationssikkerhedsstandarden ISO 27001 og god praksis på området. Vi har i beretningen valgt at afrapportere de væsentligste revisionsresultater, som omfatter 11 revisionskriterier fra sikkerhedsbekendtgørelsen og 7 revisionskriterier fra ISO 27001. Institutionerne har endvidere haft et udkast til beretning i høring.

Vores vurdering af institutionernes praksis på området fremgår af de enkelte tabeller. Vi har vurderet, at det ikke er tilfredsstillende, hvis fx en institution enten ikke har udarbejdet retningslinjer for at sikre fortrolige personoplysninger, eller retningslinjerne er meget mangelfulde. Omvendt har vi vurderet, at det er tilfredsstillende, hvis en institution fx har udarbejdet retningslinjer for at sikre fortrolige personoplysninger, også selv om der er mindre mangler i retningslinjerne. De røde, gule og grønne cirkler i tabellerne udtrykker dermed Rigsrevisionens vurdering af institutionernes forvaltning, hvorimod man ikke direkte kan udlede, om en rød cirkel fx indebærer, om retningslinjerne helt mangler, eller om retningslinjerne findes, men at de er meget mangelfulde.

Undersøgelsens resultater underbygges af erfaringer fra tidligere it-revisioner, jf. beretning til Statsrevisorerne om revisionen af statsregnskabet for 2011 (afsnit III.C, s. 32-37, og afsnit III.D, s. 37-45) og beretning til Statsrevisorerne om revisionen af statsregnskabet for 2012 (pkt. 37 og pkt. 262).

Datatilsynet har endvidere oplyst, at de løbende behandler sager om sikkerhedsbrister hos institutioner og virksomheder, og Datatilsynet har over de seneste 5-6 år konstateret en stigning i antallet af sager om dette.

Bilag 2. Undersøgelsens resultater og institutionernes fremadrettede initiativer

Undersøgelsens resultater
Dette bilag indeholder en oversigt over undersøgelsens samlede resultater i forhold til, om institutionerne har efterlevet sikkerhedsbekendtgørelsens bestemmelser om fortrolige personoplysninger. Resultaterne gælder for de undersøgte it-systemer og for de udvalgte punkter i sikkerhedsbekendtgørelsen, som vi har undersøgt.

Undersøgelsens samlede resultater vedrørende institutionernes efterlevelse af sikkerhedsbekendtgørelsen

	Arbejdsskadestyrelsen	Institut for Menneskerettigheder	Danmarks Statistik	Forsvarskommandoen	Rigspolitiet	SKAT	Socialstyrelsen	Sundhedsstyrelsen
Er der retningslinjer for at sikre personoplysninger?	🟢	🔴	🟢	🟢	🟢	🟢	🟡	🟡
Er retningslinjerne opdateret årligt?	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴
Kontrolleres brugeradgange halvårligt?	🔴	🔴	🟢	🟢	🔴	🔴	🔴	🔴
Registreres afviste adgangsforsøg?	🟢	🟢	🟢	🟢	🟢	🟢	🔴	🟢
Følges der op på afviste adgangsforsøg?	🟡	🟢	🟢	🟢	🟢	🟡	🔴	🟡
Registreres medarbejdernes opslag på enkeltpersoner?	🟢	🔴	🔴	🟢	🟢	🟢	🟢	🟢
Slettes logregistreringerne?	🟢	🔴	🔴	🔴	🔴	🔴	🔴	🔴
Er der en aftale med databehandleren?	🟢	IR	🟢	🟢	🟢	🔴	🔴	🟢
Følges der op på databehandleraftalen?	🔴	IR	🔴	🟢	🔴	🔴	🔴	🔴
Er der retningslinjer for tilsyn?	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴
Føres der tilsyn med sikkerhedsforanstaltningerne?	🔴	🔴	🔴	🟢	🔴	🟡	🔴	🟡
Antal undersøgte punkter, der ikke er tilfredsstillende	**5**	**7**	**6**	**2**	**6**	**6**	**9**	**5**

🔴 Ikke tilfredsstillende, da der forekommer væsentlige mangler.
🟡 Delvist tilfredsstillende.
🟢 Tilfredsstillende, men mindre mangler kan forekomme.
IR Ikke relevant.

