ANVISNINGAR OM INFORMATIONS-SÄKERHETEN I RIKSDAGEN

RIKSDAGENS E-POSTREGLER

RIKSDAGENS KANSLIS PUBLIKATION 5/2005

ANVISNINGAR OM INFORMATIONS-SÄKERHETEN I RIKSDAGEN

RIKSDAGENS E-POSTREGLER

RIKSDAGENS KANSLIS PUBLIKATION 5/2005

ISBN 951-53-2705-9 (nid.)
ISBN 951-53-2706-7 (PDF)
ISSN 1239-1638 (nid.)
ISSN 1795-7230 (pdf)

TILL LÄSAREN

Anvisningarna om informationssäkerheten inleds med ett påpekande om att riksdagens verksamhet huvudsakligen består av informationsbehandling, vilket gör att riksdagen är mycket beroende av information och informationsteknik. Detta beroende kommer att öka i framtiden när informationstekniken blir en allt viktigare del av arbetsprocesserna i riksdagen. Informationssäkerheten angår oss alla i vårt dagliga arbete.

Informationen måste säkras. Av anvisningarna om informationssäkerheten framgår hur Du kan skydda information, system, service och datakommunikation. Anvisningarna behandlar inte bara principiella frågor och lagstiftning utan också procedurer för informationshanteringen.

Riksdagen inför också nya e-postregler. I dag är e-posten ett betydande kommunikationsmedel, men till dags dato har vi saknat tillräckligt detaljerad spelregler för hur den ska användas. E-postreglerna innehåller i många fall mycket konkreta råd och föreskrifter om e-postanvändning och kompletteras med en sammanfattning av lagstiftning som är relevant i sammanhanget.

Var och en som arbetar i riksdagen gör klokt i att sätta sig in i regelverket – inte minst för sitt eget bästa.

Dataadministrationschef Olli Mustajärvi

INNEHÅLL

ANVISNINGAR OM INFORMATIONS-SÄKERHETEN I RIKSDAGEN

Godkänd av kanslikommissionen 11.11.2004

RIKSDAGENS KANSLIS PUBLIKATION 5/2005

SAMMANDRAG

Kom ihåg!

- ✓ Varje informationsanvändare är ansvarig för informationssäkerheten.
- ✓ Genom informationssäkerhet ser man också till att den offentliga informationen är korrekt, aktuell och tillgänglig.
- ✓ Låt inte andra använda ditt användarnamn och ditt lösenord.
- ✓ Skriv inte ned ditt lösenord.
- ✓ Välj inte ett lösenord som är lätt att gissa, t.ex. namnet på din make eller ditt barn.
- ✓ Spara viktig information i din hemkatalog på H-disken.
- ✓ Undvik onödiga papperskopior.
- ✓ Informationen på internet är inte nödvändigtvis korrekt – kontrollera informationens riktighet.
- ✓ Informationen på internet är skyddad av upphovsrätt – kontrollera att informationen får användas.
- ✓ Internetanvändarens identifieringsuppgifter sparas alltid i webbsidornas loggfiler.
- ✓ Det finns separata anvisningar om användningen av e-post; kom dessutom ihåg att det kan finnas andra specialanvisningar som måste beaktas när du hanterar information.

FÖRORD

Riksdagens förvaltningsdirektör tillsatte den 22 april 2004 en arbetsgrupp som skulle ta fram ett förslag till anvisningar för informationssäkerheten i riksdagen. Till ordförande utsågs riksdagens biträdande generalsekreterare Jarmo Vuorinen och till medlemmar utskottsråd Kaisa Vuorisalo, utskottsråd Risto Eerola, dataadministrationschef Juha Suomalainen och datachef Kari T. Sipilä. Sipilä slutade på riksdagen i maj 2005, men har deltagit i arbetsgruppens arbete även efter det. Som arbetsgruppens sekreterare fungerade Eerola och Sipilä. Arbetsgruppen skulle lägga fram sitt förslag senast den 30 juni 2004.

Arbetsgruppen utförde sitt uppdrag genom att granska frågor som gäller informationssäkerhet både med tanke på lagstiftningsarbetet och med tanke på riksdagens förvaltning. Både behovet av informationsförvaltning och den gällande lagstiftningen har beaktats.

Arbetsgruppen noterade under arbetets gång att tillämpningen av offentlighetslagstiftningen på riksdagens kanslikommission i dagens läge inte baseras på en uttrycklig bestämmelse i lag, utan att den faktiskt grundar sig på en passus i motiven till propositionen om den nya grundlagen. Det rättsliga läget kan därför enligt arbetsgruppen inte anses vara tillfredsställande i detta avseende. Dessutom vill arbetsgruppen väcka frågan om det behövs regler för riksdagens informationsverksamhet som komplement till dessa anvisningar.

Arbetsgruppen överlämnade sitt förslag till anvisningar för informationssäkerheten i riksdagen till förvaltningsdirektören den 29 juni 2004. Därefter har gruppen gått igenom de yttranden och synpunkter som inkommit och utifrån dessa i förekommande fall ändrat sitt förslag. Tyvärr har alla synpunkter inte kunnat beaktas, eftersom det regelverk som gäller offentligheten i riksdagens verksamhet och riksdagshandlingarnas offentlighet i någon mån avviker från regelverket för statsrådet och den tillhörande statsförvaltningen.

Arbetsgruppen har påpekat att riksdagen bör överväga separata anvisningar för god informationshantering.

Helsingfors den 5 november 2004

På arbetsgruppens vägnar

Jarmo Vuorinen
ordförande

INLEDNING

Riksdagens verksamhet består huvudsakligen av informationsbehandling, vilket gör att riksdagen är mycket beroende av information och informationsteknik (IT). I framtiden lär denna tendens förstärkas ytterligare. I takt med informationssamhällets utveckling ökar den mängd information som ska hanteras. Ett centralt mål inom informationssäkerheten är att garantera att informationshanteringen fungerar, att informationen kan förvaltas och att verksamheten kan fortgå i alla lägen.

Största delen av den information som hanteras på riksdagen är offentlig. Men även offentlig information måste skyddas. Det är ytterst viktigt att se till att informationen är korrekt, aktuell och tillgänglig. Informationssäkerheten tryggar högkvalitativ och tillgänglig information.

Riksdagen omfattas delvis av andra regler än regeringen och den underlydande statsförvaltningen när det gäller behandlingen av ärenden och handlingars offentlighet. Därför kan inte heller de regler som gäller för statsförvaltningen tillämpas direkt på riksdagen och dess verksamhet, utan det behövs separata anvisningar.

Genom dessa anvisningar, särskilt kapitel 3 och 4, fastställs förfaringssätten för hantering av den information samt de handlingar o.d. som erhålls i samband med arbetet, oavsett vilken form informationen eller handlingarna presenteras i. Anvisningarna gäller riksdagsledamöterna och deras assistenter, riksdagens tjänstemän och övriga anställda samt alla andra som arbetar i riksdagen och använder riksdagens informationssystem. Anvisningarna omfattar också sex bilagor. Det finns separata anvisningar för användningen av e-post i riksdagen.

1 INFORMATIONSSÄKERHET

1.1 Begreppet informationssäkerhet

Begreppet informationssäkerhet innebär att information, system, tjänster och datakommunikation skyddas med hjälp av administrativa, tekniska och varje användares personliga åtgärder. Information skyddas mot hot från uppsåtliga, oaktsamma och oavsiktliga åtgärder.

I dessa anvisningar avses med information sådan information som hanteras, lagras eller överförs i olika former. Informationen finns normalt i form av en handling, men även ljud- och bildupptagningar, databaser o.d. omfattas av anvisningarna.

Informationssäkerheten måste garanteras under alla steg av informationshanteringen. Hit hör bl.a. skapande, användning, ändring, lagring, överföring, spridning, kopiering, arkivering och förstöring av informationen.

Informationssäkerheten gäller både offentlig och hemlig information. Målet med informationssäkerheten är att garantera informationens riktighet och tillgänglighet. Ur riksdagens synvinkel är informationens riktighet och tillgänglighet bland de viktigaste sakerna, eftersom en stor del av den information som hanteras i riksdagen har anknytning till lagstiftning. En adekvat informationssäkerhet innebär en garanti såväl för riktighet och tillgänglighet som för sekretess, när sådan är påkallad.

I dessa anvisningar anses informationssäkerheten omfatta följande grundläggande punkter:

- Tillgänglighet
- Integritet
- Autentisering
- Oavvislighet
- Konfidentialitet

Tillgänglighet

Tillgänglighet innebär att informationen alltid finns tillgänglig för den som behöver och är behöriga att få den, även under undantagsförhållanden. Dessutom måste det tillses att information inte förstörs till följd av extern verksamhet. Det är viktigt att allmänheten har åtkomst till offentlig information.

Integritet

Integritet innebär att informationens innehåll alltid är korrekt och aktuell och att den är skyddad mot obehöriga ändringar. Kravet på integritet är mycket centralt för riksdagen.

Autentisering och oavvislighet

Autentisering innebär att den som använder eller producerar information vid behov kan identifieras.

Oavvislighet innebär att det är möjligt att också i efterhand bevisa vem som har använt eller gjort ändringar i informationen. Detta gäller även offentlig information.

Konfidentialitet

Konfidentialitet innebär att informationen är tillgänglig endast för dem som är behöriga att använda den. I fråga om offentlig information innebär konfidentialitet att informationen i förekommande fall kan användas av alla.

1.2 Informationsägare

Begreppet informationsägare hör intimt ihop med informationssäkerhet. Vanligen är det informationsproducenten eller den organisation som producerat informationen som är informationsägare. Ägaren ansvarar för uppgifterna och bestämmer hur informationen ska användas. Vidare bestämmer informationsägaren hur informationen ska klassas, och ingen annan har rätt att ändra klassificeringen (jfr dock 2.2.2 och 3.4). Vanligen gäller detta informationens konfidentialitet, men det kan även gälla andra grundläggande aspekter av säkerheten. Det är bra att minnas att var och en är ägare till sin egen information och därmed i sista hand själv ansvarar för den.

Informationssäkerheten och de förfaringssätt som ska följas bygger på gällande författningar samt på dessa anvisningar och andra interna regler.

Informationssäkerheten omfattar inte enbart informationsteknik, utan även andra sätt att hantera information samt säkra lokaler. Säkra lokaler innebär att lokalerna är i ändamålsenligt skick och att de uppfyller de krav som ställs för förvaring och användning av informationen. Detta gäller speciellt arkiv, datasalar och korskopplingar i datatrafiken. All informationssäkerhet bygger i sista hand på säkra lokaler. Dessa två stöder varandra och måste ligga på samma nivå.

1.3 Hot mot informationssäkerheten

Det största hotet mot informationssäkerheten är obehörig användning av information. Med obehörig användning avses en situation där en obehörig person får tillgång till information eller där en behörig person använder information på ett sätt som han eller hon inte har rätt till.

Risken för obehörig användning av information ökar om informationen inte har skyddats tillräckligt bra eller om den har fel säkerhetsklassificering. Det är särskilt viktigt att skydda information som överförs eller läggs ut på internet. På internet kan informationen bli föremål för obehörig användning utan att man vet vem som har missbrukat informationen. Detta gäller i synnerhet webbplatser. Ett

typiskt hot som förekommer genom internet är att informationen ändras av någon som inte har rätt till det.

Ett borttappat datamedium (t.ex. utskrift, cd-romskiva, diskett eller minneskort) eller en borttappad databehandlingsenhet (t.ex. bärbar dator, fickdator eller mobiltelefon) utgör alltid ett hot mot de uppgifter som finns lagrade på dem. Informationen kan missbrukas om det borttappade mediet eller den borttappade enheten hamnar i orätta händer. Kom också ihåg att även informationen på mediet eller enheten försvinner antingen tillfälligt eller för gott. Ofta är informationen betydligt värdefullare än själva mediet eller enheten.

Stöld av ett datamedium eller en databehandlingsenhet medför en stor informationsrisk. Om stölden har begåtts endast på grund av apparatens värde, är det mycket sannolikt att den lagrade informationen går förlorad. Om stölden har begåtts på grund av informationen, är det mycket sannolikt att informationen kommer att missbrukas.

Information kan också ändras eller förstöras indirekt. Det största hotet i detta avseende är datavirus. Virusen kan förstöra data, och dessutom kan de öppna datasystemet för obehörig användning. Risken för virusspridning är stor när internet används, men virus kan spridas även via datamedium eller e-post.

2 INFORMATIONENS OFFENTLIGHET OCH SEKRETESS

2.1 Lagstiftningsarbetet

2.1.1 Plenum

Bestämmelser om offentligheten i riksdagens verksamhet finns i *grundlagens 50 §*. Enligt den är *riksdagens plenum* offentliga, om inte riksdagen av synnerligen vägande skäl beslutar något annat i ett enskilt ärende. Vid behov kan riksdagen också besluta om offentligheten i fråga om de handlingar som behandlats i slutna plenum. Bestämmelser om protokoll och beslutsprotokoll från plenum finns i 69 och 70 § i riksdagens arbetsordning. Ett protokoll blir offentligt när det har undertecknats av riksdagens generalsekreterare och justerats av presidiet. Ett beslutsprotokoll blir offentligt när det har undertecknats av riksdagens generalsekreterare. Bestämmelser om publicering av riksdagshandlingar finns i 71 § i riksdagens arbetsordning.

