Viestintävirasto
Kommunikationsverket

15.6.2016

Motivering till och tillämpning av föreskrift 68

Domännamnsföreskrift

MPS 68

Innehåll

Avdelning A Centrala ändringar

I denna avdelning beskrivs de centrala ändringarna i föreskrift 68 jämfört med de tidigare gällande föreskrifterna om domännamn.

1 Ändringar

Denna är den första versionen av föreskrift 68. Föreskriften har sammanställts av följande tidigare gällande föreskrifter:

- Föreskrift 37 E/2006 M om tekniska konfigurationer för och tillåtna tecken i finländska domännamn
- Föreskrift 52 A/2006 M om tekniska konfigurationer för och tillåtna tecken i ax-domännamn

Föreskrifterna 37 E/2006 M och 52 A/2006 M upphävs genom en ny föreskrift 68 när ändringarna enligt informationssamhällsbalken (917/2014) [1] träder i kraft den 5 september 2016. De föreskrifter som ska upphävas handlar om konfiguration av namnservrar med domännamn, e-postförbindelser, kraven på SOA-post (Start of Authority) samt domännamnets längd och tillåtna tecken. Så gott som alla krav i de föreskrifter som ska upphävas ingår i den nya föreskriften. Det har gjorts några ändringar i kraven:

- Skyldigheten att uppge namnservrar för domännamn enligt 2 § i de föreskrifter som ska upphävas har strukits med anledning av lagändringen. Om namnservrar dock uppges, ska de konfigureras i enlighet med föreskrift 68.
- Den nya föreskriften innehåller inte längre några bestämmelser om e-postförbindelser.
- De krav på domännamnets form i föreskrift 68 som tidigare gällt fi-domännamn gäller som sådana även domännamn under toppdomänen ax. Detta innebär att möjligheten att använda samiska nationella tecken även gäller domännamn under toppdomänen ax, till skillnad från tidigare.
- I föreskriften ingår inte längre kravet på att serienumren och klockorna för SOA-posterna inte väsentligt får avvika från de internetstandarder och -rekommendationer som publicerats. Kravet har ändrats till en rekommendation i detta dokument.

Den nya föreskriften 68 innehåller en del tidigare gällande regler, men ändringarna i reglerna om domännamn genom informationssamhällsbalken påverkar också föreskriften. I och med informationssamhällsbalken har registrarerna av domännamn fått nya skyldigheter. Lagen innehåller bestämmelser om en ny verksamhetsmodell enligt vilken domännamn ska skaffas hos den egna registraren. Registraren administrerar dessutom domännamn på användarnas vägnar och därför föreskrivs vissa uttryckliga skyldigheter för registrarerna i lagen. Enligt de nya reglerna som föreskrivs genom informationssamhällsbalken ska registraren sörja för informationssäkerheten i sin

verksamhet och meddela den myndighet som förvaltar domännamnsregistret om betydande störningar i informationssäkerheten.

Bestämmelser om de nya skyldigheterna finns i 2, 4 och 5 kap. i föreskrift 68. Föreskrift 68 innehåller följande bestämmelser:

- 2 kap: olika skyldigheter för registrarer (anmälan om inledande eller nedläggning av verksamhet, ändringar i uppgifter, information om förbudsbeslut av den myndighet som förvaltar domännamnsregistret, rådgivningsskyldighet gentemot användare, anteckning av uppgifter om användare i domännamnsregistret, registrarens gränssnitt mot Kommunikationsverkets domännamnsregister, överföring av domännamn till en annan användare och byte av registrar)
- 3 kap: tekniska konfigurationer för domännamn (domännamnets form och konfigurationer för frivilliga namnservrar)
- 4 kap: hantering av registrarens informationssäkerhet
- 5 kap: anmälningsskyldighet vid störningar i informationssäkerheten.

2 Konsekvenser

Den viktigaste ändringen i föreskriften hänför sig till preciseringen av registrarernas skyldighet enligt 170 § 1 mom. 6 punkten i informationssamhällsbalken. Det är fråga om en registrars skyldighet att sörja för informationssäkerheten i sin verksamhet.

2.1 Konsekvenser för informationssamhället

Det uttryckliga syftet för denna föreskrift är att åstadkomma positiva konsekvenser för informationssamhället genom att främja informationssäkerheten i förmedlingen av domännamn och genom att säkerställa att fi-roten och ax-roten hålls uppdaterade på ett informationssäkert sätt. Denna föreskrift har också många positiva konsekvenser för användare som skaffar domännamn, emedan föreskriften preciserar innehållet i och kvaliteten på registrarernas tjänst.

Föreskriften innehåller närmare föreskrifter om de uppgifter som registraren ska lämna till myndigheten som förvaltar domännamnsregistret. Genom föreskriften preciseras också registrarernas rådgivningsskyldighet som avses i informationssamhällsbalken och gäller förutsättningar för innehållet och formen i det domännamn som ska registrerars. Genom föreskriften preciseras också de förfaranden som registrarerna måste iaktta, om användaren vill överföra domännamnet till en annan användare eller om användaren vill byta registrar. Föreskriften kan således anses förbättra användarnas ställning och klargöra registrarernas roll.

Föreskriften kan anses främja informationssäkerheten i registrarernas verksamhet, emedan informationssamhällsbalkens skyldighet att sörja för informationssäkerheten har preciserats så detaljerat som möjligt. Å andra sidan är föreskriften flexibel till den del att aktörerna i praktiken själva kan avgöra hur de uppfyller föreskriftens skyldigheter för att åstadkomma det eftersträvade resultatet. Föreskriften kan anses minska störningar i inform-

ationssäkerheten, när kraven på informationssäkerheten i registrarernas verksamhet beskrivs tillräckligt noggrant. Föreskriften kan alltså också till denna del bedömas ha positiva konsekvenser för informationssamhället.

