

Dataskyddspolitiken vid
Statens revisionsverk



Statens revisionsverk har i dag fastställt bifogade dataskyddspolitik. Beslutet är i kraft fr.o.m. 1.5.2008 tills vidare.

Helsingfors den 30 april 2008.

Generaldirektör Tuomas Pöysti

Dataskyddschef Tuomo Salminen

1 Inledning

1.1 Strategiska målsättningar för dataskyddspolitiken

Med dataskyddspolitiken vid Statens revisionsverk definieras dataskyddets målsättningar, strategiska tyngdpunktsområden, ansvar, principerna för skyddet och informationen vid revisionsverket.

Revisionsverkets strategiska målsättningar har definierats i det 25.1.2007 godkända dokumentet "Statens revisionsverks strategi för åren 2007 - 2012". Dataskyddspolitiken stöder att revisionsverkets strategiska målsättningar uppnås.

Dataskyddspolitiken kompletteras av revisionsverkets egna och riksdagens dataskyddsföreskrifter och instruktioner. Dataskyddsförfarandena och de åtgärder med vilka dataskyddet upprätthålls och utvecklas, har sammanställts i verkets planer och instruktioner (bl.a. planerna gällande dataskydd, arkivbildning, kommunikation, personal, kriskommunikation och beredskap samt instruktionerna om dataskydd och upphandling). När revisionsverkets dataskyddsdokument uppgörs beaktas i tillämpliga delar de instruktioner som har utfärdats av ledningsgruppen för datasäkerheten inom statsförvaltningen (VAHTI).

Den strategiska målsättningen för revisionsverkets datasäkerhet är, att verket fungerar som exempel för förvaltningen i utvecklandet och upprätthållandet av dataskyddskulturen. Tyngdpunktsområden är att en god informationshantering förverkligas i verkets samtliga funktioner, att personalens dataskyddskunnande upprätthålls och utvecklas samt att personalen engageras för dataskyddet och de instruktioner som gäller angående detta.

De operativa tyngdpunktsområdena i dataskyddet är systemens användbarhet, kryptering av informationen, tillförlitlig identifiering av användarna, hantering av användarrätter, ordnande av dataskyddsutbildning jämte instruktioner samt avvärjande av attacker utifrån, filtrering av skräppost och avvärjande av skadliga program.

Revisionsverket iakttar minst den av riksdagen fastställda dataskyddsnivån. Dessutom beaktas till behövliga delar de externa kraven på förverkligande av dataskyddet.

1.2 Begreppet dataskydd och dess betydelse

Med dataskydd avses att information, informationssystem och deras tjänster vad konfidentialitet, enhetlighet, tillgänglighet och användbarhet beträffar skyddas så, att mot dem riktade hot inte orsakar betydande skada på Statens revisionsverks verksamheter. I revisionsverkets verksamheter skall beaktas de förpliktelser som ingår i bestämmelser, föreskrifter och instruktioner, och som utgör centrala kriterier vid bedömningen av dataskyddsåtgärdernas kvalitet.

Målsättningen för dataskyddet är att sörja för att det faktamaterial som revisionsverket erhållit från revisionsobjekten och i den egna verksamheten under hela livscykeln behandlas i enlighet med bestämmelser, föreskrifter och instruktioner. Revisionsverkets personal är skyldig att i sitt eget arbete sörja för att dataskyddet förverkligas på en tillräcklig och adekvat nivå samt att ägna uppmärksamhet åt de hot som riktas mot datamaterial och informationssystem. Var och en är skyldig att påtala med dataskyddet förenade risker på det sätt som beskrivs i planer och instruktioner.