Kilde: Rigsrevisionen.

Institutionernes fremadrettede initiativer

Det fremgår af høringssvarene, at flere af de undersøgte institutioner har planlagt initiativer eller allerede har iværksat tiltag for at rette op på de kritikpunkter, som Rigsrevisionen har påpeget. De positive tilkendegivelser fremgår ikke af beretningen, fordi de fremadrettede initiativer endnu ikke er implementeret, og fordi vi ikke har efterprøvet, om de allerede iværksatte tiltag fungerer tilfredsstillende. Nedenstående oversigt viser institutionernes fremadrettede initiativer.

Institutionernes fremadrettede initiativer

Resultater i beretningen	Tilkendegivelser i høringssvaret
Retningslinjerne er ikke opdateret årligt	Forsvarskommandoen har tilkendegivet, at retningslinjerne vil blive ajourført inden udgangen af 2014. SKAT har tilkendegivet, at nye retningslinjer vil foreligge ultimo september 2014.
Brugeradgange kontrolleres ikke halvårligt	Rigspolitiet har tilkendegivet, at en ny løsning muliggør en halvårlig kontrol. Socialstyrelsen har tilkendegivet, at en halvårlig kontrol af brugerrettigheder på alle kritiske systemer blev besluttet i maj 2014. SKAT har oplyst, at Skatteministeriets Interne Revisions evaluering fra marts 2013 viste, at kontrollen af brugeradgange ikke var tilstrækkelig. SKAT igangsatte ved årsskiftet 2013/14 et arbejde med at forbedre kontrollen, som forventes afsluttet inden udgangen af 2014.
Afviste adgangsforsøg registreres ikke	Socialstyrelsen undersøger muligheden for at indføre registrering af afviste adgangsforsøg.
Logregistreringer slettes ikke	Forsvarskommandoen og SKAT tilkendegiver, at en praksis indføres, så logregistreringer slettes halvårligt.
Der mangler en aftale med databehandleren	SKAT har oplyst, at der i juni 2014 blev indgået en aftale med databehandleren. Socialstyrelsen har oplyst, at arbejdet med at udfærdige databehandleraftaler er iværksat.
Der følges ikke op på databehandleraftalen	Rigspolitiet har oplyst, at der fremadrettet vil blive indhentet en revisorerklæring om de tekniske og organisatoriske sikkerhedsforanstaltninger. Danmarks Statistik har oplyst, at de nu vil følge regelmæssigt op på, om sikkerhedsforanstaltningerne efterleves hos databehandleren.
Der mangler retningslinjer for tilsyn	SKAT har oplyst, at de nye retningslinjer for tilsyn forventes at ligge klar ultimo september 2014. SKAT vil vurdere omfang af og struktur på tilsynet. Socialstyrelsen har oplyst, at de har udarbejdet nye retningslinjer for tilsyn, og at de er i gang med at implementere dem.

Kilde: Rigsrevisionen på baggrund af oplysninger fra de undersøgte institutioner.