2.1.2 Utskottssammanträdenas och utskottsärendenas offentlighet

Utskottens sammanträden är i regel inte offentliga. Ett utskott kan dock besluta att sammanträdet är offentligt till den del det inhämtar upplysningar för behandlingen av ett ärende. Dessa bestämmelser gäller både det utskott som bereder ärendet och de utskott som lämnar utlåtande om det. *Ärendet* blir offentligt i utskottet när utskottet har slutbehandlat det, om inte något annat följer av till exempel ett sekretessbeslut om ärendet.

Enligt grundlagens 50 § 3 mom. ska utskottens medlemmar iaktta sådan *sekretess* som utskotten av tvingande skäl anser att ett ärende särskilt kräver. Vid behandlingen av Finlands internationella förhållanden eller ärenden som gäller Europeiska unionen ska medlemmarna iaktta sådan sekretess som stora utskottet eller utrikesutskottet efter att ha hört statsrådet anser att ärendets natur kräver.

2.1.3 Handlingars offentlighet och sekretess

Bestämmelser om utskottshandlingarnas offentlighet finns i riksdagens arbetsordning. Över varje utskottssammanträde upprättas ett protokoll med information om vilka medlemmar som varit närvarande och vilka sakkunniga som hörts samt förslagen och besluten med omröstningar. Ett utskottsprotokoll blir offentligt när sekreteraren har kontrasignerat det, och handlingarna, dvs. de dokument som utskottet har utarbetat och mottagit för behandlingen av ärendet (t.ex. de skriftliga utlåtanden som sakkunniga lämnat till utskottet), blir i sin tur offentliga när ärendet har slutbehandlats i utskottet. En riksdagsgrupp som inte är företrädd i ett utskott eller en utskottsdelegation har rätt att få en kopia av handlingarna i ett ärende som inte är slutbehandlat, om de inte är hemliga.

Riksdagens arbetsordning anger *grunderna för sekretessbeläggning* av handlingar. En handling ska vara hemlig om

- utlämnande av uppgifter ur den skulle vålla betydande skada för Finlands internationella förhållanden eller kapital- och finansmarknaden, eller

- den innehåller affärs- eller yrkeshemligheter eller uppgifter om någons hälsotillstånd eller ekonomiska ställning.

Den sistnämnda sekretessgrunden innehåller en klausul om skaderekvisit. Enligt den kommer sekretessbeläggning i fråga endast om utlämnandet av uppgifter skulle vålla betydande olägenhet eller skada. En sådan olägenhet eller skada kan dock förbigås om ett betydande samhälleligt intresse kräver att handlingen ges offentlighet.

Ett utskott kan också av något annat liknande tvingande skäl besluta att en handling ska vara hemlig. På grund av riksdagsarbetets offentliga karaktär kan sekretessbeläggning baserad på ett sådant enskilt beslut endast ske subsidiärt och exceptionellt.

De handlingar som med stöd av 50 § 3 mom. i grundlagen omfattas av sekretess bildar en egen grupp hemliga handlingar.

Angående *sekretesstiden* för utskottens handlingar följs lagen om offentlighet i myndigheternas verksamhet (offentlighetslagen). Handlingarna är då i regel sekretessbelagda i 25 år, om inte något annat föreskrivs eller förordnas. Utskottet kan dock också besluta om en kortare sekretesstid. Sekretesstiden kan enligt offentlighetslagen förlängas om det är uppenbart att en handling, när den vid utgången av sekretesstiden blir offentlig, kommer att medföra betydande olägenhet för de intressen till vilkas skydd sekretess har föreskrivits.

För de *utskottstjänstemän* som deltar i lagstiftningsarbetet gäller i fråga om offentlighet och sekretess avseende handlingar och deras innehåll samt i fråga om tystnadsplikt de bestämmelser som gäller för utskotten.

Enligt motiven till grundlagspropositionen ska riksdagens övriga organ i sin verksamhet i tillämpliga delar följa de bestämmelser som gäller för utskott. Detta gäller till exempel talmanskonferensen.

2.2 Förvaltningen

2.2.1 Offentlighet

Enligt offentlighetslagen avses med *myndighet* även riksdagens ämbetsverk, dvs. riksdagens kansli, statsrevisorernas kansli och riksdagens justitieombudsmans kansli samt statens revisionsverk, som finns i anknytning till riksdagen. Detta betyder att riksdagens förvaltning följer samma offentlighetsbestämmelser som statsförvaltningen i övrigt. Trots att offentlighetslagen inte som sådan kan tillämpas på verksamheten i riksdagens kanslikommission påpekas det i motiven

till grundlagspropositionen att kanslikommissionen i tillämpliga delar följer samma offentlighetsprinciper som statsförvaltningen i övrigt.

På riksdagens förvaltning tillämpas till exempel offentlighetslagens allmänna bestämmelser om tidpunkten för när en handling blir offentlig, rätten att ta del av myndigheternas offentliga handlingar, sekretess, tystnadsplikt för den som är verksam vid en myndighet och myndigheternas skyldigheter för att lagens syfte ska nås.

I offentlighetslagen avses med *myndighetshandling* en handling som innehas av en myndighet och som har upprättats av myndigheten eller av någon som är anställd hos myndigheten eller som har inkommit till myndigheten för behandlingen av ett visst ärende eller i övrigt inkommit i samband med ett ärende som hör till myndighetens verksamhetsområde eller uppgifter. Offentlighetslagen gäller även köpta tjänster. Därför anses en handling ha blivit upprättad av en myndighet även när den har upprättats på uppdrag av myndigheten, och en handling ha inkommit till en myndighet även när den har inkommit till den som verkar på uppdrag av myndigheten eller i övrigt för myndighetens räkning, för att denne ska kunna utföra sitt uppdrag.

Som *myndighetshandling* enligt offentlighetslagen *betraktas i regel inte* de handlingar som upprättats för en myndighets interna arbete. Dessa handlingar omfattas av offentlighetslagen bara om de innehåller sådan information att de enligt arkivlagstiftningen ska överföras till ett arkiv.

Med myndighetshandling *avses* enligt offentlighetslagen *inte* heller sådana minnesanteckningar som ännu inte har lämnats in för föredragning eller någon annan behandling av ett ärende och som har gjorts av den som är anställd hos en myndighet eller den som är verksam på uppdrag av en myndighet. Det är alltså fråga om en handling som hör till offentlighetslagens tillämpningsområde först när handlingen är klar för tjänstemannens del och denne har överlämnat den till den instans som fattar beslut eller i övrigt behandlar ärendet. Att presentera handlingen för chefen eller någon annan för synpunkter eller råd anses inte utgöra överlämnande i den meningen.

Detaljerade bestämmelser om *tidpunkten för när en handling som upprättats av en myndighet blir offentlig* finns i 6 § i offentlighetslagen. Bestämmelserna är ändå sekundära i förhållande till sekretessbestämmelserna, dvs. handlingen blir offentlig *bara till den del som den inte behöver hållas hemlig enligt de nedan nämnda bestämmelserna*. De mest typiska handlingarna blir offentliga enligt följande:

- En anteckning i ett diarium eller någon annan förteckning: när den har införts.

- En myndighets begäran om anbud, utredning eller utlåtande samt en myndighets framställning, förslag, initiativ, meddelande eller ansökan, inklusive bilagor: när de har undertecknats eller bekräftats på motsvarande sätt; en begäran om komplettering av ett anbud samt utredningar som har

sammanställts för behandlingen av anbudsärendet: först när ett avtal har ingåtts i ärendet.

- Undersökningar och statistik som en myndighet har tagit fram samt med dem jämförbara utredningar som bildar självständiga helheter och beskriver de alternativ som föreligger i allmänt betydelsefulla avgöranden eller planer samt grunderna för och verkningarna av dessa avgöranden eller planer, också när utredningen anknyter till ett ärende som i övrigt inte är slutbehandlat: när de är färdiga för avsett ändamål.

- Ett protokoll upprättat av en myndighet: när det efter justeringen har undertecknats eller bekräftats på motsvarande sätt, om det inte har upprättats för beredning av ett ärende (t.ex. kommittéprotokoll) eller för myndighetens interna arbete.

- Ett beslut, ett utlåtande och en expedition av en myndighet, ett avgörande fattat av en myndighet i egenskap av avtalspart och myndighetens promemorior för behandlingen av dessa: i enlighet med huvudregeln när de har undertecknats eller bekräftats på motsvarande sätt.

Med avvikelse från vad som sägs ovan blir ett kommittébetänkande, en utredning eller någon annan motsvarande handling som är avsedd för allmän distribution offentlig när den innehas av myndigheten för att distribueras, dvs. i tryckt form eller mångfaldigad på något annat sätt.

En handling som har inkommit till en myndighet för behandling av ett ärende eller annars i samband med ett ärende som hör till myndighetens verksamhetsområde eller uppgifter blir i enlighet med huvudregeln offentlig när myndigheten har fått den. Sådana handlingar är t.ex. reseräkningar från anställda hos myndigheten och ansökningshandlingar riktade till myndigheten. Dessa handlingar kan innehålla sekretessbelagda delar. Specialbestämmelser om exempelvis anbudsförfaranden finns i offentlighetslagens 7 §.

2.2.2 Sekretess

Sekretessen har två olika dimensioner: skyldigheten att hålla handlingen hemlig och tystnadsplikten gällande den hemliga informationen.

Sekretess avseende en handling innefattar förbud mot att visa den sekretessbelagda handlingen eller att ge ut en kopia av den. Grunderna för sekretessbeläggning av myndighetshandlingar anges i offentlighetslagens 24 §.

Tystnadsplikten gäller tjänstemannens agerande. Det innebär ett förbund mot att yppa sekretessbelagd information oavsett om informationen har sparats eller inte. Information som omfattas av tystnadsplikt kan finnas i en handling eller så kan det röra sig om muntlig information. Med avseende på det faktiska tillämpningsområdet är tystnadsplikten således mer omfattande än sekretessen.

Enligt offentlighetslagen får inte den som är anställd hos en myndighet röja en handlings sekretessbelagda innehåll eller en uppgift som skulle vara sekretessbelagd

om den ingick i en handling, och inte heller någon annan omständighet som den anställde har fått kännedom om i samband med sin verksamhet hos myndigheten och för vilken tystnadsplikt föreskrivs genom lag. Lagen säger också explicit ut att en uppgift för vilken tystnadsplikt gäller inte heller får röjas efter det att verksamheten hos myndigheten har upphört eller det uppdrag som utförts för myndighetens räkning har avslutats. Tystnadsplikten är således inte knuten till att anställningen fortfarande pågår.

Tystnadsplikten är inte begränsad enbart till tjänsteinnehavare, utan den gäller även andra anställda. Enligt offentlighetslagen gäller tystnadsplikten även praktikanter och andra som faktiskt verkar hos en myndighet.

Också ett uppdragsförhållande, t.ex. ett avtal om tjänsteupphandling, utsträcker tystnadsplikten till andra personer än myndighetspersoner. I dessa fall gäller tystnadsplikten de sekretessbelagda uppgifter som myndigheten lämnat ut till uppdragstagaren. På samma grunder gäller tystnadsplikten även dem som är anställda hos den som utför ett myndighetsuppdrag.

Till sekretessen hör även ett *förbud mot utnyttjande*. Det innebär att den som tystnadsplikten gäller inte får använda sekretessbelagda uppgifter för att skaffa sig själv eller någon annan fördel eller för att skada någon annan. Förbudet mot utnyttjande gäller även efter att anställningen eller uppdraget har upphört.

Enligt 25 § i offentlighetslagen ska en *anteckning om sekretess* alltid göras i en handling som ges ut till en part och som ska vara sekretessbelagd på grund av en annan parts intresse eller av allmänt intresse. Anteckning om sekretess får göras också på andra sekretessbelagda handlingar. Av anteckningen ska framgå till vilka delar handlingen är sekretessbelagd och vad sekretessen grundar sig på. Om sekretessen grundar sig på en bestämmelse som innehåller en s.k. klausul om skaderekvisit, får anteckningen emellertid göras så att bara den bestämmelse som sekretessen grundar sig på framgår av anteckningen. Anteckningen om sekretess har *inte* några *självständiga rättsverkningar*, vilket innebär att uppgifter ur en handling inte kan vägras endast på den grunden att handlingen innehåller en anteckning om sekretess. *Sekretessen ska avgöras separat i varje enskilt fall med tillämpning av offentlighetslagen.*

Uppgifter om en sekretessbelagd myndighetshandling eller om dess innehåll får lämnas ut enligt de grunder som nämns i offentlighetslagen. När endast en del av en handling är sekretessbelagd, får uppgifter i den offentliga delen lämnas ut om det är möjligt utan att den sekretessbelagda delen röjs.