2 2. Ekonomiska konsekvenser

Det är avgiftsfritt att utöva registrarverksamhet. I motsats till flera andra register över toppdomäner innehåller informationssamhällsbalken inte några bestämmelser om en skyldighet för registrarer att betala för denna roll. Informationssäkerhetsskyldigheter om vilka det bestäms i informationssamhällsbalken och som preciserats genom Kommunikationsverkets föreskrift kan medföra kostnader för registrarerna. Det kan beräknas att genomförandet av informationssäkerhetsskyldigheterna kan orsaka extra kostnader för många registrarer åtminstone när verksamheten inleds. Å andra sidan ska det beaktas att en del av registrarerna redan har tagit hänsyn till informationssäkerheten. De existerande färdigheterna att iaktta föreskriften medför då inte några extra kostnader utan de ekonomiska konsekvenserna är små.

Syftet med föreskriften är att precisera de lagstadgade informationssäkerhetsskyldigheterna, men aktörerna får dock själv avgöra hur de uppfyller föreskriftens skyldigheter på ett så kostnadseffektivt sätt som möjligt. Det finns flera olika sätt att sörja för informationssäkerheten. Arten av registrarens verksamhet är också av betydelse med tanke på informationssäkerhetskraven. Registraren kan använda antingen Kommunikationsverkets webbläsargränssnitt eller EPP-gränssnitt. Kostnaderna för informationssäkerheten för det senare alternativet är större, emedan registrarens system som ansluts till EPP-gränssnittet måste uppfylla kriterierna härledda från skyddsnivå (IV) i Katakri (verktyg för informationssäkerhetsauditering) i fråga om datatrafiken och informationssystemen.

Föreskriften är utarbetad i en arbetsgrupp och i samarbete med branschaktörer och övriga intressentgrupper. På remissen har man hänvisat till eventuella kostnadseffekter, men utlåtandena innehåller inte några egentliga kostnadsberäkningar.

Det är svårt att bedöma kostnadseffekterna för uppfyllandet av föreskriftens skyldigheter, eftersom registarerna är mycket olika sinsemellan. Vissa aktörer (t.ex. teleföretag) har redan lagstadgade informationssäkerhetsskyldigheter som gäller hela organisationen, och därför medför de nya skyldigheterna för förmedling av domännamn inte nödvändigtvis några väsentliga extra kostnader. Det är också att konstatera att de kostnader som föreskriften eventuellt medför är större i början än på sikt. Då vetskapen om informationssäkerheten och informationssystemen har nått den behövliga nivån, är kostnaderna för underhållet och utvecklingen av systemen och informationssäkerhetskulturen inte lika stora som i början.
Det år mycket svårt att beräkna de direkta kostnaderna i euro som föreskriften medför. Det är också att beakta att de skyldigheter som hänför sig till själva informationssäkerheten samt övriga skyldigheter har tagits in i lag och föreskriften endast preciserar lagens krav. Intressentgruppernas

expertis har utnyttjats under hela beredningen och på så sätt har man försökt minimera den administrativa belastningen som föreskriften orsakat. Med hänsyn till omständigheterna ovan kan det anses att registrarerna genom föreskriften inte åläggs nya skyldigheter som skulle medföra väsentliga extra kostnader för aktörerna. Skyldigheterna är ändamålsenliga och nödvändiga för att genomföra syftet med informationssamhällsbalken och föreskriften. Som helhet kan det anses att föreskriften kortvarigt kan medföra extra kostnader för registrarer, men på lång sikt medför föreskriften besparingar till exempel i form av färre informationssäkerhetsstörningar. Störningarna betyder utredningar och skador som också orsakar kostnader. Det förebyggande informationssäkerhetsarbetet kan anses medföra besparingar på lång sikt.

2.3. Övriga konsekvenser för registrarer

Föreskriftens krav gäller också myndigheter, om de har gjort en anmälan om registrarverksamhet. Skyldigheterna kan bedömas medföra likadana ändringar i myndigheternas tekniska system, funktionella processer och personalresurser som hos övriga registrarer. Det kan dock bedömas att föreskriftens konsekvenser inte hindrar myndigheternas möjligheter att agera inom ramen för sina resurser.

Föreskriften har vissa konsekvenser för Kommunikationsverkets verksamhet, då verkets skyldighet är att utöva tillsyn över efterlevnaden av informationssamhällsbalken och domännamnsföreskriften. Föreskriften har dock inga personalkonsekvenser för Kommunikationsverkets tillsynsuppgifter. Föreskriften har inte några nämnvärda konsekvenser för miljön eller avsevärda övriga samhälleliga konsekvenser.

Avdelning B Motivering till enskilda paragrafer och anvisningar för tillämpning

1 kap. Allmänna bestämmelser

Detta kapitel behandlar föreskriftens kapitel 1, dvs. de allmänna bestämmelserna i föreskriften.

1 § Föreskriftens syfte

Föreskriftens 1 § beskriver syftet med och principerna för föreskriften. Kraven i föreskriften syftar till att uppnå dessa mål, och tillämpningen av föreskriften styrs av målen. De mål som beskrivs i paragrafen bör utgöra utgångspunkter i alla aktiviteter som sker vid förmedling av domännamn.

Enligt 1 § är syftet med föreskriften att

1) trygga en aktuell och informationssäker förvaltning av domännamnsregistret samt fi- och ax-roten,

2) trygga domännamnsanvändarnas tillgång till information om de krav som gäller domännamnets form och innehåll,
3) främja smidig överföring av domännamn eller smidigt byte av registrar,
4) främja domännamnets funktion,
5) trygga informationssäkerheten vid förmedling av domännamn,
6) trygga att den myndighet som förvaltar domännamnsregistret har tillgång till information om informationssäkerhetsstörningar vid förmedling av domännamn.

I föreskriften är avsikten att fastställa minimikraven på genomförande av informationssäkerheten. Strävan är att registrarerna ska beakta informationssäkerheten som en del av den dagliga verksamheten. Med andra ord syftar föreskriften till att säkerställa att informationssäkerhetsfrågor beaktas rutinmässigt och i effektiva processer som en del av förmedlingen av domännamn.