Bilag 3. Ordliste

Adgangsstyring	Adgangsstyring handler om krav til administration, begrænsning og kontrol af adgangen til institutionens informationer, medarbejdernes brug af mobilt udstyr og fjernarbejdspladser.
Behandling af oplysninger	Behandling af oplysninger dækker bl.a. over indsamling, registrering, systematisering, opbevaring, tilpasning eller ændring, selektion, søgning, brug, videregivelse ved transmission, formidling eller enhver anden overladelse, sammenstilling eller samkøring samt blokering, sletning eller tilintetgørelse.
Dataansvarlig	En fysisk eller juridisk person, en offentlig myndighed, en institution eller ethvert andet organ, der alene eller sammen med andre afgør, til hvilket formål og med hvilke hjælpemidler der må foretages behandling af oplysninger. Den dataansvarlige kan overlade det til en anden at udføre selve den praktiske behandling af personoplysninger på den dataansvarliges vegne.
Databehandler	En fysisk eller juridisk person, en offentlig myndighed, en institution eller ethvert andet organ, der behandler oplysninger på den dataansvarliges vegne.
Databehandleraftale	Når en dataansvarlig overlader en behandling af oplysninger til en databehandler, kræver det, at der indgås en skriftlig aftale mellem den dataansvarlige og databehandleren – en såkaldt databehandleraftale. Det skal fremgå af aftalen, at databehandleren kun handler efter instruks fra den dataansvarlige, og at databehandleren skal træffe forskellige tekniske og organisatoriske sikkerhedsforanstaltninger.
Digitalisering	Omsætning af fx data, lyd og billeder til digital form samt udbredelse af elektroniske medier og computerbaserede forretningsgange.
DS 484 og ISO 27001	Informationssikkerhedsstandarder. DS 484 er en dansk standard, mens ISO 27001 er internationalt anerkendt. Der er forskel på sikkerhedsstandarderne, men for dem begge gælder det, at efterlevelse af standarden er en metode til at sikre virksomhedernes informationer.
Fortrolige oplysninger	Det afgørende for, om en oplysning skal anses for fortrolig, vil være en vurdering af, om oplysningen er af en sådan karakter, at den efter den almindelige opfattelse i samfundet bør kunne forlanges unddraget offentlighedens kendskab. Oplysninger om racemæssig eller etnisk baggrund, politisk, religiøs eller filosofisk overbevisning, fagforeningsmæssige tilhørsforhold, helbredsforhold, seksuelle forhold, strafbare forhold og væsentlige sociale problemer (som er nævnt i lov om behandling af personoplysninger § 7, stk. 1, og § 8, stk. 1) vil utvivlsomt være fortrolige oplysninger. Det samme gælder oplysninger om interne familieforhold, fx stridigheder, og oplysninger om selvmordsforsøg og ulykkestilfælde. Herudover vil fx oplysninger om indtægts- og formueforhold samt arbejds-, uddannelses- og ansættelsesmæssige forhold efter omstændighederne også være fortrolige. Oplysninger, jf. persondatalovens §§ 7 og 8, kaldes også for følsomme personoplysninger.
Fysisk sikkerhed	En institution skal være tilstrækkeligt sikret mod eksterne trusler med alarmer, adgangskontrol og beskyttelse af informationsaktiverne. Institutionens informationsaktiver skal være sikret mod fx oversvømmelse, kabelnedbrud og brand.
Logge	At registrere de autoriserede brugeres anvendelser.
Personoplysninger	Enhver form for information om en identificeret eller identificerbar fysisk person (den registrerede). Ved identificerbar person skal forstås en person, der direkte eller indirekte kan identificeres, bl.a. ved et identifikationsnummer eller et eller flere elementer, der er særlige for en given persons fysiske, fysiologiske, psykiske, økonomiske, kulturelle eller sociale identitet, fx en adresse.

Risikovurdering	Ved risikovurdering vurderer institutionen, hvilke systemer der er forretningskritiske, og som virksomheden skal beskytte med konkrete sikkerhedsforanstaltninger. En risikovurdering tager udgangspunkt i institutionens forretningsmæssige forhold, trusselsbilledet, sårbarheden og konsekvenserne for institutionen, hvis et uheld skulle ske.
Sikkerhedsforanstaltninger	Betegner i denne beretning en praksis eller tiltag, der forbedrer it-sikkerheden, dvs. bestræbelser, som tages i anvendelse for at modvirke fejl, tab og misbrug af oplysninger og sikre tilgængeligheden til it-systemer og oplysninger.
Årsrevision	Rigsrevisionens årsrevision består af løbende revision af bl.a. forretningsgange og interne kontroller, herunder it-revision og afsluttende revision af bl.a. årsregnskabet. Resultatet af den løbende revision afrapporteres normalt til den pågældende institution og det tilhørende ministerium.