2 Omständigheter som styr dataskyddsverksamheten

I 18.1 § i lagen om offentlighet i myndigheternas verksamhet (621/1999) föreskrivs för myndigheterna å ena sidan en skyldighet att se till att offentlig information är tillgänglig i rätt tid och å andra sidan en skyldighet att skydda sekretessbelagd information mot missbruk. Enligt 32.1 § i personuppgiftslagen (523/1999) är den registeransvariga skyldig att genomföra de tekniska och organisatoriska åtgärder som behövs för att skydda personuppgifter mot obehörig åtkomst och mot förstöring, ändring, utlämnande och översändande som sker av misstag eller i strid med lag eller mot annan olaglig behandling. I arkivlagen (831/1994) föreskrivs om arkivbildarens skyldighet att förvara handlingar så, att de är skyddade mot förstörelse, skada och obehörig användning (ArkL 12.1 §).

Som ett syfte med lagen om elektronisk kommunikation i myndigheternas verksamhet (13/2003) har angetts att öka datasäkerheten i förvaltningen, med vilket för sin del avses att möjliggöra användning av elektroniska dataöverföringsmetoder (1 §). Myndigheterna skall ordna tillräcklig datasäkerhet både för medborgare, företag och samfund vid elektroniska tjänster och i informationsutbytet mellan myndigheterna.

Syftet med lagen om integritetsskydd i arbetslivet (759/2004) är att i arbetslivet genomföra de grundläggande fri- och rättigheter som tryggar skyddet för privatlivet och övriga grundläggande fri- och rättigheter som tryggar skyddet för den personliga integriteten. I lagen föreskrivs särskilt om omständigheter som berör personalsäkerheten, såsom behandlingen av arbetstagares personuppgifter, tester och kontroller som utförs på arbetstagare samt om de krav som ställs på sådana, om teknisk övervakning på arbetsplatsen samt om framtagning och öppnande av de anställdas e-post.

Statens revisionsverks arkivbildningsplan (446/01/05) innehåller grundläggande anvisningar om hur det faktamaterial som uppstår som resultat av verkets verksamhet skall behandlas och registreras, om sätten och formerna för dess förvaring och dess offentlighet samt beskrivningar av informationssystemen och de övriga instruktioner som berör behandlingen av dokument.

3 Hot och risker som riktar sig mot datasäkerheten

Hoten mot dataskyddet riktar sig mot datamaterial i elektronisk form och på papper, personalen, den fysiska säkerheten, utrustningar, programvara, datakommunikationstjänster och användningen av system. Hoten följs kontinuerligt med och om dem rapporteras till ledningen och övriga ansvarspersoner.

De hot och risker som riktar sig mot dataskyddet har definierats i verkets dataskyddsplan.

Dataskyddsriskerna kartläggs och dataskyddsåtgärderna har getts prioritetsordning så, att ifall riskerna realiserar, de inverkar så litet som möjligt på verkets verksamhet. Dataskyddsåtgärderna har getts prioritetsordning i verkets dataskyddsplan.

4 Datasäkerhetens betydelse för organisationen

Enligt 90.2 § i grundlagen (731/1999) finns Statens revisionsverk för revisionen av statsfinanserna och iakttagandet av statsbudgeten.