Med *informationssäkerhet* avses enligt 3 § 1 mom. 28 punkten i informationssamhällsbalken administrativa och tekniska åtgärder genom vilka det säkerställs att information är tillgänglig endast för dem som har rätt att använda den, att informationen inte kan ändras av andra än dem som har rätt till detta samt att informationen och informationssystemen kan utnyttjas av dem som har rätt att använda informationen och systemen. Informationssäkerhet innebär m.a.o. åtgärder för att säkerställa informationens konfidentialitet, integritet och tillgänglighet. Syftet med denna föreskrift är att främja att dessa mål ska uppnås.

2 § Tillämpningsområde

Denna paragraf handlar om föreskriftens tillämpningsområde. Föreskrift 68 tillämpas på domännamn under toppdomänen fi och ax samt på förmedling och administrering av dem.

Kraven i föreskriften är indelade i följande fem sakhelheter:
- Kapitel 2 handlar om vissa krav för registrarverksamheten.
- Kapitel 3 handlar om tekniska krav för domännamn.
- Kapitel 4 handlar om särskilda krav för hantering av registrarens informationssäkerhet.
- Kapitel 5 handlar om anmälningsskyldighet vid störningar i informationssäkerheten.

2.1 Domännamn under toppdomänen fi och toppdomänen ax

Enligt 3 § 1 mom. 35 punkten i informationssamhällsbalken avses med *domännamn* en adress på internet under den nationella toppdomänen fi eller toppdomänen ax för landskapet Åland i form av ett namn som består av bokstäver, siffror eller andra tecken eller en kombination av dem.

2.2 Förmedling och administrering av domännamn

Med förmedling av domännamn avses registreringar i domännamnsregistret. Enligt 164 § 2 mom. i informationssamhällsbalken får endast verksam-

hetsutövare som enligt 165 § har lämnat in en anmälan om registrarverksamhet, dvs. *en registrar*, får göra registreringar i domännamnsregistret. Enligt 167 § 1 mom. i informationssamhällsbalken ska ett domännamn registreras på domännamnsanvändaren. Registraren ska i domännamnsregistret anteckna korrekta och uppdaterade uppgifter som identifierar domännamnsanvändaren samt den e-postadress som ska användas för hörande och delgivning.

Domännamnsförvaltning omfattar alla åtgärder som en registrar vidtar för att upprätthålla uppgifterna om domännamn i domännamnsregistret. Enligt exempelvis 170 § 1 mom. 2 punkten i informationssamhällsbalken ska en registrar uppdatera uppgifterna i domännamnsregistret och enligt 5 punkten på begäran av domännamnsanvändaren avregistrera ett domännamn innan dess giltighetstid har löpt ut (uppsägning). Med domännamnsförvaltning avses även förmågan att göra anteckningar i domännamnsregistret med hjälp av tekniska arrangemang som Kommunikationsverket har fastställt samt att sörja för informationssäkerheten i verksamheten.

2.3 Domännamnsanvändare

Med *domännamnsanvändare* avses enligt 164 § 3 mom. i informationssamhällsbalken en juridisk person, en enskild näringsidkare eller en annan sammanslutning eller en fysisk person som *ett domännamn kan registreras på.*

2.4 Domännamnsregister

Med *domännamnsregister* avses enligt 164 § 1 mom. i informationssamhällsbalken Kommunikationsverkets register över domännamn under toppdomänen fi och med fi-rot en databas med teknisk information om domännamn för styrning av internettrafiken. Ax-domännamnsregistret och ax-roten drivs enligt nuvarande praxis av Ålands landskapsregering på basis av en överenskommelseförordning som föreskrivs med stöd av 32 § i självstyrelselagen för Åland (1144/1991).

2.5 Föreskriftens tillämpningsområde i fråga om domännamn under toppdomänen ax

Enligt 2 § i föreskriften tillämpas föreskriften också på domännamn under toppdomänen ax samt på förmedling och administrering av dem. Kommunikationsverket vill dock påminna om att bestämmelserna om domännamn under toppdomänen fi och ax i föreskriftens 9 § avviker från varandra i fråga om registrarernas tekniska gränssnitt mot domännamnsregistren. En registrar som förmedlar och administrerar domännamn under toppdomänen fi kan anteckna domännamn i Kommunikationsverkets domännamnsregister via verkets EPP-gränssnitt. Om registraren använder Kommunikationsverkets EPP-gränssnitt som ett tekniskt gränssnitt, måste den uppfylla Katakri-kraven som gäller informationssäkerhet enligt föreskriftens 20 §. Vid registrering och administrering av domännamn under toppdomänen ax är

det enda tillgängliga tekniska gränssnittet, åtminstone för tillfället, webbläsargränssnittet på www.whois.ax.

Föreskriften kan vid behov senare kompletteras med tekniska gränssnittsspecifikationer som gäller förmedling och administrering av domännamn under toppdomänen ax.

Enligt 163 § 1 mom. i informationssamhällsbalken tillämpas 21 kap. om domännamn också på domännamn under toppdomänen för landskapet Åland (toppdomänen ax) samt på domännamnsverksamhet och registreringstjänster för domännamn i samband därmed. Enligt 163 § 2 mom. ska bestämmelserna om det domännamnsregister som förvaltas av Kommunikationsverket också tillämpas på registret över domännamn under toppdomänen ax. Enligt motiveringen till paragrafen ska överföring av befogenhet mellan riket och landskapet Åland när det gäller administrering av toppdomänen ax i enlighet med nuvarande praxis regleras genom en särskild avtalsförordning.

I motiveringen till informationssamhällsbalken konstateras det även att en anmälan om inledande av registrarverksamhet enligt 165 § 1 mom. i lagen för toppdomänen ax ska göras till Ålands landskapsregering.