Utlämnande av information ur en sekretessbelagd handling utgör alltså ett undantag som kräver stöd i lag. Enligt 26 § i offentlighetslagen utgör en uttrycklig specialbestämmelse i lag eller samtycke från den som sekretessen är avsedd att skydda *allmänna grunder för undantag*. Dessutom får en myndighet lämna ut uppgifter som gäller exempelvis någon annans ekonomiska ställning eller en affärs- eller yrkeshemlighet eller sådana omständigheter som avses i 24 § 1 mom. 32 punkten i offentlighetslagen och som gäller någons privatliv. Då krävs ändå att uppgiften behövs för att en enskild eller en annan myndighet ska kunna upp-

fylla en i lag föreskriven upplysningsplikt eller för att en ersättning eller något annat yrkande som ska handhas av den myndighet som lämnar ut uppgiften ska kunna genomföras. En myndighet får också lämna ut sekretessbelagda uppgifter för ett uppdrag som myndigheten gett eller någon uppgift som i övrigt handhas för myndighetens räkning, om detta är nödvändigt för att uppdraget eller uppgiften ska kunna skötas.

Offentlighetslagen innehåller också särskilda bestämmelser om utlämnande av sekretessbelagda uppgifter *till en annan myndighet* och om rätten att lämna ut sådana uppgifter *till utländska myndigheter och internationella organ*.

Dessutom bör det noteras att *en part*, till exempel den sökande i ett ärende, har rätt att hos den myndighet som behandlar eller har behandlat ärendet ta del av en myndighetshandling som kan eller har kunnat påverka behandlingen, även om handlingen inte är offentlig. Offentlighetslagen anger emellertid flera undantag från denna regel.

3 HANTERING AV INFORMATIONSMATERIAL

3.1 Rättslig grund

De regler som gäller för hanteringen av informationsmaterial på riksdagen bygger huvudsakligen på riksdagens arbetsordning när det gäller lagstiftningsarbetet och på offentlighetslagen när det gäller förvaltningen. Dessutom finns det särskilda regler för hanteringen av vissa typer av informationsmaterial. Det rör sig i synnerhet om *personuppgiftslagen* (523/1999), där 2 kap. anger de allmänna principerna för behandlingen av personuppgifter och 3 kap. innehåller bestämmelser om behandlingen av känsliga uppgifter och personbeteckningar.

Enligt *lagen om dataskydd vid elektronisk kommunikation* (516/2004) är alla identifierings- och lokaliseringsuppgifter som uppkommer vid elektronisk kommunikation, såsom telefonsamtal och e-postmeddelanden, i princip konfidentiella. De omfattas därför av tystnadsplikt och förbud mot utnyttjande. Bestämmelser om rätten att behandla dessa uppgifter finns i 3 och 4 kap. Lagen innehåller också bestämmelser om i vilka fall och hur en s.k. sammanslutningsabonnent (t.ex. riksdagen) har rätt att för dataskyddsändamål ingripa i kommunikation som sker i dess kommunikationsnät.

Utöver regler för behandlingen av uppgifter som följer av lagstiftning kan hanteringen av handlingar regleras med hjälp av *klassificering av informationsmaterial med avseende på deras hantering*. En sådan klassificering används för att främja goda rutiner för informationshanteringen, men kan inte i sig utgöra grunden för sekretess eller på något annat sätt begränsa offentligheten. Klassificeringen måste ändå beaktas när dokument hanteras, lagras och förstörs.

3.2 Hur klassificeras handlingar på riksdagen?

Alla uppgifter och handlingar som behandlas på riksdagen *klassificeras* på grundval av innehåll enligt följande:

- offentlig ("julkinen")
- för internt bruk ("sisäiseen käyttöön")
- hemlig ("salainen").

Klassificeringen *måste anges på alla handlingar som inte är offentliga*. På offentliga handlingar behövs således ingen anteckning. När det gäller hanteringen av stora mängder *upptagningar för internt bruk* för vilka det redan finns en inarbetad klassificeringspraxis (t.ex. utskottens arbetsdokument) behöver den enskilda handlingens klassificering eller spridning inte heller nödvändigtvis anges. I övrigt följs de gällande reglerna och anvisningarna vid hanteringen av dessa handlingar.

Med undantag av ovan nämnda avvikelser ansvarar den tjänsteman som klassificerar informationen för att handlingen eller motsvarande förses med en anteckning om klassificeringen och om omfattningen på spridningen.

Det *beredningsmaterial* som framtagningen av en handling e.d. genererat behandlas och lagras i enlighet med dess klassificering. Om materialet är hemligt och hanteras av minst tre personer, ska det stämplas eller märkas på något annat lämpligt sätt. Allt beredningsmaterial som inte längre behövs ska förstöras omedelbart.

Exempel på klassificeringen av information finns i *bilaga 1*. Närmare anvisningar om förfarandena enligt bilagorna 1–6 ges vid behov av de byrå- eller enhetschefer som ansvarar för informationen och handlingarna.

Offentliga uppgifter

Största delen av den information som hanteras på riksdagen är offentlig. Informationen är inte sekretessbelagd enligt lag och kan därmed ges ut.

Om aktiva åtgärder ska vidtas för att offentliggöra information ligger ansvaret på riksdagsinformationen.

Uppgifter för internt bruk

Klassen "För internt bruk" kan användas när det är fråga om

- en handling som tagits fram för myndighetens interna arbete och som inte innehåller uppgifter vars beskaffenhet eller natur medför att handlingen bör överföras till ett arkiv, eller

- en halvfärdig handling, dvs. anteckningar som författaren inte överlåtit för föredragning eller annan ärendebehandling.

Även om uppgifter avsedda för internt bruk inte är hemliga bör de diskuteras och utväxlas bara inom den personkrets som är nödvändig för behandlingen av ärendet.

Handlingar i gruppen "För internt bruk" motsvaras av de handlingar som på vissa myndigheter betecknas *Får inte röjas för utomstående* (*Ei saa antaa tietoja sivullisille (ets)*) och *Endast för tjänstebruk* (*Vain virkakäyttöön*).

Hemliga uppgifter

Uppgifter ska klassas som hemliga bara om det finns grund för sekretessbeläggning i lag.

Eftersom de handlingar som anknyter till lagstiftningsarbetet i regel är offentliga är det särskilt viktigt att de handlingar sekretessbeläggs som är hemliga enligt 43 § 3 mom. i riksdagens arbetsordning eller som innehåller uppgifter som omfattas av den sekretess som kan beslutas på grundval av grundlagens 50 § 3 mom. Denna sekretess anknyter vanligen till ärenden som stora utskottet eller utrikes-

utskottet behandlar. Dessa utskott beslutar då om sekretessens omfattning med bindande verkan även för de andra utskotten.

I fråga om förvaltningen finns de centrala bestämmelserna om sekretess i offentlighetslagen. Detaljerade sekretessbestämmelser finns i lagens 24 § 1 mom., som har en förteckning på 32 punkter över sekretessbelagda myndighetshandlingar. Bestämmelserna skyddar bl.a.

- statens utrikespolitiska intressen och internationella relationer
- statens säkerhet och befolkningsskydd
- allmänintresset i brottsutredningar och annan polisverksamhet
- skyddsarrangemang för personer, byggnader, inrättningar, konstruktioner samt data- och kommunikationssystem och genomförande av arrangemangen
- skötseln av inkomst-, finans-, penning- och valutapolitik
- finans- och försäkringssystemets tillförlitlighet och funktionsduglighet
- förtroendet för kapital- och finansmarknaden
- förutsättningarna för myndigheternas inspektionsverksamhet
- intresset att skydda naturen
- intressen som gäller forskning och statistik
- ekonomiska intressen
- professionella intressen inom forskning och utveckling som kan jämställas med en affärs- eller yrkeshemlighet
- provs eller testers funktion
- privatlivet.

I offentlighetslagen bygger sekretessen avseende en handling i de flesta fall på de uppgifter handlingen innehåller: i dessa fall ligger huvudvikten således på den information som finns i handlingen. Vissa av offentlighetslagens sekretessbestämmelser bygger på absolut sekretess. Då måste handlingen villkorslöst hållas hemlig. De flesta sekretessbestämmelserna i offentlighetslagen innehåller ändå en s.k. *klausul om skaderekvisit*, som har använts för att försöka begränsa sekretessen till vad det intresse som ska skyddas kräver i det enskilda fallet. *Klausulens inverkan på sekretessen varierar beroende på om lagens presumtion är att handlingen är offentlig eller hemlig.* När utgångspunkten är att en handling är offentlig, ska den stadgas vara hemlig om utlämnande av uppgifter på det

sätt som avses i bestämmelsen skadar intressen som ska skyddas. Om presumtionen däremot är sekretess får uppgifter lämnas ut endast om det är uppenbart att detta inte leder till i bestämmelsen närmare angiven skada för det intresse som ska skyddas. Oavsett presumtionen i bestämmelsen *ska en bedömning av skadevållande göras från fall till fall*.

Sekretessbelagda uppgifter får lämnas ut till utomstående bara om denna rätt föreligger enligt lag. Diskussioner och annat informationsutbyte ska begränsas till den krets som har rätt att ta del av uppgifterna. Denna krets framgår normalt av handlingens sändlista e.d.

Klassen "hemlig" motsvaras på vissa myndigheter av klassen *Personhemlig* (*Henkilösalainen*).

3.3 Hur ska förfrågningar om information hanteras?

Uppgifter ur en offentlig handling ska enligt offentlighetslagen ges så snart som möjligt, dock senast *inom två veckor* efter det att myndigheten har mottagit en begäran om att få ta del av handlingen. I specialfall får uppgifterna lämnas ut ända upp till en månad efter begäran om att få ta del av handlingen. Det rör sig om fall där

- de begärda handlingarna är många
- handlingarna innehåller sekretessbelagda delar eller
- om någon annan därmed jämförbar omständighet gör att det krävs specialåtgärder för att behandla och avgöra ärendet.

I normalfallet får det således ta högst två veckor att svara på en begäran om att få ta del av en handling, men *generellt sett måste en förfrågan besvaras betydligt snabbare.* Riksdagens justitieombudsman har i sin praxis bedömt att beslut om en handlings offentlighet måste fattas samma dag som begäran inkommer.

Notera särskilt att det är riksdagens bibliotek som behandlar förfrågningar om handlingar efter det att handlingar som utskotten tagit fram eller erhållit har överlåtits för arkivering.

3.4 Vem ansvarar för informationssäkerheten?

Primärt är det den som använder informationen som har ansvaret för den. Det kan röra sig t.ex. om samma person som äger eller producerat informationen eller som har tagit fram handlingen. Var och en som har att göra med information är skyldig att sörja för informationssäkerheten för egen del. Om uppgifterna är hemliga eller avsedda för internt bruk ansvarar varje användare för att uppgifterna hålls hemliga eller endast lämnas till behöriga personer.

Informationsägaren är skyldig att vid behov klassificera handlingen (informationen) med avseende på vem som får hantera den. I bilaga 1 finns en tabell med

exempel på klassificeringen av information. Det är motiverat att utgå från att information från en myndighet, organisation eller internationell samarbetspartner ska hanteras på det sätt som informationsägaren kräver om inte annat följer av de specialbestämmelser som gäller för riksdagsarbetet. Om informationen är klassificerad ska den behandlas som information enligt motsvarande eller närmast motsvarande klass på riksdagen.

4 INFORMATIONSTEKNIK OCH SÄKERHETSFRÅGOR

4.1 Generellt

I datasystem identifieras användarna med hjälp av *användarnamn och lösenord*. De används vid behov för att autentisera vem som har använt systemet. Användarnamnet ger användaren åtkomsträtt till de datasystem och uppgifter som han eller hon behöver i sitt arbete och har behörighet att använda. Åtkomsträttigheterna beviljas av systemägaren. Endast ägaren eller dennes ombud kan ge åtkomsträtt till ett datasystem.

Användarnamnet är alltid personligt och får under inga omständigheter ges till en annan användare. Du är alltid själv ansvarig för allt som görs med ditt användarnamn. Som användare har du inte rätt att låta någon annan använda datasystemet utan systemägarens tillstånd.

Riksdagens informationssystem och den information de innehåller får i princip endast användas för tjänste- och arbetsuppgifter. Undvik att i onödan skriva ut eller kopiera information för internt bruk och hemlig information, eftersom extra papperskopior ökar risken för att informationen hamnar i fel händer.

Det lönar sig att *spara* informationen på en nätdisk (t.ex. ditt eget material på H-skivan), eftersom den då regelbundet säkerhetskopieras och därmed vid behov kan återställas. Den information som bara finns på hårddisken till din arbetsstation (C-skivan) kan gå förlorad om din dator går sönder.

Om den information som du ska hantera har klassificerats som information för internt bruk eller hemlig information och ska vidarebefordras, måste du som användare se till att ingen annan än de som har rätt att hantera informationen får den.

4.2 Internet

Internet är en bra informationskälla och praktiskt när man vill överföra information. Dessutom är internet ett utmärkt verktyg för den som vill offentliggöra information. Internet är inte ett sammanhängande nät, utan det består av flera nät som kopplats till varandra med TCP/IP, en standard för datakommunikation. Internet har ingen ansvarig operatör, och det finns inga internationella överenskommelser som reglerar eller garanterar dess funktion och innehåll.

Det går alltid att kopiera, lagra och modifiera information som finns ute på internet, utan att det syns på själva informationen. På internet överförs informationen ofta via flera nät. Ofta är det omöjligt att i efterhand utreda vilka vägar informationen har tagit genom nätet. Informationen kan överföras via olika rutter varje gång du använder nätet eller t.o.m. under samma session.