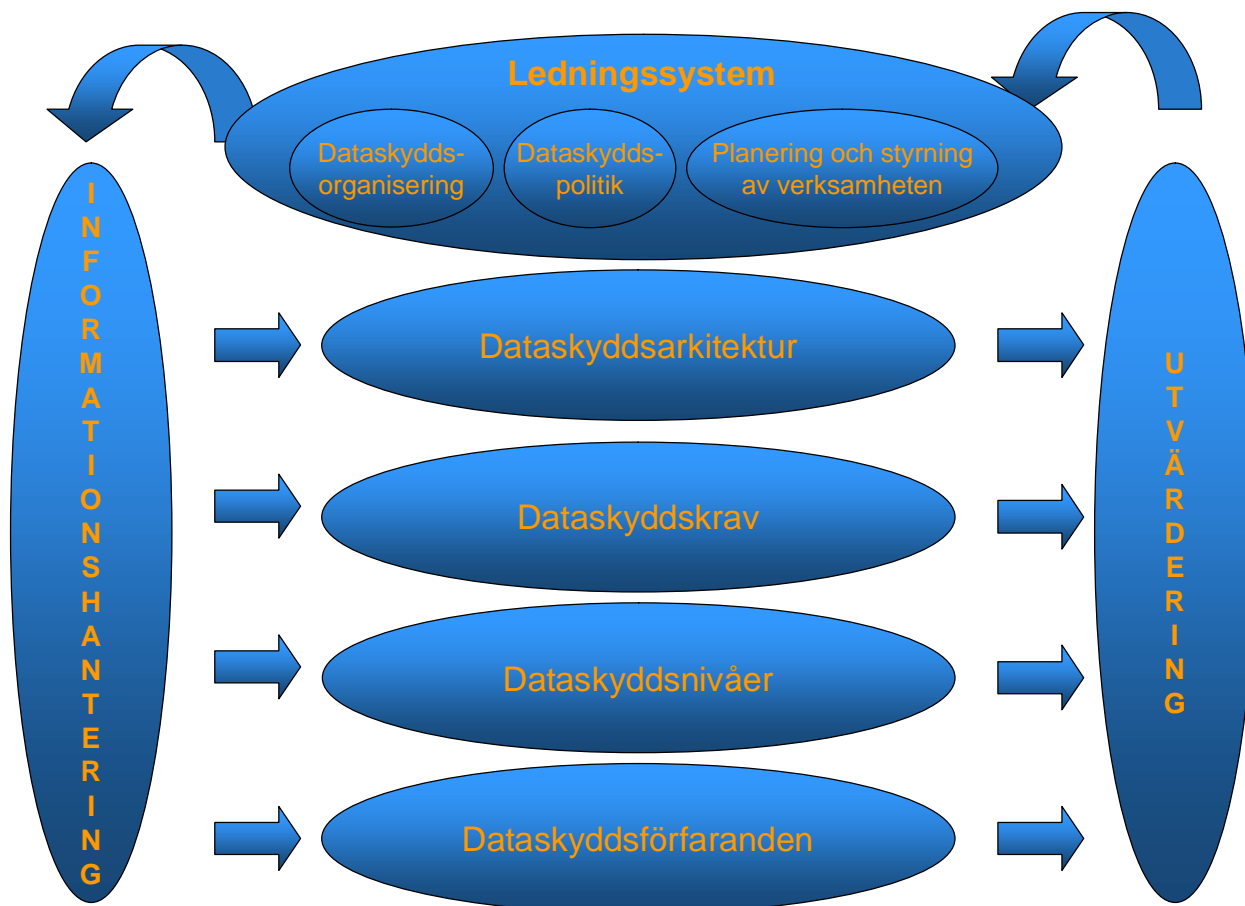
Enligt 1 § i lagen om Statens revisionsverk (676/2000) har revisionsverket till uppgift att granska lagligheten av och ändamålsenligheten i statsfinanserna samt iakttagandet av statsbudgeten. Dessutom har i 2-3 § i lagen om vissa medelöverföringar mellan Finland och Europeiska gemenskaperna för revisionsverket föreskrivits rätt att granska i i lagen definierade medelöverföringar.

6 § i lagen om Statens revisionsverk ålägger revisionsverket att årligen före utgången av september till riksdagen ge en berättelse om sin verksamhet. Revisionsverket har till uppgift att till revisionsobjekten meddela om de observationer som har framkommit vid revisionerna. Revisionsverket stöder med sin revisions- och sakkunnigverksamhet beslutsfattandet i riksdagen genom att erbjuda oavhängig revisionsinformation. Med revisionsverksamheten påverkas hur verksamheten inom förvaltningen utvecklas.

Med dataskyddsåtgärderna säkerställs utförandet av de i lagstiftningen ålagda uppgifterna, varmed verkställs utarbetandet av det faktamaterial som ges i berättelsen till riksdagen samt i rapporteringen till revisionsobjekten. Dessutom beaktas i planeringen och genomförandet av dataskyddsåtgärderna revisionsverkets strategiska målsättningar. Utförandet av revisionsverkets kärnuppgifter stöds av högklassiga och fungerande stödtjänster.