Grundlagsutskottet har i sitt utlåtande (18/2014 rd - RP 221/2013 rd) konstaterat att i ett ärende där riket har lagstiftningsbehörighet har rikets myndighet i regel också behörighet i landskapet Åland. Genom en överenskommelseförordning enligt 32 § i självstyrelselagen för Åland kan dock uppgifter som hör till riksförvaltningen överföras på landskapets förvaltningsmyndigheter. Skötseln av de registeruppgifter på Åland som avses i 163 § 2 mom. i informationssamhällsbalken överförs således från Kommunikationsverket till Ålands landskapsregering först genom en sådan överenskommelseförordning som avses i proportionsmotiven. Den myndighet som förvaltar domännamnsregistret och nämns i 165 § 1 mom. i informationssamhällsbalken betyder alltså Ålands landskapsregering i fråga om ax-domäner.

2.6 Allmänna begränsningar av föreskriftens tillämpningsområde

Informationssamhällsbalken tillämpas inte på andra toppdomäner och inte heller på domännamnsverksamhet i samband därmed, och därför lämnas de utanför denna föreskrifts tillämpningsområde. Andra toppdomäner är exempelvis de generiska domännamnen .com och .net samt de nationella toppdomänerna som .se för Sverige.

3 § Definitioner

I föreskriftens 3 § beskrivs de definitioner som används i föreskriften. I föreskriften definieras inte igen de begrepp som definieras i informationssamhällsbalken, och å andra sidan har definitionerna utformats så att de inte står i strid mot definitionerna i lagen. Definitionerna enligt informat-

ionssamhällsbalken beskrivs i den punkt ovan som gäller 2 § i detta dokument.

3.1 Domännamnets överföringskod

Med domännamnets överföringskod avses en av den myndighet som förvaltar domännamnsregistret (Kommunikationsverket eller Ålands landskapsregering) angiven kod med vilken ett domännamn kan överföras från en användare till en annan.

3.2 Kod för registrarbyte

Med kod för registrarbyte avses i föreskriften en kod med vilken förvaltningen av ett domännamn kan överföras från en registrar till en annan. I regel skapas koden av den gamla registraren. I undantagsfall kan den myndighet som förvaltar domännamnsregistret skapa en kod om den gamla registraren av någon anledning försummar sina skyldigheter enligt informationssamhällsbalken.

3.3 Gammal registrar

Med gammal registrar avses i föreskriften en registrar som avstår från förvaltningen av ett domännamn vid registrarbyte.

3.4 Ny registrar

Med ny registrar avses i föreskriften en registrar som tar emot förvaltningen av ett domännamn vid registrarbyte.

2 kap. Krav som gäller registrarer

I 2 kap. i föreskriften fastställs registrarernas anmälnings- och rådgivningsskyldigheter, de identifieringsuppgifter som ska antecknas i domännamnsregistret, kraven på gränssnitt för domännamnsregistret samt proceduren för överföring av domännamn och byte av registrar.

4 § Uppgifter som lämnas i anmälan om bedrivande av registrarverksamhet

Föreskriftens 4 § innehåller mer detaljerade bestämmelser om vilka identifieringsuppgifter en registrar ska lämna till den myndighet som förvaltar domännamnsregistret innan den inleder sin verksamhet. Enligt motiveringen till informationssamhällsbalken avses med den myndighet som förvaltar domännamnsregistret i praktiken Kommunikationsverket för toppdomänen fi och Ålands landskapsregering för toppdomänen ax.

Enligt 165 § 1 mom. i informationssamhällsbalken ska en registrar göra en anmälan till den myndighet som förvaltar domännamnsregistret innan den inleder sin verksamhet. Anmälan ska innehålla registrarens identifieringsuppgifter, den e-postadress som ska användas för hörande och delgivning samt andra uppgifter som behövs för tillsynen.

Enligt 4 § i föreskriften ska en registrars anmälan om bedrivande av verksamhet till den myndighet som förvaltar domännamnsregistret, utöver en e-postadress enligt 165 § i informationssamhällsbalken (en s.k. processadress), också innehålla följande uppgifter:
1) registrarens namn,
2) registrarens FO-nummer, personbeteckning eller, i avsaknad av dessa, annan uppgift som identifierar registraren,
3) registrarens postadress,
4) registrarens telefonnummer,
5) namnet på registrarens kontaktperson,
6) telefonnummer till registrarens kontaktperson,
7) e-postadress till registrarens kontaktperson.

I 4 § i föreskriften fastställs för det första vilka identifierings- och kontaktuppgifter som krävs för anmälan om bedrivande av registrarverksamhet, bland annat registrarens namn, företagets eller sammanslutningens FO-nummer eller den fysiska personens personbeteckning. Om företaget saknar ett finskt FO-nummer, kan exempelvis något annat registreringsnummer användas som identifieringsuppgift. Utländska fysiska personer har inte nödvändigtvis någon finsk personbeteckning och i så fall anges personens födelsetid som annan uppgift som identifierar användaren. Uppgifter som ska anmälas är också de adressuppgifter, uppgifter om kontaktpersoner och deras kontaktuppgifter som behövs för att nå personerna. I motiveringen till 165 § i informationssamhällsbalken anges största delen av de uppgifter som ska anmälas.

Kommunikationsverket konstaterar att personuppgiftslagen (523/1999) är en allmän lag för behandling av personuppgifter. Lagens bestämmelser tillämpas på all behandling av personuppgifter, om det inte finns motsvarande specialbestämmelser i andra lagar. Europeiska unionens personuppgiftsdirektiv har också satts i kraft genom personuppgifslagen. Specialbestämmelser om behandlingen av personuppgifter finns också i flera andra lagar om olika ämnen. De kan t.ex. gälla rätt att samla in och registrera personuppgifter, att lämna ut och lagra personuppgifter eller innehållet i ett personregister. Även Europeiska unionens författningar kan innehålla bestämmelser som är direkt tillämpliga på behandlingen av personuppgifter eller som inverkar på behandlingen. Lagen om offentlighet i myndigheternas verksamhet (offentlighetslagen 621/1999) tillämpas på utlämnande av personuppgifter ur myndigheternas personregister, om inte något annat föreskrivs för en viss funktion. Bestämmelserna om sekretess och god informationshantering påverkar också behandlingen av personuppgifter. Dataskyddsombudsmannen styr och övervakar verkställigheten av personuppgiftslagstiftningen. Mer information om reglering av personuppgifter och den reform av dataskyddsreglering som sker år 2018 finns på Dataombudsmannens webbplats på www.tietosuoja.fi.