På internet kan en användare på riksdagen identifieras på organisationsnivå. Varje gång du är inne på en webbplats eller använder en nättjänst ser den som tillhandahåller tjänsten att någon på riksdagen använder den.

Den allmänt tillgängliga informationen på internet är inte alltid autentisk och korrekt. Som användare måste du själv kontrollera uppgifternas riktighet och autenticitet samt försäkra dig om att du har rätt att använda uppgifterna. I synnerhet bör de upphovsrättsliga frågorna beaktas. Du får inte ladda ned sådant material från internet som är upphovsrättsligt skyddat, om du inte har behörighet att använda materialet.

4.3 Fjärranvändning

Med fjärranvändning avses all användning av information som sker utanför riksdagen med riksdagens datorer. Som fjärranvändare kan du vara uppkopplad till riksdagens nät eller så kan du behandla informationen utan uppkoppling.

Om du arbetar med uppkoppling på riksdagens nät, dvs. *med fjärrskrivbord*, är förbindelsen mellan din bärbara arbetsstation och riksdagens datorer *skyddad* med ett särskilt program. I samband med annan fjärranvändning är uppkopplingen inte skyddad.

Hemliga uppgifter får hanteras endast i skyddade miljöer. Vid fjärranvändning utan skyddad uppkoppling måste du som användare se till att de uppgifter som du avser att hantera inte har klassats som hemliga. Om du hanterar uppgifter i en oskyddad miljö och samtidigt är uppkopplad på internet, måste du se till att uppgifterna viruscheckas innan du återför dem till riksdagens nät.

Du måste ge akt på alla apparater och datamedier i samband med fjärranvändning och får absolut inte låta någon utomstående använda dem. *Bärbara arbetsstationer, telefoner eller datamedier får aldrig lämnas utan uppsikt på öppen plats.* Undvik i synnerhet att lämna dem på ett synligt ställe i bilen.

4.4 Utomstående personer på riksdagen

När det gäller informationssäkerhet behandlas de aktörer som inte hör till riksdagens personal enligt samma principer som de anställda. Dessa utomstående måste informeras om sitt ansvar och sina skyldigheter enligt lag. Om en dylik utomstående person måste ges tillgång till hemlig information ska leveransavtalet eller en liknande handling ange dennes skyldigheter i fråga om sekretess. När sekretessbelagda uppgifter ges till en enskild person som riksdagen inte ingår ett särskilt avtal med, ska personen informeras om sina skyldigheter när det gäller sekretess i en separat handling (åtagande). Den berörda enhetschefen ansvarar för att dessa åtaganden ingås och sparas.

4.5 Påföljder vid brott mot informationssäkerheten

Den som inte följer lagen, dessa anvisningar eller reglerna om informationssäkerhet kan i lindrigaste fall fråntas sin rätt att använda riksdagens informationssystem.

5 HUR SKÖTS ÄRENDEN SOM GÄLLER INFORMATIONSSÄKERHET?

På riksdagen samordnas informationssäkerheten av *dataadministrationsbyrån*, som assisterar ledningen när det gäller att se till att informationssäkerheten fungerar. Du kan kontakta byrån både i IT-frågor och t.ex. när du har problem med klassificeringen av handlingar med avseende på informationssäkerheten.

Ansvaret för att övervakningen av informationssäkerheten ordnas ligger på cheferna för de enheter som producerar eller hanterar information. Cheferna ska se till att informationen hanteras i enlighet med dessa anvisningar (inklusive bilagorna) och att de anställda på enheten får tillräckligt med information om informationssäkerheten.

BILAGA 1–6

Bilaga 1 Exempel på klassificering av information

Offentlig	För internt bruk	Hemlig
Syftet med riksdagens verksamhet och riksdagens huvuduppgifter	Ärenden som utskotten bereder	
Riksdagsenheternas verksamhetsstrategier Avdelningarnas och enheternas utvecklingsplaner och budgetar		
Organisationsplaner Matriklar		
Meddelanden		
Tal, föredrag, utredningar och statistik efter publicering	Interna och halvfärdiga utredningar	
Användningen av riksdagens medel		
		Kredituppgifter o.d. för företag och enskilda
		Patientuppgifter
Meddelanden från EU efter offentliggörande		Hemligt EU-material i stora utskottet
Principer och anvisningar om informationssäkerheten		Lösningar avseende informationssäkerheten (kontroller och detaljuppgifter om dessa)
		Riksdagens katastrofplan
		Riksdagens beredskapsplaner och andra förberedelser
Upphandling och entreprenad, efter att avtal slutits. Meddelandet om upphandlingen är offentligt, när det har undertecknats eller bekräftats på annat sätt.	Anbud innan beslut om upphandling fattats	Upphandling och entreprenad som gäller säkerheten

Offentlig	För internt bruk	Hemlig
Typ av dator Antalet persondatorer De vanliga kontorsprogrammen		Detaljerad konfigurering av datorutrustningen; säkerhetsutrustningen
Datasystemet som helhet	Dokumenten och egenskaperna i de enskilda systemen	Säkerhetssystemen
	Arrangemang för tidsredovisning och passagekontroll	Riksdagens säkerhetsarrangemang i specialsituationer

Bilaga 2 Märkning av klassificeringen

Offentlig	För internt bruk	Hemlig
Ingen märkning	Skriv eller stämpla vid behov "För internt bruk" ("Sisäiseen käyttöön") på första sidan vid titeln på handlingen	Skriv eller stämpla vid behov "Hemlig" ("Salainen") på första sidan vid titeln på handlingen

Bilaga 3 Muntlig kommunikation

Kommunikationsteknik	För internt bruk	Hemlig
Telefonsamtal	Tillåtet	Vid behov så att utomstående inte hör
Dect-telefon, andra radiotelefoner (utan krypteringsanordning)	Tillåtet	Förbjudet
GSM-telefon	Tillåtet	Vid behov så att utomstående inte hör
Telefonsvarare, röstbrev	Tillåtet	Förbjudet
Samtal på allmänna färdmedel och offentliga platser	Bör undvikas, se till att ingen utomstående hör dig	Förbjudet

Bilaga 4 Informationshantering i elektroniska kommunikationssystem

Teknik	För internt bruk	Hemlig
Telefax (inkl. e-fax)	Tillåtet	Kontrollera att du valt rätt mottagarnummer och att faxet går fram med en provsändning. Skicka det egentliga meddelandet. (En namngiven mottagare eller dennes ombud måste stå vid mottagarapparaten.)
Telefax med krypteringsanordning	Tillåtet	Tillåtet
Intern e-post	Tillåtet	Tillåtet till dem som behöver informationen i sitt arbete
Extern e-post och e-brev	Tillåtet	Tillåtet endast om du använder en krypteringsteknik som riksdagens dataadministrationsbyrå godkänt
Riksdagens intranät (Fakta osv.)	Tillåtet	Tillåtet om åtkomsten begränsas till dem som är behöriga att se handlingen
Andra internettjänster	Tillåtet	Förbjudet

Bilaga 5 Hantering av pappershandlingar, ritningar, mikrofilm o.d.

Åtgärd	För internt bruk	Hemlig
Upprättande av sändlista (vanligen i slutet av handlingen)	De anställda som behöver informationen i arbetet	Endast de som absolut behöver informationen i sitt arbete, och dessutom måste de berörda personerna och grupperna nämnas på sändlistan
Övervakning av hur informationen används (ägare = informationsproducenten eller mottagaren av information utifrån)	Ägaren ger anvisningar vid behov	Ägaren eller dennes ombud (t.ex. en sekreterare) övervakar och för i anslutning till originalet förteckning över vem som fått informationen
Kopiering	Extra kopior kan tas efter behov i arbetet	De som står på sändlistan; någon på sändlistan eller dennes ombud, t.ex. sekreteraren, för bok över dem som fått extra kopior
Sändning per internpost	På samma sätt som normalpost, vid behov i slutet kuvert	Med kurir i slutet kuvert; märk kuvertet "personligt" ("henkilökohtainen") under mottagarens namn

Åtgärd	För internt bruk	Hemlig
Sändning per post	På samma sätt som normalpost i slutet kuvert	Endast med kurir
Öppning av försändelse	Mottagaren eller dennes ombud	Mottagaren eller dennes uttryckligen behöriga ombud för hemlig post (t.ex. en sekreterare)
Diarieföring	Enligt anvisningarna för diarieföring	Diariets offentlighet avgörs separat för varje meddelande. Anteckningen i diariet kan vara sekretessbelagd i sin helhet bara om också uppgiften om att ärendet har inletts är hemlig.
Arkivering	Enligt anvisningarna för arkivering	Bland de sekretessbelagda handlingarna
Lån	Kan utlånas för tjänsteändamål	Lånas inte ut
Förvaring på riksdagen	Vid behov i låst rum eller skåp	I låst rum, låda, skåp, kassaskåp, valv e.d.
Extern förvaring (hemma, på hotell osv.)	I låst utrymme	I låst rum, låda, skåp, kassaskåp, valv e.d.
Förvaring under resa	Om möjligt i låst portfölj	Alltid i låst portfölj som inte får lämnas ur sikte
Dokumentförstöring - vem? - hur?	De som står på sändlistan eller deras ombud, t.ex. en sekreterare eller expeditionsvakt, förstör dokumentet med en dokumentförstörare eller lägger det i ett låst uppsamlingskärl	De som står på sändlistan eller deras ombud, t.ex. en sekreterare, förstör dokumentet med en dokumentförstörare (remsorna får vara högst 0,8 mm x 20 mm) eller lägger det i ett låst uppsamlingskärl
Förstöring: stordia, skyddspapper, färgband - vem? - hur?	Den som innehar materialet lägger det i ett låst uppsamlingskärl	Den som innehar materialet lägger det i ett låst uppsamlingskärl eller förstör materialet med en dokumentförstörare (remsorna får vara högst 0,8 mm x 20 mm)

Bilaga 6 Hantering av information i elektronisk form

Åtgärd	För internt bruk	Hemlig
Hantering vid en arbetsstation i riksdagens övervakade lokaler.	Skärmsläckare med lösenord rekommenderas	Tillåtet bara när hanteringen pågår. Spara därefter informationen på ett datamedium, som ska förvaras i ett låst metall- eller kassaskåp
Hantering vid en arbetsstation i riksdagens övervakade lokaler och med uppkoppling till klassificerad information på nätet	Du måste ha ett personligt domännamn och lösenord	Du måste ha ett personligt domännamn och lösenord
Hantering vid en bärbar persondator som innehåller klassificerad information och transporteras utanför riksdagen	Du måste använda lösenordsskyddad skärmsläckare	Du måste använda datorlösenord och säkerhetsprogram Du måste använda skärmsläckare med lösenord Du ansvarar personligen för övervakningen
Fjärrhantering vid en arbetsstation med uppkoppling till klassificerad information på riksdagen	Du måste ha ett personligt domännamn och ett lösenord Du måste använda den uppkopplingsteknik som dataadministrationsbyrån godkänt	Du måste ha ett personligt domännamn och ett lösenord Du måste använda den uppkopplingsteknik som dataadministrationsbyrån godkänt
Hantering i ett informationssystem	Behörighetsmekanism baserad på personliga användarnamn och lösenord	Behörighetsmekanism baserad på personliga användarnamn och lösenord Dataadministrationsbyrån ska ha godkänt skyddet för informationssystemet
Kopiering och vidarebefordring	Beroende på behörighet Vidarebefordran beroende på vad som krävs för arbetet	Förbjudet
Utskrift på gemensam skrivare på riksdagen	Tillåtet	Utskriften ska övervakas av någon på sändlistan eller dennes ombud
Förvaring av datamedier[1] på riksdagen	Vid behov i ett låst rum eller skåp	I låst rum, låda, skåp, kassaskåp, valv e.d.
Förvaring av datamedier[1] utanför riksdagen: hemma, på hotell osv.	I låst utrymme	I låst rum, låda, skåp, kassaskåp, valv e.d.
Förvaring av datamedier[1] på resa	Om möjligt i låst portfölj	Alltid i låst portfölj som inte får lämnas ur sikte
Sändning av datamedier[1]	I sluten förpackning enligt sändlista t.ex. per post	Endast med kurir till namngiven mottagare personligen

Åtgärd	För internt bruk	Hemlig
Återanvändning (ny användare) av datamedier[1] på riksdagen	Tillåtet om - filen raderas (DEL-kommando) eller - datamediet formateras (FORMAT-kommando)	Förbjudet Datamediet måste förstöras om informationsägaren inte längre använder det
Förstöring av datamedier[1]	Gör mediet oanvändbart (bryt, böj e.d.)	Med datamedieförstörare
Radering av information från hårddisken i samband med datorbyte	Riksdagens helpdesk raderar informationen och initierar hårddisken	Användaren raderar filerna Riksdagens helpdesk raderar informationen och initierar hårddisken
Sändning av persondator för extern service	Hårddisken bör tas loss från persondatorn Återställande av informationen på hårddisken kräver överenskommelse från fall till fall och en tillförlitlig motpart	Riksdagens helpdesk tar loss hårddisken före servicen Återställande av informationen på hårddisken kräver överenskommelse från fall till fall och en tillförlitlig motpart

1) Med datamedium avses disketter, zipskivor, cd-romskivor, magnetband och andra mobila medier.