5 Systemet för administrering av dataskyddet

Hur systemet för administrering av dataskyddet verkställs har beskrivits närmare i revisionsverkets dataskyddsplan. Systemet för administreringen av dataskyddet utvecklas när lagstiftningen, instruktionerna och förfarandena förändras. Systemet har i sina huvuddrag beskrivits i nedanstående figur, och i det tillämpas standarden IEC/ISO 27001:2005.



FIGUR 1. SYSTEMET FÖR ADMINISTRERING AV DATASKYDDET

6 Dataskyddsansvar

6.1 Dataskyddsansvar vid revisionsverket

Den dataskyddspolitik och den dataskyddsplan som iakttas vid revisionsverket har godkänts av generaldirektören. Revisionsverkets högsta ledning svarar för att dataskyddet beaktas i verkets strategiska målsättningar.

Dataskyddschefen ser till att dataskyddet vid revisionsverket iakttas i enlighet med dataskyddspolitiken och dataskyddsplanen.

Dataförvaltningen har det allmänna ansvar för säkerheten gällande datakommunikation, programvara och utrustningar. Dokumentförvaltningen och verksamhetsenheterna har det allmänna ansvaret för datamaterialets säkerhet. För personalsäkerheten och den fysiska säkerheten ansvarar förvaltningschefen.

Vid revisionsverket fungerar en dataskyddsgrupp, som har till uppgift att utveckla verkets till dataskyddet anknutna förfaranden, utveckla instruktionerna och behandla observationer som berör dataskyddet.

Ansvaren har definierats närmare i revisionsverkets arbetsordning.

6.2 Samarbetspartnerns ansvar

I fråga om riksdagens s.k. gemensamma system iakttas riksdagens interna förfaranden. Leverantörerna av utlagda tjänster bör i tillämpliga delar iakttas revisionsverkets dataskyddsinstruktioner och föreskrifter, och dessa bör beaktas när avtal ingås.

7 Dataskyddsutbildning och information

För informationen om dataskyddsfrågor vid revisionsverket svarar på det allmänna planet verkets ledningsgrupp i samarbete med dataskyddschefen och informationsfunktionen.

Revisionsverkets offentliga informationsmaterial har publicerats på verkets internet-sidor (www.vtv.fi).

I revisionsverkets kriskommunikation iakttas verkets kommunikationsplan. För den externa information som anknyter till dataskyddet svarar informatören.

Dataskyddet utgör en väsentlig del av det kontinuerliga utvecklandet av verkets kunande, för vilket sörjs med en adekvat och planmässig dataskyddsutbildning.

För nyanställda ordnas en introduktion i verkets dataskyddsförfaranden och instruktioner före arbetsuppgifterna påbörjas.

I planeringen och verkställandet av dataskyddsutbildningen beaktas hur uppgifter, produkter och tjänster utvecklas.

Om uppdateringen av dataskyddsinstruktionerna informeras aktivt, och vid behov ordnas särskild utbildning för specifika målgrupper.

8 Övervakningen av hur dataskyddet förverkligas

Var och en i personalen är skyldig att meddela om sina observationer gällande dataskyddet. I övervakningen av dataskyddet deltar förutom personalen också olika sam-

arbetsinstanser. I övervakningen accentueras den roll som innehas av ledningen, för-
männen, dataförvaltningen och den systemansvariga personalen.

Verket har med sina intressegrupper ingått överenskommelser om övervakningsupp-
gifterna. Denna övervakning hänför sig särskilt till serverna och datakommunikatio-
nen.

9 Verksamheten i undantagssituationer och förhållanden

Vid brand- och räddningssituationer i normala förhållanden handlas i enlighet med
skyddsplanen. Åt personalen har getts skriftliga handlingsdirektiv inför situationer av
hot och alarm.

I undantagssituationer handlas vid verket i enlighet med beredskapsplanen.