Kommunikationsverket konstaterar att alla registrarer av domännamn under toppdomänen fi och ax är skyldiga att följa personuppgiftslagstiftningen i tillämpliga delar vid behandlingen av personuppgifter. Kommunikations-

verket konstaterar också att det är en förvaltningsmyndighet förpliktad av annan lagstiftning som gäller myndighetsverksamhet, t.ex. förvaltningslagen (434/2003). På utlämnande av personuppgifter ur Kommunikationsverkets domännamnsregister tillämpas lagen om offentlighet i myndigheternas verksamhet. Om offentliggörande av uppgifter ur domännamnsregistret på Kommunikationsverkets webbsidor bestäms i 167 § 2 mom. i informationssamhällsbalken.

4.1 Lagstadgad processadress och övriga e-postadresser

I 312 § 2 mom. i informationssamhällsbalken föreskrivs om Kommunikationsverkets absoluta rätt att för hörande och delgivning använda den e-postadress som är införd i domännamnsregistret. Därför kan en handling eller ett beslut som gäller domännamn alltid delges genom e-post. Denna så kallad processadress har stor rättslig betydelse och enligt 165 § i lagen är det obligatoriskt för registrarerna att ange den till den myndighet som förvaltar domännamnsregistret. Därför hänvisar 4 § i föreskriften till lagens bindande bestämmelse. Med hjälp av en processadress kan Kommunikationsverket snabbt delge bindande beslut, eftersom beslutet eller handlingen enligt 312 § 2 mom. i lagen då anses ha delgivits den tredje dagen efter det att meddelandet sändes, om inte något annat visas. En rätt processadress för en registrar är en viktig uppgift och med tanke på registrarens rättsskydd är det ytterst viktigt att den är uppdaterad.

Lagen eller föreskriften utgör inget hinder för att anmäla andra e-postadresser än de som används för officiella höranden eller delgivningar. Även andra e-postadresser kan anges för Kommunikationsverkets elektroniska system, om en registrar anser att det är nödvändigt att exempelvis hålla de e-postadresser som används vid behandling av dagliga ärenden av teknisk karaktär i anslutning till domännamnet åtskilda från de obligatoriska processadresserna. Enligt lagen är det emellertid obligatoriskt att ange endast en e-postadress.

4.2 Anmälan om ändringar i uppgifterna

Enligt 165 § 2 mom. i informationssamhällsbalken ska Kommunikationsverket utan dröjsmål informeras om ändringar i de uppgifter som registraren har anmält. Enligt motiveringen till bestämmelsen ska registrarerna uppdatera ändringar i uppgifterna utan dröjsmål. Kommunikationsverket rekommenderar att registrarerna uppdaterar ändringar i uppgifterna i Kommunikationsverkets databas inom tre (3) dagar.

5 § Anmälans form och inlämnande av den till den myndighet som förvaltar domännamnsregistret

I 5 § i föreskriften ingår en bestämmelse om på vilket sätt anmälan om bedrivande av registrerarverksamhet enligt 165 § 1 mom. i informationssamhällsbalken ska göras. Paragrafen gäller också anmälningar om ändringar i de uppgifter som registrarerna har lämnat. Enligt paragrafen ska ändringarna för fi-domäner göras via Kommunikationsverkets elektroniska webb-

tjänst på www.kommunikationsverket.fi. För ax-domäner föreskrivs att ändringarna ska göras på adressen www.whois.ax.

Den som ska göra en anmälan om bedrivande av registrarverksamhet får i Kommunikationsverkets elektroniska system basinformation om alla rättigheter och skyldigheter för registrarerna som avses i informationssamhällsbalken och Kommunikationsverkets föreskrift. Senast i anslutning till anmälan kan den som gör anmälan ta del av de rättigheter och skyldigheter som bygger på författningar och som gäller den anmälda verksamheten. Information finns också på förhand tillgänglig på Kommunikationsverkets webbplats för att verket ska kunna säkerställa att de som bedriver eller har för avsikt att bedriva registrarverksamhet är medvetna om rättigheterna och skyldigheterna i anslutning till verksamheten.

En förteckning förs över de verksamhetsutövare som har anmält sig som registrarer, och basinformation om dem läggs ut på Kommunikationsverkets webbplats. I basinformationen ingår verksamhetsutövarnas identifieringsuppgifter och verksamhetsuppgifter av allmän karaktär. Syftet är att underlätta möjligheterna att få uppdaterad information om verksamhetsutövare, vilket är särskilt nödvändigt för användarna.

De övriga uppgifter som fastställs i 4 § i föreskriften lämnas ut av Kommunikationsverket enligt de krav som föreskrivs i lagen om offentlighet i myndigheternas verksamhet (621/1999).

6 § Anmälningar till kunder om ändringar i registrarens verksamhet

Föreskriftens 6 § innehåller mer detaljerade bestämmelser om de anmälningar som en registrar ska ge till sina kunder, om den lägger ned sin verksamhet eller har av den myndighet som förvaltar domänamnsregistret fått ett beslut där registraren förbjuds att bedriva registrarverksamhet under högst ett år.

I 6 § 1 mom. i föreskriften ingår en bestämmelse om att om verksamheten läggs ned ska registraren informera varje kund om detta. Syftet med bestämmelsen är att säkerställa att kunden de facto får informationen. Information som enbart läggs ut på exempelvis registrarens webbplats kan inte anses vara tillräcklig, även om den bör läggas ut även där. Med hjälp av kundernas e-postadresser kan registraren effektivt rikta informationen, men det kan också vara nödvändigt att försöka nå kunderna per telefon.