RIKSDAGENS E-POSTREGLER

Godkända av kanslikommissionen 11.11.2004

RIKSDAGENS KANSLIS PUBLIKATION 5/2005

SAMMANDRAG

Att tänka på!

- ✓ Följ allmänt accepterade nätikettregler för e-post.
- ✓ Ett e-postmeddelande är ett skriftligt dokument som någon annan kan behandla och kopiera.
- ✓ Den externa e-posttrafiken har ingen ångerfunktion.
- ✓ Respektera mottagarens e-brevlåda. Sänd inga kedjebrev, julhälsningar eller skämt i den interna e-posten.
- ✓ På internet är e-posten som en lapp på en offentlig anslagstavla – alla kan läsa den.
- ✓ E-postadressen måste vara exakt annars går meddelandet till fel person eller försvinner.
- ✓ Internet gör det möjligt att skicka e-post i någon annans namn.
- ✓ E-posten är avsedd för korta meddelanden som sparas under en överskådlig tid. Program och omfattande material ska skickas på annat sätt än per e-post.
- ✓ Det finns inga garantier för att eller när ett e-postmeddelande går fram. Om du vill försäkra dig om att mottagaren har fått ditt meddelande – be om kvittering.

FÖRORD

Riksdagens e-post är en viktig intern och extern kommunikationsform. Eftersom e-posten blir allt populärare har det uppkommit ett behov att lägga fast gemensamma spelregler för e-postanvändningen för att systemet ska fungera friktionsfritt. Tanken är att dessa regler ska vara till nytta i det syftet.

Reglerna har gjorts upp utifrån behoven riksdagen och dess ämbetsverk. De grundar sig på gällande lagstiftning och god informationshantering. Anvisningar som har gjorts upp på andra håll inom statsförvaltningen har också utnyttjats, liksom de etiska principer som formulerats bland aktiva internetanvändare.

Reglerna har kommit till på uppdrag av ledningsgruppen för riksdagens dataförvaltning och de har tagits fram av en arbetsgrupp som bestått av:

Datachef (till 30.5.2004) Kari T. Sipilä, riksdagens förvaltningsavdelning, ordförande
Utskottsråd Ritva Bäckström, riksdagens utskottssekretariat
Referendarieråd Jorma Kuopus, riksdagens justitieombudsmans kansli
Inspektionsråd Kaj Laine, statsrevisorernas kansli
Riksdagssekreterare Marja Wallin, riksdagens centralkansli
Planerare Outi Juntura, riksdagens förvaltningsavdelning.

Arbetet har präglats av en god och konstruktiv anda. Debatten om reglernas utformning var mycket livlig och hade många intressanta infallsvinklar. Arbetsgruppen ville formulera bra, tydliga och lättlästa regler med välgrundade och begripliga anvisningar för hur e-posten ska användas.

Helsingfors den 24 maj 2004

Kari T. Sipilä

INLEDNING

Bakgrund

Riksdagens e-postregler innehåller allmänna anvisningar för användningen av e-post i intern kommunikation, i kommunikationen mellan riksdagen och medborgarna/kunder samt i kommunikationen myndigheter emellan.

Reglerna uttrycker samtidigt riksdagens e-postpolicy.

Utgångspunkter för användningen

Avsikten med e-post var ursprungligen att förmedla korta meddelanden som sparas under en kort tid. E-posten fungerar bäst i intern kommunikation. Numera har man också börjat överföra större material med e-post. Det finns inga internationella överenskommelser om förmedling av e-post och inte heller en enda ansvarig operatör, utan principerna för att skicka e-post baserar sig på ett enhetligt kommunikationsprotokoll. Även om e-postprotokollet är bristfälligt när det gäller kryptering av meddelanden och deras integritet används e-post över hela världen i elektronisk kommunikation.

Det är därför all orsak att undvika att skicka känsliga uppgifter i externa e-postmeddelanden. Sekretessbelagd information får inte skickas med e-post utan kryptering.

Terminologi

Med intern e-post avses e-posttrafik mellan användare i riksdagens e-postsystem.

Med extern e-post avses e-posttrafik som går ut på internet från riksdagens e-postsystem eller som kommer in i e-postsystemet från internet.

Med elektroniskt meddelande avses information som har sänts med en elektronisk dataöverföringsmetod på det sätt som avses i lagen om elektronisk kommunikation i myndigheternas verksamhet. Gränsen mellan ett meddelande och ett dokument är inte alltid entydig. Beroende på sammanhanget kan ett meddelande också vara ett dokument.

Med elektroniskt dokument avses ett elektroniskt meddelande som hänför sig till anhängiggörandet eller behandlingen av ett ärende eller till delgivningen av ett beslut.

1 INTERN KOMMUNIKATION

Du kan lita på att ett meddelande som skickats inom riksdagens e-postsystem går fram, att systemet fungerar och är säkert samt att sekretessen bibehålls. Det interna e-postsystemet erbjuder färdiga sändlistor vilket minskar risken för att ett meddelande går till fel person. Den interna kommunikationen kan omfatta sändande av handlingar, meningsutbyte eller information genom sändlistor.

2 EXTERN KOMMUNIKATION

Den externa kommunikationen går från riksdagen via internet till mottagaren eller från en avsändare via internet till riksdagen. Det väsentliga är att meddelandet passerar internet. Riksdagens dataadministrationsbyrå har inga möjligheter att garantera meddelandenas säkerhet eller deras väg över internet. När det uppstår fel är det arbetskrävande och ofta rentav omöjligt att reda ut varför ett meddelande har dröjt eller försvunnit. Det finns inte någon särskild operatör som har ansvar för internet och inte heller någon internationell överenskommelse för att säkerställa internets funktionsduglighet. Det enda man har kommit överens om är dataöverföringsstandarder och hur de ska följas.

2.1 Officiella kontakter med ministerier

Ministerierna har upprättat egna regler för sin e-postanvändning. E-posttrafiken mellan ministerierna och riksdagen sker via statsrådets kanslis slutna nät och inte över internet. Statsrådets kanslis nät är ett fysiskt separerat och säkert nät som omfattar alla ministerier. Även om kontakten med statsrådets kanslis nät är bruten överförs inte e-postmeddelandena via internet till ministerierna. Konfidentiellt och officiellt material kan sålunda förmedlas per e-post från och till följande myndigheter (uppgifterna uppdaterade 20.5.2004):

- vn.fi och vnk.fi – statsrådets kansli
- vm.fi – finansministeriet
- tpk.fi – republikens presidents kansli
- mmm.fi – jord- och skogsbruksministeriet
- vyh.fi och miljo.fi – miljöministeriet
- formin.fi – utrikesministeriet
- mintc.fi – kommunikationsministeriet
- intermin.fi – inrikesministeriet
- mol.fi – arbetsministeriet
- bof.fi – Finlands Bank rata.bof.fi,
- rata.bot.fi och rahoitustarkastus.fi – Finansinspektionen
- stm.fi – social- och hälsovårdsministeriet

- minedu.fi – undervisningsministeriet
- om.fi – justitieministeriet
- okv.fi – justitiekanslersämbetet
- ktm.fi – handels- och industriministeriet

2.2 E-post från medborgarna till riksdagen

Vid behov kan alla e-postärenden mellan myndigheter, organisationer och medborgare skötas via officiella e-postadresser. Riksdagens officiella e-postadresser är:

- eduskunta@eduskunta.fi
- kirjaamo@eduskunta.fi
- eoa-kirjaamo@eduskunta.fi
- valtiontilintarkastajat@eduskunta.fi
- kirjaamo@vtv.fi
- eduskunta@riksdagen.fi
- kirjaamo@riksdagen.fi
- eoa-kirjaamo@riksdagen.fi
- statsrevisorerna@riksdagen.fi

De meddelanden som kommer in till de officiella adresserna genomgår inte någon filtrering med avseende på skräppost eller innehåll, däremot raderas automatiskt alla e-post-meddelanden som har virus. Den som sköter e-brevlådan för en officiell adress är skyldig att gå igenom all e-post som har kommit in.

3 PRINCIPERNA FÖR HANTERING AV E-POST

3.1 E-postadresserna och hur de publiceras

Riksdagens e-postadresser kan antingen vara privata (förnamn.efternamn@riksdagen.fi), officiella (kirjaamo@riksdagen.fi) eller relatera till kundservicefunktioner (t.ex. virastoavustajat, turvallisuus). Det går inte att skicka e-post till internet från de sist nämnda adresserna. Den privata e-postadressen (förnamn.efternamn@riksdagen.fi) fungerar också på finska (eduskunta.fi), engelska (parliament.fi) och franska (parlement.fi).

I Julha-registret hittar du samtliga e-postadresser till riksdagen och dess ämbetsverk (http://www.julha.fi).

3.2 Användarnamn och lösenord

Alla anställda vid riksdagen och dess ämbetsverk samt riksdagsledamöterna får ett användarnamn förutsatt att deras anställningsförhållande är minst en månad långt. Användaren ansvarar själv i alla sammanhang för sitt användarnamn och dess användning. Ge därför inte ut lösenordet till ditt användarnamn. När du är ledig måste du själv se till att din vikarie har rätt att använda din e-brevlåda.

E-postsystemets lösenord ska bytas var sjätte månad eller vid behov oftare. Välj ett lösenord som har minst åtta tecken och som utomstående inte kan gissa sig till. Lösenordet är enbart avsett för personligt bruk.

3.3 Hantering av officiell e-post

Avsikten med e-post är framför allt att förmedla meddelanden och spara dem under en kort tid. Elektronisk kommunikation kan ske antingen med elektroniska meddelanden eller elektroniska dokument. Med elektroniska meddelanden avses information som har sänts med en elektronisk dataöverföringsmetod. Med elektroniska dokument avses ett elektroniskt meddelande som hänför sig till anhängiggörandet eller behandlingen av ett ärende eller till delgivningen av ett beslut. Ibland kan det vara svårt att avgöra om det rör sig om ett meddelande eller ett dokument. Beroende på sammanhanget kan ett meddelande också vara ett sådant dokument som avses i lagen om offentlighet i myndigheternas verksamhet.

E-post som har sänts till de officiella e-postadresserna (eduskunta@riksdagen.fi, kirjaamo@riksdagen.fi, eoa-kirjaamo@riksdagen.fi, statsrevisorerna@riksdagen.fi och kirjaamo@vtv.fi) ska vidarebefordras till dem som sköter ärendet. Om möjligt ska också svaren sändas från en officiell e-postadress.

Den som sänder ett e-postmeddelande ansvarar själv för meddelandet och för att det kommer fram inom utsatt tid. Avsändaren ska också själv se till att meddelandet sänds till rätt adress. På internet kan ett enda felaktigt tecken resultera i att posten går till fel adress, förutsatt att den felaktiga adressen existerar. För att minska osäkerhetsfaktorerna i ansvarsfrågan ska den som sköter en officiell e-postlåda omedelbart underrätta avsändaren om att meddelandet/dokumentet har tagits emot, om det inte rör sig om sådan skräppost som avses i punkt 6.2. Efter att avsändaren har underrättats övergår ansvaret för meddelandet och dess behandling på mottagaren. Om du själv får officiell e-post till din egen e-brevlåda ska du genast styra den till en officiell e-postadress.

Av informationssäkerhets- och kommunikationstekniska skäl är det inte tillåtet att sända eller automatstyra offentlig e-post till en privat e-postadress (i ett externt e-postsystem såsom luukku, hotmail, yahoo).

3.4 Hantering av privat e-post

Användningen av e-post på arbetsplatser, också i riksdagen, aktualiserar frågor kring arbetstagarnas och tjänstemännens integritetsskydd. Om ett e-postmeddelande är privat kan det vara motiverat att skriva "Personligt/Privat" i rubrikfältet. Det finns också skäl att i den interna e-posten definiera meddelandets konfidentialitetsnivå (privat, internt, vanligt). Om avsändaren i den interna e-posten i fältet "egenskaper" (ominaisuudet) har skrivit privat, får det inte sändas vidare automatiskt och inte heller läsas av en person som eventuellt har fått s.k. sekreterarrättigheter, dvs. rätt att läsa meddelanden i mottagarens e-brevlåda.

Kom ihåg att *e-posttrafiken mellan riksdagen och utomstående e-postsystem inte är krypterad*. Sänd därför inga konfidentiella eller känsliga personuppgifter t.ex. om någons hälsotillstånd i ett privat e-postmeddelande till utomstående e-postsystem.

Det är tillåtet för de anställda att skaffa sig privata e-postadresser (t.ex. till en browserbaserad gratis e-post) och använda dem i riksdagens datorer.

3.5 E-postmeddelanden som kommer till fel adress

Om du får ett e-postmeddelande som är avsedd för en annan person får du inte yppa något om meddelandet eller utnyttja det.

Om en myndighet/tjänsteman får ett e-postmeddelande som är avsett för en annan myndighet ska det överföras till den rätta myndigheten på det sätt som sägs i förvaltningslagen.

Ett e-postmeddelande som är avsett för en annan person (t.ex. din namne) ska styras till den rätta adressen, om du känner till den. Om du inte har den rätta

adressen förutsätter god nätikett att du upplyser avsändaren om att han eller hon har skickat sitt meddelande till fel person. Du ska också radera meddelandet.