Grupperna för skydd av dokument vid undantagssituationer har definierats i arkiv-
bildningsplanen.

Bilaga 1: Definitioner

Med fysisk säkerhet avses

- de åtgärder, med vilka till databehandlingen hörande objekt skyddas mot fysiska olyckor eller försök till skadande. Utrustningar och datalagren skyddas mot obehöriga personer och olika brand-, vatten- och fastighetsskador

Administrativ datasäkerhet

- innebär ledning av datasäkerheten och är utgångspunkten för verkets hela dataskyddsverksamhet

Personalsäkerhet

- innebär hantering av till personalen anknutna risker vad gäller personalens lämplighet, uppgiftsbeskrivningar, vikariat, rättigheter till information och användarrätter, skydd, säkerhetsutbildning och övervakning.

Med en god informationshantering avses att

- dokumentens och informationssystemens samt de i dem ingående uppgifternas tillgänglighet, användbarhet, skydd, enhetlighet och övriga på uppgifternas kvalitet inverkan omständigheter ombesörjs med tillräckliga åtgärder. Enligt offentlighetslagen hör till en god informationshantering att omsorgsfullt upprätthålla diarium och beskrivningar av informationssystem, sådana arrangemang som förutsätts av handlingars offentlighet, adekvat dataskydd och datasäkerhet, utbildning av och information till personalen om dessa omständigheter, övervakning av att instruktionerna om dem iakttas, samt förberedelse inför de planerade förvaltningsreformernas inverkan på handlingars offentlighet, sekretessbeläggning samt uppgifternas kvalitet.

Med användarsäkerhet avses

- den säkerhet som anknyter till användningen av datateknik, användarmiljön, databehandlingen och dess kontinuitet samt stöd-, upprätthållnings-, utvecklings- och underhållsfunktioner.

Med utrustningssäkerhet avses

- ett delområde av datasäkerheten, som innebär att säkerställa databehandlings- och datakommunikationsutrustningarnas användbarhet, funktion, sammansättning, underhåll

och kvalitetssäkring.

Programvarusäkerhet

- är ett delområde av datasäkerheten och innefattar operativsystem, middle ware, tillämpningsprogram och datakommunikationsprogramvara. Till området hör förfaranden för identifiering, isolering, tillgänglighetstillsyn och säkring av programvaran, åtgärder för kontroll och uppdagande, loggförfaranden, säkring av programvarans kvalitet samt säkerhetsåtgärder med anknytning till upprätthållande och uppdatering av programvaran.

Med risk avses

- sannolikheten för att ett hot förverkligas och leder till en viss förlust eller skada
- den med hotet förenade skadans värde eller förväntade värde uttryckt i pengar

Enhetlighet i information och databehandling innebär

- att informationen är äkta, oförfalskad, utan inre motstridigheter, täckande, aktuell, riktig och användbar
- egenskapen, att informationen eller budskapet inte har ändrats obehörigt, och att eventuella ändringar kan verifieras i registreringskedjan

Med konfidentiell information och databehandling avses

- att informationen förvaras konfidentiellt och att de rättigheter som hänför sig till uppgifterna, databehandlingen och datakommunikationen bevaras mot äventyrande och kränkningar
- det, i vilken mån konfidentialiteten betraktas som viktig

Med informationens och databehandlingens tillgänglighet och användbarhet avses

- egenskapen, att informationen, datasystemet eller tjänsten finns åtkomlig och användbar för dem som har rätt till dem vid önskad tidpunkt och på erforderligt sätt

Med datamaterialsäkerhet avses

- identifiering, klassificering och övervakning av uppgifter och de system som innehåller dessa i olika skeden av hanteringen

Med datakommunikationssäkerhet avses

- åtgärder, med vilka tryggas uppgifternas säkerhet när de förflyttas från ett system till

ett annat antingen inom organisationen eller mellan organisationer

Med dataskyddspolitiken avses

- den av ledningen på organisationsnivån antagna uppfattningen om datasäkerhetens målsättningar, principer och förverkligande