Enligt 165 § 2 mom. i informationssamhällsbalken ska Kommunikationsverket och kunderna, om verksamheten läggs ned, informeras om detta minst två veckor i förväg. Enligt motiveringen till momentet gäller detsamma om verksamheten avbryts. Såsom för anmälan om inledning av verksamheten har det i lagmotiveringen konstaterats att också anmälningar om nedläggning av verksamheten görs till Ålands landskapsregering för toppdomänen ax. Syftet med bestämmelsen är att säkerställa domännamnsanvändarens tillgång till ett fungerande domännamn och att säkerställa att användaren

hinner byta domännamnsadministratör innan registrarens verksamhet upphör. Kommunikationsverket rekommenderar att registrarerna, av de skäl som framgår av motiveringen till lagen, informerar Kommunikationsverket och kunderna även när verksamheten avbryts tillfälligt.

I 6 § 2 mom. i föreskriften åläggs registrarerna att informera varje kund även när registrarens verksamhet avbryts tillfälligt med anledning av förbudsbeslut av den myndighet som förvaltar domännamnsregistret. Om registraren bryter mot lag eller bestämmelser, föreskrifter och beslut som utfärdats med stöd av lag, kan Kommunikationsverket enligt 171 § 2 mom. i informationssamhällsbalken förbjuda registraren att registrera domännamn eller göra anteckningar som gäller domännamn i domännamnsregistret. Enligt bestämmelsen ger Kommunikationsverket dessförinnan en anmärkning och ett eventuellt beslut där Kommunikationsverket ålägger registraren att inom en rimlig tid rätta till felet eller försummelsen.

Enligt motiveringen till momentet kan ett förbudsbeslut överklagas och Kommunikationsverket verkställer i praktiken förbudet genom att hindra att registraren via tekniska gränssnitt kommer åt att göra registreringar eller ändringar i domännamnsregistret. Kunderna måste i en sådan situation hitta en ny registrar och kravet att registraren ska informera om saken är sålunda ett viktigt minimikrav från domännamnsanvändarens synpunkt. Syftet med detta moment i föreskriften är att säkerställa att kunden de facto får informationen. Dessutom ska Kommunikationsverket lägga ut information om förbudsbeslut på sin webbplats.

7 § Registrarens rådgivningsskyldighet gentemot användare

Föreskriftens 7 § innehåller närmare föreskrifter om på vilket sätt registrarerna ska sörja för den informations- och rådgivningsskyldighet som avses i 170 § 1 mom. 1 punkten i informationssamhällsbalken. Enligt bestämmelsen ska en registrar innan ett domännamn registreras tillhandahålla behövlig information enligt denna lag om kraven på domännamnets innehåll och form. Föreskriftens 7 § innehåller närmare föreskrifter om vilka lagstadgade uppgifter som ska lämnas till användarna.

Enligt föreskriftens 7 § ska en registrar, utöver vad som bestäms i 3 § 21 punkten och 166 § i informationssamhällsbalken, innan den registrerar ett domännamn, ge användare följande närmare uppgifter om de förutsättningar som gäller domännamnets innehåll och form:
1) krav på domännamnets form enligt föreskriftens 12 §
2) uppgifter om namn som är införda i Finlands handels-, förenings-, stiftelse- eller partiregister
3) uppgifter om varumärken som är införda i Finlands eller Europeiska unionens varumärkesregister.

I motiveringen till 170 § 1 mom. 1 punkten i informationssamhällsbalken beskrivs registrarernas informations- och rådgivningsskyldighet. En registrar ska ge sina kunder och aktörer som vill registrera domännamn den information om förutsättningarna för registrering av domännamn som avses i

166 § i en lättillgänglig och utförlig form innan domännamnet registreras. Informationen bör vara tillgänglig på ett sådant sätt att domännamnssökanden kan förvissa sig om de krav som gäller domännamnens utformning och innehåll innan domännamnet registreras. I synnerhet när det gäller skyddade namn och märken bör kunderna känna till förutsättningarna innan domännamnen registreras. Syftet med bestämmelsen är att felaktiga och lagstridiga domännamnsregistreringar ska kunna undvikas. Registraren måste för egen del aktivt se till att domännamnsregistreringar är förenliga med lagen. I motiveringen till bestämmelsen konstateras det särskilt att det slutliga ansvaret för att ett domännamn är lagligt fortfarande kommer att finnas hos domännamnsanvändaren.

Enligt 166 § 1 mom. i informationssamhällsbalken får ett domännamn bestå av minst två och högst 63 tecken. Enligt 2 mom. 1 punkten i bestämmelsen får ett domännamn vid registreringstidpunkten inte motsvara någon annans skyddade namn eller märke, om inte domännamnsanvändaren kan ge en godtagbar grund för registreringen av domännamnet. Dessutom får det enligt 2 punkten i momentet inte likna någon annans skyddade namn eller märke, om domännamnet registreras i uppenbart vinnings- eller skadesyfte.

Enligt definitionen i 3 § 1 mom. 21 punkten i informationssamhällsbalken avses med *skyddat namn och skyddat märke* ett namn eller märke som är infört i handels-, varumärkes-, förenings-, stiftelse- eller partiregistret eller en inarbetad firma, ett sekundärt kännetecken eller ett varumärke enligt firmalagen (128/1979) eller varumärkeslagen (7/1964) samt namnet på ett offentligt samfund, ett statligt affärsverk, en självständig offentligrättslig inrättning, en offentligrättslig förening samt på en främmande stats beskickning eller på ett organ i dem.

Uppgifter om de namn som är införda i Finlands handels-, förenings-, stiftelse- eller partiregister finns i Patent- och registerstyrelsens (PRS:s) register och är tillgängliga för allmänheten i PRS webbtjänster. De varumärken som har skyddats genom registrering i Finland finns antingen i PRS varumärkesdatabas eller i ett register som förs av Europeiska Unionens immaterialrättsmyndighet (EUIPO).

Enligt definitionen ovan avses med skyddat namn eller skyddat märke även en inarbetad firma, ett sekundärt kännetecken eller ett varumärke enligt firmalagen eller varumärkeslagen. Sådana icke-registrerade namn och märken finns därför inte i registren ovan. Kommunikationsverket har i sin beslutspraxis förhållit sig återhållsamt till sådana krav på återkallande som bygger på ett påstående om att en firma eller ett varumärke hade inarbetats innan det omstridda domännamnet registrerades. Kommunikationsverkets tvistelösning är en administrativ process där det inte är möjligt att göra en bedömning av en omfattande kännetecknsrättslig bevisning. Kännetecknsrättsliga tvister ska lösas i domstol, medan Kommunikationsverket ingriper i tydliga rättskränkningar.