Om din e-postadress ändras (t.ex. nytt efternamn) går all e-post som kommer in på din gamla adress till den nya adressen under en månad. Under denna månad ska du själv meddela din nya adress till dem du brukar ha e-postkontakt med.

3.6 Förfarande när en e-postanvändare är borta tillfälligt/för en viss tid

Vid en förutsebar frånvaro för en viss tid, t.ex. vid tjänstledighet, stängs e-posten. Den som har fjärråtkomst till e-posten har tillgång till sin e-post också under sådan frånvaro. När ett tjänsteförhållande/anställningsförhållande upphör, upphör också rätten att använda e-posten. Du ska själv meddela din nya e-postadress till dem du brukar ha e-postkontakt med.

I lagen om integritetsskydd i arbetslivet föreskrivs att arbetsgivaren under arbetstagarens tillfälliga eller tidsbestämda frånvaro med arbetstagarens samtycke får reda ut och öppna meddelanden som har inkommit till arbetstagaren eller som denne har sänt och som hört till arbetsgivaren. Lagen innehåller också bestämmelser om när och hur sådana meddelanden kan öppnas utan arbetstagarens samtycke (se 6 kap. 18-20 § i lagen om integritetsskydd i arbetslivet).

3.7 Förfarande vid dödsfall

Om en anställd avlider stänger dataadministrationsbyrån den avlidnes e-post och raderar all post.

3.8 Vidarebefordring av e-post

Automatisk vidaresändning av e-post från riksdagens e-postsystem är alltid förbjudet. Detta för att informationssäkerheten och kommunikationerna ska fungera så bra som möjligt. Förbudet gäller

- vidaresändning till en privat e-postadress under ledigheter,
- vidaresändning till en annan e-postadress under tjänstledighet eller
- vidaresändning av meddelanden från en allmän adress till en utomstående privat e-postadress.

Riksdagsanställda kan tryggt fjärranvända e-posten från vilken som helst internetuppkopplad dator med en tillräcklig säkerhetsnivå, dvs. en dator som tillåter krypterade HTTPS-förbindelser. Den som vill fjärranvända e-posten på detta sätt behöver dessutom ett autentiseringskort, vilket i sin tur förutsätter förvaltningsdirektörens tillstånd till fjärranvändning.

3.9 Rensa i e-brevlådan

Riksdagens e-brevlådor för användare är 70 Megabyte (20.5.2004). Ett snabbt och fungerande e-postsystem förutsätter att nya meddelanden blir lästa eller antecknade som lästa och att så få meddelanden som möjligt (högst 500 meddelanden) sparas i mappen för inkomna meddelanden (saapuneet). För att e-postsystemet inte ska överbelastas raderas varje lördag från alla användares mappar för inkomna och utgående meddelanden (saapuneet ja lähtevät) e-postmeddelanden som är äldre än sex månader. Den som vill spara meddelanden längre än sex månader ska flytta dem till andra mappar. Ett fungerande mappsystem dit meddelanden flyttas är ett bra sätt att skapa ordning och reda i e-posten.

3.10 Sändlistor

Meddelanden på basis av omfattande sändlistor (t.ex. "eduskunta") bör med hjälp av e-postens schemafunktion inskränkas till lugna tider. Det är förbjudet att använda e-posten för privat annonsering till hela personalen (jag köper/jag säljer/uthyres). För sådana ändamål har vi intranet (Fakta, sisäpiiri) eller SRV:s forum. Undvik att sända julhälsningar till hela personalen.

3.11 Elektronisk signatur

Riksdagens e-postsystem stöder S/MIME-standarden som möjliggör kryptering av meddelanden och elektronisk signatur. Signaturen skyddar meddelandets integritet (= förändringsskydd) och verifierar avsändaren. Men riksdagen har ännu inte gått in för kryptering av e-posten och elektronisk signatur t.ex. med ett elektroniskt id-kort. Sekretessbelagt material ska därför inte sändas per e-post via internet.

4 E-POST OCH INFORMATIONSSÄKERHET

Varken e-postmeddelanden eller bilagor kan garanteras grundläggande skydd och säkerhet när de passerar internet. Den behövliga informationssäkerheten måste skapas separat. De generella kraven på säkerhet är:

- Sekretess – informationen finns tillgänglig endast för behöriga personer.
- Integritet - informationen förvanskas inte på vägen.
- Spårbarhet – parterna kan identifieras med säkerhet.
- Tillförlitlighet – parterna kan identifieras i efterskott och det kan påvisas att de har skrivit meddelandet såsom det framstår.
- Tillgänglighet – tjänsterna kan alltid utnyttjas vid behov.

Andra problem i anslutning till e-postens säkerhet är:

- virus
- skräppost
- försvunna meddelanden
- dröjsmål med frambefordringen av meddelanden

Inget tekniskt system är så vattentätt att alla dessa brister i informationssäkerheten kan elimineras, utan riskerna måste accepteras som en del av e-postens egenskaper, och e-posten bör användas med beaktande av dem. Riskerna kan visserligen reduceras med riktiga förfaringssätt och en fungerande administration för e-posten. Varje användare ansvarar för egen del för att främja informationssäkerheten i e-postanvändningen.

5 UNDERHÅLL AV E-POSTEN

E-posten måste underhållas för att funktionssäkerheten ska garanteras. Därför vidtas åtgärder för att förhindra möjligheten att ta emot skadliga program och skräppost. Vid behov begränsas dessutom bilagornas storlek.

5.1 Begränsning av e-postmeddelandenas och bilagornas storlek

Dataadministrationsbyrån har rätt att definiera begränsningar för e-postmeddelanden och bilagor. En form av begränsning är t.ex. att filtrera bort alltför stora (över 20 Megabyte, över 50 bilagefiler) meddelanden och filer eller meddelanden och filer som skadar eller äventyrar riksdagens informationssäkerhet – såsom program av typen exe, bat, com, javascript m.fl. Användarna informeras om dessa begränsningar.

Riksdagen iakttar god informationshantering och dataadministrationsbyrån kontrollerar därför genom olika program meddelanden och bilagor för att upptäcka eventuella virus och andra skadliga program. Dataadministrationsbyrån är skyldig att från inkommande och utgående e-posttrafik eliminera meddelanden och bilagor som innehåller virus eller andra skadliga program.

Riksdagen har ett heltäckande antivirusprogram. Programmen finns på e-postservrarna och användarnas datorer. Dataadministrationsbyrån försöker hålla sig à jour med vilka virus som är på gång. Om, mot förmodan, något virus, en mask eller något annat skadligt program lyckas tränga sig igenom riksdagens virusbekämpningssystem informerar dataadministrationsbyrån om detta och vidtar omedelbart åtgärder för att bli av med viruset. Det finns ingen anledning att skicka vidare e-postmeddelanden som varnar för virus. Meddelandena är i allmänhet falska larm som kan jämställas med skräppost. Om du misstänker att din dator har drabbats av ett virus eller ett skadligt program ska du underrätta dataadministrationsbyråns helpdesk (Atk-tuki).

5.2 Skräppost

Med skräppost eller spam avses all oönskad e-post, i allmänhet reklampost, som sänds till en stor mängd mottagare utan deras samtycke. I takt med den ökade internetanvändningen har avsiktlig störning av e-posten blivit ett allvarligt problem. För närvarande finns det rentav färdiga s.k. spamprogram som möjliggör massiva störningar av e-postsystemet. För den vanliga användaren tar sig störningarna uttryck i ökad post som leder till att e-posten fungerar långsammare eller kanske inte alls. Ett annat sätt att störa posten är att sända meddelanden i användarnas namn och att fylla brevlådan.

Besvara aldrig skräppost. Om du svarar avslöjar du att adressen fungerar, vilket ökar risken för att ditt namn kommer med på andra sändlistor för skräppost.

Dataadministrationsbyrån försöker med tekniska åtgärder minska skräppostproblemet genom att förhindra mottagning av post från kända skräppostsservrar. Skräppostspärrarna täcker riksdagens hela e-postsystem. Den enskilda användaren kan dessutom med hjälp av en s.k. agent i Teamwears e-postprogram Tiimiposti skapa egna spärrar.

Det är förbjudet att inom riksdagens e-postsystem eller från riksdagens system skicka skräppost, olagligt material eller material som strider mot god sed (t.ex. kränkande, rasistiskt eller sårande material).

5.3 Övervakningen av e-posten och datanätet

För att trygga informationssäkerheten och systemets funktioner övervakar dataadministrationsbyrån e-posten. Meddelandesekretessen eller användarintegriteten kränks inte i övervakningen. Inte heller den övriga övervakningen av nätanvändningen kränker grundlöst användarnas integritet. Under speciella förhållanden kan det bli nödvändigt att detaljutreda användningen.

5.4 Hur logginformationen från e-posten och nätanvändningen samlas in och sparas

I riksdagen utnyttjas logginformationen endast av underhållspersonalen för uppgifter av teknisk natur. Personalen har tystnadsplikt. De uppgifter som avses här är t.ex. åtgärder för att säkerställande av servicenivån samt utredning och statistikföring av störningar.

Dataadministrationsbyrån kan överlåta spårinformation till t.ex. Kommunikationsverket (www.ficora.fi) i samband med att kränkningar av informationssäkerheten eller akuta attacker mot nätets funktioner utreds. Motsvarande uppgifter kan också lämnas till andra systemoperatörer i Finland. Med spårinformation avses här t.ex. exakt logginformation om attackkontakter. Samtidigt kan det vara nödvändigt att lämna uppgifter i anslutning till ett enskilt användarnamn. Uppgiftslämningen begränsas alltid till sådana användarnamn som på goda grunder kan antas ha kommit i fel händer eller vars innehavare kan antas ha gjort sig skyldig till det brott som är föremål för utredning. Uppgiftsöverlåtelserna registreras.

5.5 Underhållspersonalens ansvar

Helpdesken ber alltid den användare som instrueras om lov att genom fjärranvändning komma in på användarens skärm. Helpdesken har tystnadsplikt också när personalen genom fjärranvändning opererar i användarens dator.

Dataadministrationsbyrån utser de personer som ansvarar för riksdagens e-postsystem. Med e-postsystemet avses serversystemet som omfattar maskinvaran och reservprogrammen, särskilt e-postserverprogrammen, dataöverföringsförbindelserna, de e-postmeddelanden som hanteras av servern samt hanteringsreglerna.

Till underhållspersonalen hör de personer som på grund av sitt arbete kommer åt logginformation och andra personers meddelanden. De har tystnadsplikt och de har förbundit sig att iaktta reglerna för underhållspersonal.

6 LAGSTIFTNING

I en bilaga till dessa regler finns en sammanfattning av lagstiftning som har samband med e-postanvändning i arbetslivet. Lagstiftningen redovisas genom att innehållet i författningarna och deras betydelse för e-posten refereras kort. Tanken är att för dem som är intresserade ge en samlad bild av lagstiftningsbasen. Den arbetsgrupp som beredde dessa regler fann det även viktigt att som grund för sitt eget arbete reda ut lagstiftningsbasen. Riksdagens e-postregler fungerar ändå som ett självständigt avsnitt och förutsätter inte att läsaren fördjupar sig i själva lagstiftningen.

7 NÄTIKETT

Internet och e-posten är utmärkta arbetsredskap både när det gäller att söka information och hålla kontakt med andra. Det är ändå alltid bra att komma ihåg att både e-posten och internet är väldigt oskyddade och informationen rör sig okrypterad i ett offentligt nät. På Internet är din e-post som en offentlig anslagstavla – den kan läsas av alla.

Det är lätt att förvanska en okrypterad och osignerad e-post. Vem som helst kan sända e-post i någon annans namn och det är inte helt fel att vara lite misstänksam mot inkommande e-post.

Det finns inga garantier för att e-posten når mottagaren eller hur snabbt det går. Det är alltid avsändaren som ansvarar för att ett meddelande når fram. Ett bra sätt att säkerställa detta är att förse sitt meddelande med en uttrycklig begäran om kvittering.

Ett e-postmeddelande är ett skriftligt dokument som kan sparas länge. Meddelandet måste med andra ord tåla hantering i många nya sammanhang. Ett allmänt råd på vägen är att du inte ska skriva något sådant i e-posten som du inte kan säga direkt till den det berör.

Det är mycket lätt att kopiera och vidarebefordra post till utomstående utan att den som sänt ett meddelande vet om detta. Också detta är bra att minnas när man skriver e-postmeddelanden. Innan du vidarebefordrar eller skriver ut/distribuerar ett meddelande ska du tänka efter om det eventuellt var avsett endast för dig.

Respektera mottagarens brevlåda. Låt bli att vidarebefordra kedjebrev. Stora utskick, t.ex. julhälsningar, belastar både e-postsystemet och mottagarens e-brevlåda.

En e-postadress är värdefull egendom. Det är inte lätt att byta den och ofta medför ett byte också en hel del besvär. Skräppost kan förstöra din e-postadress och

göra den oanvändbar. Håll därför noga reda på din privata e-postadress och tänk efter två gånger innan du ger ut den till någon. Vanligen lönar det sig att vara återhållsam med att lämna uppgifter när man registrerar sig i någon internet-tjänst.

Läs mera om nätikett:

- http://tuki.elisa.net
- http://www.passagen.se

Exempel på informationssäkerhetsanvisningar:

- http://www.tieke.fi/tietoturvaopas/opas.html

8 KÄLLOR

- Internet-datasäkerhetsanvisning för statens informationsförvaltning, Ledningsgruppen för datasäkerhet inom statsförvaltningen 1/2003
- Direktiv om hantering av elektronisk post och logguppgifter, Ledningsgruppen för datasäkerhet inom statsförvaltningen 5/2001
- Arkivverkets/Riksarkivets/gällande föreskrifter, anvisningar och rekommendationer i Internet
- http://www.narc.fi/sve/ohjeet.html och
- http://www.narc.fi/johto/hyvatiedon-hallinta2.pdf
- JHS 132. Rekommendation av delegationen för informationsförvaltningen inom den offentliga förvaltningen.
- Hantering av informationssystem och material i elektrisk form. Föreskrift och anvisning 126/40/01, 22.5.2001 (Arkivverket, normen gäller 1.7.2001-30.6.2005).
- Arkivfunktionens krav vid hantering av elektronisk post. Riksarkivets Föreskrift och anvisning 5/06/97, 19.11.1997

Lagar, förordningar och principbeslut

- Finlands grundlag (731/1999)
- Förvaltningslagen (434/2003)
- Personuppgiftslagen (523/99)
- Språklagen (423/2003)
- Lag om elektronisk kommunikation i myndigheternas verksamhet (13/2003)
- Lag om elektroniska signaturer (14/2003)
- Lag om integritetsskydd vid telekommunikation och dataskydd inom televerksamhet (565/1999)
- Lag om integritetsskydd i arbetslivet (477/2001), revideras 2004, RP 162/2003 rd
- Lag om offentlighet i myndigheternas verksamhet (621/1999)

- Arkivlagen (831/1994)
- Lag om riksdagens tjänstemän (1197/2003)
- Statsrådets principbeslut om om möjligheterna att uträtta ärenden elektroniskt, utveckla tjänster och minska insamlandet av data, 5.2.1998

BILAGA

Lagstiftning om e-postanvändning

E-postreglerna kompletteras med en sammanhållen och kortfattad redogörelse för den lagstiftning som har relevans för e-postanvändaren eller den som underhåller e-posten. Bestämmelserna omfattar allt från den grundlagsskyddade meddelandesekretessen till myndigheternas skyldighet att iaktta en god förvaltning. Det finns också särskilda bestämmelser om dataskydd i arbetslivet. Den nya lagen om dataskydd vid elektronisk kommunikation innehåller viktiga bestämmelser om e-postanvändning. Också de bestämmelser som gäller myndigheters handlingar, god informationshantering samt arkivering bör beaktas. Elektronisk kommunikation i myndighetsutövning kan ordnas på olika sätt och bestämmelserna om detta gäller också e-postanvändningen.

Finlands grundlag

Sekretessen i fråga om förtroliga meddelanden är en grundläggande rättighet. Enligt 10 § i grundlagen är vars och ens privatliv, heder och hemfrid tryggade. Också brev- och telefonhemligheten samt hemligheten i fråga om andra förtroliga meddelanden är okränkbar. Enligt lagens förarbeten (RP 309/1993 rd) är syftet med bestämmelsen att skydda förtroliga meddelanden med avseende på utomstående. Bestämmelsen skyddar samtidigt andra uppgifter i anslutning till sådana meddelanden, exempelvis identifikationsuppgifter. Bestämmelsen om förtroliga meddelanden är så extensivt utformad att den så väl som möjligt ska kunna tillämpas också på de nya former av kommunikation som följer av den ständigt pågående utvecklingen på området. Bestämmelsen gäller också kommunikation i olika typer av datanät såsom e-post. Meddelanden som avsänts och mottagits per e-post omfattas alltså av skyddet.

Den ovan nämnda bestämmelsen skyddar förtrolig kommunikation mot olagliga ingrepp. Det här innebär att en arbetsgivare inte har tillgång till en arbetstagares meddelanden i datanätet eftersom kommunikationen vid sidan av meddelanden som klart hänför sig till arbetsuppgifterna också kan innehålla förtroliga meddelanden. I lagen om integritetsskydd i arbetslivet (759/2004) föreskrivs om när arbetsgivaren har rätt att ta fram och i vissa fall öppna ett meddelande som avsänts från/inkommit till arbetstagarens e-post.

Genom lag kan också i övrigt bestämmas om sådana begränsningar i meddelandehemligheten som är nödvändiga vid utredning av brott som äventyrar individens eller samhällets säkerhet eller hemfriden, vid rättegång och säkerhetskontroll samt under frihetsberövande.

I 21 § 2 mom. i grundlagen föreskrivs att garantier för en god förvaltning ska tryggas genom lag. Kraven på god förvaltning innebär exempelvis att en myn-

dighet i alla kontakt med sina kunder, inklusive elektronisk kommunikation, ska följa serviceprincipen. I förvaltningslagen (434/2003) och i lagen om elektronisk kommunikation i myndigheternas verksamhet (13/2003) finns närmare föreskrifter om god förvaltning.

Förvaltningslagen

Den nya förvaltningslagen (434/2003) som reglerar uträttande av ärenden och behandling av förvaltningsärenden hos myndigheter trädde i kraft den 1 januari 2004. Lagen bekräftade vedertagen praxis när det gäller god förvaltning men förde också med sig nya aspekter. I den nya lagen finns föreskrifter t.ex. om förfarandet när handlingar sänds till en myndighet och från en myndighet till kunden.

Förvaltningslagens 7 § förpliktar myndigheterna att följa serviceprincipen och ge adekvat service. I lagens 8 § föreskrivs om myndigheternas skyldighet att inom ramen för sin behörighet och enligt behov ge sina kunder råd i anslutning till skötseln av ett förvaltningsärende samt svara på frågor och förfrågningar som gäller uträttandet av ärendet. Rådgivningen ska vara avgiftsfri. Om ett ärende inte hör till myndighetens behörighet, ska den i mån av möjlighet hänvisa kunden till den behöriga myndigheten. God förvaltningssed innebär också att myndigheten inom skälig tid ska ge ett sakligt svar på tillräckligt individualiserade förfrågningar och andra kontakter från kunderna. Dessa skyldigheter gäller inte enbart de traditionella formerna av kommunikation utan även kommunikation genom e-post eller andra elektroniska dataöverföringsmetoder.

Enligt 17 § tillställs en handling på avsändarens eget ansvar den i ärendet behöriga myndigheten under dess kontaktadress. Det är också avsändaren som ska se till att handlingen kommer in till myndigheten inom tidsfristen. Enligt 23 § ska en myndighet dessutom på en parts begäran uppge när ett avgörande kan förväntas samt besvara förfrågningar om hur behandlingen fortskrider. En myndighet som av misstag har tillställts en handling för behandling av ett ärende i vilket myndigheten inte är behörig ska utan dröjsmål överföra handlingen till den myndighet som den anser vara behörig (21 §). Detta gäller både handlingar på papper och elektroniska handlingar.

Språklagen

Syftet med språklagen är att vars och ens rätt till rättvis rättegång och god förvaltning garanteras oberoende av språket samt att individens språkliga rättigheter förverkligas utan att han eller hon särskilt behöver begära det. Detta gäller både sedvanliga sätt att kommunicera och elektronisk kommunikation. I 27 § i språklagen fastställs att i skriftväxling mellan statliga myndigheter används finska, om inte den mottagande eller avsändande myndigheten är enspråkigt svensk eller det av någon annan orsak är mer ändamålsenligt att använda svenska eller något annat språk. I lagen föreskrivs dessutom om vissa situationer där mottagarens språk ska användas.

Lag om elektronisk kommunikation i myndigheternas verksamhet

Syftet med lagen om elektronisk kommunikation i myndigheternas verksamhet **(**13/2003**)** är att genom främjande av elektroniska dataöverföringsmetoder göra uträttandet och behandlingen av ärenden smidigare och snabbare. Också på annat ställe i lag finns ett flertal specialbestämmelser om elektronisk kommunikation.

Med elektroniska dataöverföringsmetoder avses elektroniska blanketter, elektronisk post och rätten att använda elektroniska datasystem, dvs. fasta tekniska uppkopplingar till datasystem. Lagen innehåller bestämmelser om myndigheternas och kundernas rättigheter, skyldigheter och ansvar vid elektronisk kommunikation. Lagen tillämpas när ärenden väcks, behandlas och avgöranden delges.

Konsekvenserna av lagen är att ett e-postmeddelande jämställs med ett brev som tillställs en myndighet och med annan kontakt i pappersform. Meddelandets rättsliga ställning beror på dess innehåll. Avgörande är om ett ärende kan hänföras till myndighetens behörighetsområde och uppgifter.

I lagen fastställs att en myndighet som har behövlig teknisk, ekonomisk och övrig beredskap inom ramen för den ska erbjuda var och en möjlighet att i syfte att anhängiggöra ärenden eller för behandlingen av dem sända meddelanden till en elektronisk adress eller specificerad anordning angivna av myndigheten. Dessutom ska var och en erbjudas möjlighet att i elektronisk form sända myndigheten anmälningar som den enligt gällande bestämmelser ska tillställas, utredningar och andra motsvarande handlingar som den begärt samt andra meddelanden.

Myndigheterna ska enligt lagen sträva efter att använda maskinvara och programvara som ur kundernas synvinkel i tekniskt hänseende är så kompatibel och lätt att använda som möjligt. Myndigheterna ska dessutom säkerställa att datasäkerheten både i kommunikationen med kunden och i informationsutbytet mellan myndigheterna är tillräcklig.

Av lagen framgår vidare att elektroniska meddelanden sänds till myndigheterna på avsändarens ansvar (8 §). Avsändarens rättsliga ställning tryggas i detta hänseende av att en myndighet enligt lagen utan dröjsmål ska meddela avsändaren av ett elektroniskt dokument att dokumentet har mottagits (12 §). Meddelandet kan sändas i form av en automatisk kvittens via datasystemet eller på något annat sätt. Enligt 21 § ska elektroniska dokument arkiveras på ett sådant sätt att det senare går att visa att de är autentiska och till innehållet oförändrade.

I 9 § finns bestämmelser om krav på underskrift. Ett elektroniskt dokument som inkommit till en myndighet behöver inte kompletteras med en underskrift om dokumentet innehåller uppgifter om avsändaren och om det inte finns anledning att betvivla dokumentets autenticitet och integritet. Om det enligt lag i ett ärende krävs en undertecknad handling, uppfylls kravet på underskrift också genom en

sådan elektronisk signatur som avses i 18 § i lagen om elektroniska signaturer (14/2003).

Elektronisk kommunikation kan inom lagens ram ordnas på det sätt som myndigheten anser bäst. En möjlighet är att använda elektronisk post. Ett problem med e-postsystemet som inte har kunnat lösas genom lagbestämmelser är den ökande mängden störande post. De problem som sammanhänger med datasäkerheten och behovet att filtrera e-postmeddelanden har gjort att utnyttjande av e-post vid elektronisk kommunikation inte är helt problemfritt. Principen om god förvaltning förutsätter nämligen att myndigheternas tillgänglighet tryggas.

Lagen om offentlighet i myndigheternas verksamhet

I lagen om offentlighet i myndigheternas verksamhet (621/1999) föreskrivs om myndighetshandlingars offentlighet, vars och ens rätt att ta del av handlingar och myndigheternas skyldighet att trygga öppenhet och god förvaltningssed i sin verksamhet. I lagen finns också bestämmelser om grunderna för sekretess samt allmänna grunder för under vilka villkor sekretessbelagda uppgifter kan lämnas ut.

Det är bra att komma ihåg att även ett meddelande som sänts eller mottagits per e-post kan vara en i lagen avsedd myndighetshandling, förutsatt att uppgifterna i ett meddelande hänför sig till myndighetens uppgifter. Med myndighetshandling avses i lagen en handling som innehas av en myndighet och som har upprättats av myndigheten eller av någon som är anställd hos en myndighet eller som har inkommit till en myndighet för behandling av ett visst ärende eller i övrigt inkommit i samband med ett ärende som hör till myndighetens verksamhetsområde eller uppgifter. En handling anses ha blivit upprättad av en myndighet även när den har upprättats på uppdrag av myndigheten. En handling anses ha inkommit till en myndighet även när den har inkommit till den som verkar på uppdrag av myndigheten eller i övrigt för myndighetens räkning, för att denne ska kunna utföra sitt uppdrag.

Som myndighetshandlingar betraktas däremot inte brev och andra handlingar som har sänts till en anställd hos en myndighet eller till en förtroendevald med anledning av något annat uppdrag eller någon annan ställning som han eller hon innehar. Inte heller handlingar som en myndighet har skaffat för intern utbildning, informationssökning eller annan därmed jämförbar intern användning betraktas som myndighetshandlingar.

När det gäller innehållet i e-postmeddelanden förutsätter tillämpningen av lagen att skyldigheten att beakta synpunkter som hänger samman med ett meddelandes/en handlings offentlighet, bevarande och sekretess beaktas.