Föreskriftens 7 § hänvisar till krav på domännamnets form enligt 12 § i föreskriften. Kraven innefattar specificeringar av tillåtna tecken i domännamn, som är bokstäverna a–z och siffrorna 0–9. Tillåtna tecken är också de nationella tecken som räknas upp i föreskriften samt bindestreck-minus. Föreskriftens 12 § 2 mom. innehåller dessutom föreskrifter om andra tekniska detaljer i domännamnens form.

Kommunikationsverket bestämmer inte på vilket sätt registrarerna ska fullgöra sin informatiosskyldighet enligt lag när det gäller de obligatoriska uppgifterna ovan. Skyldigheten kan fullgöras exempelvis på så sätt att registraren på sin webbplats länkar ett uppdaterat informationsinnehåll som fastställts av Kommunikationsverket. Kommunikationsverket har på sin webbplats uppdaterad information om uppgifter som enligt lag är obligatoriska för användarna, och andra nödvändiga anvisningar, till exempel information om Kommunikationsverkets tvistelösning.

I motiveringen till informationssamhällsbalken betonas registrarernas ansvar och skyldigheter vid övergång till den nya verksamhetsmodellen, där registrarerna har en viktig ställning. I motiveringen betonas att domännamnsanvändarnas rättigheter ska värnas om och att domännamnen ska bli korrekt registrerade i domännamnsregistret. Därför anser Kommunikationsverket att lagen medför en skyldighet för registrarer att omsorgsfullt vägleda sina kunder.

8 § Anteckning av uppgifter om användare i domännamnsregistret

Föreskriftens 8 § innehåller närmare föreskrifter om vilka identifieringsuppgifter en registrar ska anteckna om användare vid registrering av domännamn. I fråga om fysiska personer avses i 1 mom. i paragrafen med identifierings- och kontaktuppgifter användarens för- och efternamn och de uppgifter om adress och telefonnummer som behövs för att nå personen. Till de identifieringsuppgifter om en fysisk person som ska antecknas i registret hör även personbeteckning eller, i avsaknad av den, annan uppgift som identifierar användaren. Utländska fysiska personer har inte nödvändigtvis någon finsk personbeteckning och i så fall anges personens födelsetid som annan uppgift som identifierar användaren.

Föreskriftens 8 § 2 mom. fastställer att identifierings- och kontaktuppgifterna för juridiska personer och övriga organisationer som ska registreras som användare i domännamnsregistret är användarens firma och de adress- och telefonnummeruppgifter som behövs för att nå personen. Som identifieringsuppgift för juridiska personer registreras ett finskt FO-nummer eller, i avsaknad av den, annan uppgift som identifierar användaren, till exempel något annat registreringsnummer. I fråga om juridiska personer ska även namn, telefonnummer och e-postadress för användarens kontaktperson enligt föreskriften antecknas i registret.

Enligt 167 § 1 mom. i informationssamhällsbalken ska en registrar registrera ett domännamn på domännamnsanvändaren. I motiveringen till

momentet konstateras det att en kunds domännamn t.ex. inte får registreras på en registrar och att det med avseende på den faktiska domännamnsanvändarens rättigheter är viktigt att användarregistreringen har gjorts på ett korrekt sätt, särskilt när Kommunikationsverket utreder oklarheter eller tvister som hänför sig till denna lag.

Föreskriftens 8 § hänvisar till en bestämmelse i informationssamhällsbalken, som ålägger registrarerna att alltid i domännamnsregistret anteckna den e-postadress som enligt 167 § i lagen ska användas för hörande och delgivning. I 312 § 2 mom. i informationssamhällsbalken föreskrivs om Kommunikationsverkets absoluta rätt att för hörande och delgivning använda den e-postadress som är införd i domännamnsregistret. Därför kan en handling eller ett beslut som gäller domännamn alltid delges genom e-post. Denna så kallade processadressen har stor rättslig betydelse och enligt 167 § i lagen är det obligatoriskt för registrarena att ange den. Med hjälp av en processadress kan Kommunikationsverket snabbt delge bindande beslut, eftersom beslutet eller handlingen enligt 312 § 2 mom. i lagen då anses ha delgivits den tredje dagen efter det att meddelandet sändes, om inte något annat visas. En rätt processadress för en domännamnsanvändare är en viktig uppgift och med tanke på användarens rättsskydd är det högst viktigt att den hålls uppdaterad.

Enligt informationssamhällsbalken är det obligatoriskt att registrera enbart en e-postadress, men lagen och bestämmelsen utgör inget hinder för att anmäla andra e-postadresser än de som används för officiella höranden eller delgivningar. Även andra e-postadresser kan anges för Kommunikationsverkets elektroniska system, om en registrar anser att det är nödvändigt att exempelvis hålla de e-postadresser som används vid behandling av dagliga ärenden av teknisk karaktär i anslutning till domännamnet åtskilda från de obligatoriska processadresserna. Enligt 167 § i informationssamhällsbalken ska en registrar anteckna uppdaterade uppgifter om domännamnsanvändare. Enligt motiveringen till paragrafen ansvarar registraren för att de uppgifter som anmäls är korrekta och för att uppgifterna hålls uppdaterade. Om registrarens försummelser leder till att domännamnsanvändaren orsakas skador kan användaren yrka på skadestånd via domstol. Kommunikationsverket rekommenderar att registrarerna ofördröjligen informerar Kommunikationsverket om användarens uppgifter förändras.