I 18 § finns bestämmelser om myndigheternas skyldighet att genomföra en god informationshantering. En myndighet ska se till att dess handlingar och datasystem samt uppgifterna i dem är behörigen tillgängliga, användbara, skyddade

och integrerade samt sörja även för andra omständigheter som påverkar kvaliteten på uppgifterna. Det här innebär exempelvis skyldighet att vid den beredning som sker när datasystem tas i bruk samt vid beredningen av en förvaltnings- eller lagstiftningsreform utreda vilka följder de planerade åtgärderna kommer att ha för handlingsoffentligheten, handlingssekretessen och skyddet för handlingar samt handlingskvaliteten. Myndigheternas dokument- och informationshantering samt datasystemen och databehandlingen ska planeras och skötas så att både handlingsoffentligheten och arkiveringen och utplånandet av handlingar och datasystem sköts på behörigt sätt.

En god informationshantering innebär också många andra skyldigheter i anslutning till dokumenthantering. Förordningen om offentlighet och god informationshantering i myndigheternas verksamhet (1030/1999) innehåller närmare bestämmelser om detta. Enligt förordningen ska myndigheterna se över och bedöma sina dokument och datasystem och betydelsen av uppgifterna i dem. Denna skyldighet gäller inte bara pappershandlingar utan även uppgifter i elektronisk form.

Arkivlagen

På riksdagen, statsrevisorernas kansli, riksdagens justitieombudsmans kansli och statens revisionsverk tillämpas endast 6 och 7 § samt 8 § 1 och 2 mom. i arkivlagen (831/1994). I lagens 6 § definieras vad som avses med arkivmaterial. Med handling avses i lagen utöver sedvanliga pappershandlingar en på elektronisk väg eller på annat sätt åstadkommen framställning som kan läsas, avlyssnas eller annars uppfattas med tekniska hjälpmedel.

Lag om integritetsskydd i arbetslivet

I lagen om integritetsskydd i arbetslivet (759/2004, i kraft 1.10.2004) finns bestämmelser om hämtning och öppnande av e-postmeddelanden som hör till arbetstagaren. Bestämmelserna i lagens 6 kap. syftar till att säkerställa sekretessen för en arbetstagares konfidentiella meddelanden samtidigt som meddelanden som hör till arbetsgivaren och som behövs för den fortsatta verksamheten kan läsas också när arbetstagaren är frånvarande.

När riksdagen stiftade lagen framhöll den att problemen med e-postsystemens tillförlitlighet bör påpekas i samband med information och utbildning om lagen. De nya bestämmelserna om hämtning och öppnande av elektroniska meddelanden får inte leda till att allt fler för arbetsgivarens verksamhet viktiga funktioner, såsom begäran om och mottagande av offerter, sköts uteslutande per e-post. Meddelanden som är avsedda för arbetsgivaren ska i allmänhet sändas till arbetsplatsens officiella eller enheternas gemensamma e-postadresser. Därmed kan meddelanden som är viktiga för arbetsgivarens verksamhet alltid läsas av fler än en person. Behovet att hämta och läsa en enskild arbetstagares e-postmeddelanden när denne är frånvarande minskar då.

Avsikten med föreskrifterna är att skapa ett system där meddelanden som sänts till arbetstagaren eller meddelanden som arbetstagaren har sänt men som hör till arbetsgivaren ska kunna hämtas och öppnas med arbetstagarens samtycke. Annat öppnande av meddelanden som hör till arbetstagaren ska ses som en sista-handslösning och ske med iakttaganden av det förfarande som framgår av lagen.

I vissa situationer som nämns i lagen kan arbetsgivaren hämta eller öppna elektroniska meddelanden som arbetstagaren har tagit emot eller skickat endast då arbetsgivaren har vidtagit nödvändiga åtgärder för att skydda meddelandena. Till omsorgsplikten hör att arbetstagaren ges tillgång till en automatisk svarsfunktion som kan meddela avsändaren uppgifter om frånvaro och vikarie eller att arbetstagaren kan styra meddelandena till en annan av arbetsgivaren godkänd person eller adress. Alternativt kan arbetstagare samtycka till att någon annan av arbetstagaren och arbetsgivaren utsedd person kan ta emot meddelanden som skickats till arbetstagaren för att reda ut om det bland meddelandena finns sådana som är klart avsedda för arbetsgivaren och som behövs för att denne ska kunna ordna sina arbetsuppgifter.

Om arbetsgivaren uppfyller sin omsorgsplikt kan denne med iakttagande av det som föreskrivs i lagen hämta och öppna elektroniska meddelanden som hör till arbetsgivaren. Arbetsgivaren får utifrån uppgifter om meddelandets avsändare, mottagare eller rubrik ta reda på om arbetstagaren i sin frånvaro har mottagit eller omedelbart före frånvaron har skickat eller mottagit meddelanden som hör till arbetsgivaren. En förutsättning är att arbetstagaren sköter sina uppgifter självständigt för arbetsgivarens räkning och att sändande och mottagande av sådana meddelanden uppenbart hör till arbetstagarens uppgifter. Dessutom krävs det att arbetstagaren tillfälligt är förhindrad att utföra sina arbetsuppgifter och att arbetsgivaren inte på annat sätt kan få tillgång till meddelanden som hör till denne. Vidare krävs det att man inte fått kontakt med avsändaren för att utreda meddelandets innehåll eller för att få det sänt till en adress som arbetsgivaren anvisar.

Har arbetsgivaren avlidit eller är han eller hon permanent förhindrad att utföra sina arbetsuppgifter och hans eller hennes samtycke inte kan fås har arbetsgivaren rätt på motsvarande villkor att på basis av motsvarande uppgifter utreda vilka meddelanden som hör till arbetsgivaren, om det inte är möjligt att på annat sätt få reda på de ärenden som arbetstagaren skött och trygga arbetsgivarens verksamhet.

Arbetsgivaren får öppna ett hämtat meddelande om det är uppenbart att ett meddelande som arbetstagaren har sänt eller mottagit hör till arbetsgivaren. Det ska vara nödvändigt för arbetsgivaren att få reda på meddelandets innehåll för att kunna slutföra förhandlingar i anslutning till sin verksamhet, betjäna sina kunder eller trygga sina funktioner. Meddelandet ska öppnas med hjälp av den person

som har befogenheter som systemadministratör och i närvaro av en annan person.

Över öppnandet ska enligt lagen utarbetas en rapport som undertecknas av de personer som deltagit i öppnandet och av vilken framgår vilket meddelande som öppnats, varför meddelandet öppnats, tidpunkten och vem som utförde öppnandet samt till vem uppgift om meddelandets innehåll har givits. Rapporten ska utan dröjsmål tillställas arbetstagaren. Innehållet i meddelandet får inte behandlas i större utsträckning än vad som är nödvändigt och de personer som behandlar uppgifterna får inte röja meddelandets innehåll för utomstående medan arbetsavtalsförhållandet pågår eller efter att det har upphört.

Lag om dataskydd vid elektronisk kommunikation

Syftet med lagen om dataskydd vid elektronisk kommunikation (516/2004) är att trygga konfidentialitet och integritetsskydd vid elektronisk kommunikation. Avsikten är även att främja dataskydd vid elektronisk kommunikation och en balanserad utveckling av mångsidiga elektroniska kommunikationstjänster. Med begreppet meddelande avses i denna lag samtal, elektronisk post, textmeddelande, talmeddelande och annat motsvarande meddelande som i ett kommunikationsnät förmedlas mellan parterna till en mottagarkrets som inte är utvald på förhand. Med dataskydd avses administrativa och tekniska åtgärder genom vilka säkerställs att uppgifter är tillgängliga endast för dem som har rätt att använda dem, att uppgifterna inte kan ändras av andra än dem som har rätt till detta och att uppgifterna och informationssystemen kan utnyttjas av dem som har rätt att använda uppgifterna och systemen.

Enligt lagen är meddelanden, identifieringsuppgifter och lokaliseringsuppgifter konfidentiella. Men ett meddelande är inte konfidentiellt om det är föremål för allmän mottagning. Konfidentialitetsskyddet gäller också identifieringsuppgifter som influtit genom att man bläddrat i webbsidor.

Bestämmelserna om tystnadsplikt och förbud mot utnyttjande innebär att den som mottagit eller annars fått kännedom om konfidentiella meddelanden eller identifieringsuppgifter inte utan samtycke av en kommunikationspart får röja eller utnyttja ett meddelandes innehåll, identifieringsuppgifter eller uppgifter om meddelandets existens, om inte annat bestäms i lag. Det samma gäller lokaliseringsuppgifter. Bestämmelserna om tystnadsplikt och förbud mot utnyttjande tillämpas även på den som är eller varit anställd hos ett teleföretag, en tillhandahållare av mervärdestjänster, en sammanslutningsabonnent eller en teleentreprenör.

Skydd av meddelanden och identifieringsuppgifter är enligt lagen tillåtet med utnyttjande av till buds stående teknik. Men skyddet får inte störa utförandet eller användningen av nättjänster och kommunikationstjänster. För att skydda förfarandet förbjuder lagen import, tillverkning och distribution av system för av-

kodning av det tekniska skyddet vid elektronisk kommunikation. Det är inte heller tillåtet att inneha ett sådant system.

Behandling av meddelanden och identifieringsuppgifter är tillåtet i vissa i lagen särskilt nämnda situationer, exempelvis för att utföra och använda nättjänster, utveckla den tekniska behandlingen eller för att upptäcka tekniska fel och brister. Rätt att utreda innehållet i ett meddelande föreligger ändå inte.

Enligt lagen är teleföretag och den som tillhandahåller mervärdestjänster ansvariga för dataskyddet i tjänsterna. En sammanslutningsabonnent ansvarar för dataskyddet i fråga om användarnas identifieringsuppgifter och lokaliseringsuppgifter. I detta sammanhang ska avseende fästas vid hur allvarligt ett hot är, hotets tekniska nivå samt kostnaderna för att avvärja störningar.

Den allmänna styrningen och utvecklingen för att uppnå syftet med lagen hör till kommunikationsministeriet. Kommunikationsverket sköter vissa övervakningsuppgifter. I lagen om dataskydd vid elektronisk kommunikation ingår också bestämmelser om tvångsmedel, en hänvisningsbestämmelse till strafflagen samt en straffbestämmelse om dataskyddsförseelse vid elektronisk kommunikation.

Strafflagen

Strafflagens (39/1889) 38 kap. innehåller bestämmelser om informations- och kommunikationsbrott. Enligt 3 § döms den som obehörigen öppnar ett brev eller ett annat tillslutet meddelande som är adresserat till någon annan eller genom att bryta ett säkerhetsarrangemang skaffar uppgifter om ett meddelande som har upptagits elektroniskt eller med någon annan sådan teknisk metod och som är skyddat mot utomstående för kränkning av kommunikationshemlighet. För samma brott kan även den dömas som skaffar uppgifter om innehållet i ett samtal, telegram, text-, bild- eller dataöverföring eller något annat motsvarande telemeddelande eller om avsändande eller mottagande av ett sådant meddelande. I kapitlet ingår även bestämmelser om grov kränkning av kommunikationshemlighet.

I 8 § föreskrivs om dataintrång. Till straff döms den som genom att göra bruk av en användaridentifikation som han inte har rätt till eller genom att annars bryta säkerhetsarrangemang och obehörigen tränger in i ett datasystem där data behandlas, lagras eller överförs elektroniskt. För dataintrång döms också den som utan att tränga in i ett datasystem eller en del av detta med tekniska specialanordningar obehörigen tar reda på information som finns i datasystemet.

Kom ihåg

- ✓ Varje informationsanvändare är ansvarig för informationssäkerheten.
- ✓ Genom informationssäkerhet ser man också till att den offentliga informationen är korrekt, aktuell och tillgänglig.
- ✓ Låt inte andra använda ditt användarnamn och ditt lösenord.
- ✓ Skriv inte ned ditt lösenord.
- ✓ Välj inte ett lösenord som är lätt att gissa, t.ex. namnet på din make eller ditt barn.
- ✓ Spara viktig information i din hemkatalog på H-disken.
- ✓ Undvik onödiga papperskopior.
- ✓ Informationen på internet är inte nödvändigtvis korrekt – kontrollera informationens riktighet.
- ✓ Informationen på internet är skyddad av upphovsrätt – kontrollera att informationen får användas.
- ✓ Internetanvändarens identifieringsuppgifter sparas alltid i webbsidornas loggfiler.
- ✓ Det finns separata anvisningar om användningen av e-post; kom dessutom ihåg att det kan finnas andra specialanvisningar som måste beaktas när du hanterar information.

Att tänka på!

- ✓ Följ allmänt accepterade nätikettregler för e-post.
- ✓ Ett e-postmeddelande är ett skriftligt dokument som någon annan kan behandla och kopiera.
- ✓ Den externa e-posttrafiken har ingen ångerfunktion.
- ✓ Respektera mottagarens e-brevlåda. Sänd inga kedjebrev, julhälsningar eller skämt i den interna e-posten.
- ✓ På internet är e-posten som en lapp på en offentlig anslagstavla – alla kan läsa den.
- ✓ E-postadressen måste vara exakt annars går meddelandet till fel person eller försvinner.
- ✓ Internet gör det möjligt att skicka e-post i någon annans namn.
- ✓ E-posten är avsedd för korta meddelanden som sparas under en överskådlig tid. Program och omfattande material ska skickas på annat sätt än per e-post.
- ✓ Det finns inga garantier för att eller när ett e-postmeddelande går fram. Om du vill försäkra dig om att mottagaren har fått ditt meddelande – be om kvittering.