Kommunikationsverket konstaterar att personuppgiftslagen (523/1999) är en allmän lag för behandling av personuppgifter. Lagens bestämmelser tillämpas på all behandling av personuppgifter, om det inte finns motsvarande specialbestämmelser i andra lagar. Europeiska unionens personuppgiftsdirektiv har också satts i kraft genom personuppgifslagen. Specialbestämmelser om behandlingen av personuppgifter finns också i flera andra lagar om olika ämnen. De kan t.ex. gälla rätt att samla in och registrera personuppgifter, att lämna ut och lagra personuppgifter eller innehållet i ett personregister. Även Europeiska unionens författningar kan innehålla bestämmelser som är direkt tillämpliga på behandlingen av personuppgifter eller som inverkar på behandlingen. Lagen om offentlighet i myndigheternas verksamhet (offentlighetslagen 621/1999) tillämpas på utlämnande av

personuppgifter ur myndigheternas personregister, om inte något annat föreskrivs för en viss funktion. Bestämmelserna om sekretess och god informationshantering påverkar också behandlingen av personuppgifter. Dataskyddsombudsmannen styr och övervakar verkställigheten av personuppgiftslagstiftningen. Mer information om reglering av personuppgifter och den reform av dataskyddsreglering som sker år 2018 finns på Dataombudsmannens webbplats på www.tietosuoja.fi.

Kommunikationsverket konstaterar att alla registrarer av domännamn under toppdomänen fi och ax är skyldiga att följa personuppgiftslagstiftningen i tillämpliga delar vid behandlingen av personuppgifter. Kommunikationsverket konstaterar också att det är en förvaltningsmyndighet förpliktad av annan lagstiftning som gäller myndighetsverksamhet, t.ex. förvaltningslagen (434/2003). På utlämnande av personuppgifter ur Kommunikationsverkets domännamnsregister tillämpas lagen om offentlighet i myndigheternas verksamhet. Om offentliggörande av uppgifter ur domännamnsregistret på Kommunikationsverkets webbsidor bestäms i 167 § 2 mom. i informationssamhällsbalken. Enligt bestämmelsen får i fråga om fysiska personer på webbsidorna offentliggöras domännamnet och användarens namn.

9 § Registrarens gränssnitt mot den myndighet som förvaltar domännamnsregistret

Föreskriftens 9 § föreskriver om krav som gäller hur anteckningar i domännamnsregister ska genomföras i tekniskt hänseende. Som tekniskt gränssnitt mot Kommunikationsverkets domännamnsregister ska en registrar enligt paragrafens 1 mom. använda antingen samma webbläsargränssnitt som Kommunikationsverkets webbplats på www.kommunikationsverket.fi har eller det EPP-gränssnitt (Extensible Provisioning Protocol) som Kommunikationsverket har specificerat och driver.

EPP är ett XML-baserat tekniskt gränssnitt som specificeras i RFC-dokument och som en registrar kan ansluta till från sitt eget kundprogram. Kommunikationsverket tillhandahåller inget färdigt kundprogram, utan registraren ska själv programmera sitt kundprogram eller anskaffa ett sådant. EPP-gränssnittet är inte obligatoriskt, utan det är ett alternativt sätt till webbläsargränssnittet att göra registreringar och förvalta domännamn. Registrarerna kan också använda båda gränssnitten.

Enligt 9 § 2 mom. i föreskriften ska registrarens kundprogram vara kompatibelt med det EPP-gränssnitt som Kommunikationsverket har specificerat, om registraren använder Kommunikationsverkets EPP-gränssnitt. Kommunikationsverkets EPP-gränssnitt bygger på flera RFC-dokument och är förenligt med dessa till den del det är möjligt. De aktuella RFC-dokumenten finns i referenslistan [8–15].

Gränssnittsbeskrivningen finns som bilaga till föreskrift 68 och föreskriften ålägger registrarerna att genomföra EPP-gränssnittet enligt bilagan. Över-

ensstämmelse med krav ska enligt föreskriften säkerställas med hjälp av Kommunikationsverkets EPP-testsystem. För att en registrar ska kunna börja använda ett EPP-kundprogram, ska programmet testas först. Programmet ska genomgå de tester i EPP-miljön som Kommunikationsverket kräver innan registraren kan införa Kommunikationsverkets EPP-gränssnitt.

Föreskriftens 9 § 3 mom. innehåller närmare föreskrifter om de krav som gäller det tekniska genomförandet av registrering och administrering av domännamn under toppdomänen ax. Enligt momentet ska registraren som tekniskt gränssnitt använda det webbläsargränssnitt som finns på www.whois.ax. Det är ett tekniskt gränssnitt som Ålands landskapsregering tillhandahåller registrarer som gör registreringar i domännamnsregistret och administrerar domännamn under toppdomänen ax.

Om Ålands landskapsregering senare beslutar införa ett eget EPP-gränssnitt, kan föreskriften kompletteras i fråga om tekniska gränssnittsspecifikationer som gäller förmedling och administrering av domännamn under toppdomänen ax.

Enligt 170 § 1 mom. 3 punkten i informationssamhällsbalken ska en registrar kunna göra anteckningar i domännamnsregistret med hjälp av tekniska arrangemang som Kommunikationsverket har fastställt. Enligt motiveringen till punkten ska registraren ha tekniska förutsättningar att göra anteckningar i registret och att vidta andra åtgärder. Med tanke på den praktiska verksamheten har de tekniska förutsättningarna en avgörande betydelse, eftersom registraren på domännamnsanvändarens vägnar kan vidta alla åtgärder som gäller domännamnet.

10 § Överföring av domännamn till en annan användare

I 10 § i föreskriften fastställs det förfarande som ska tillämpas när en domännamnsanvändare vill överföra sitt domännamn till en annan användare. Domännamnsanvändaren ska begära överföring av registraren. Efter att registraren har fått begäran om överföring ska registraren säkerställa att användaren har rätt att överföra domännamnet och begära att den myndighet som förvaltar domännamnsregistret sänder domännamnets överföringskod till användaren.

Enligt den nya verksamhetsmodellen ska registraren genomföra överföringen tekniskt. Av registraren krävs ändamålsenlig och tillräcklig noggrannhet för att säkerställa att ingen annan än den som har registrerats som användare av domännamnet ber om överföring. Skyldigheten att försäkra sig om användarens rätt att begära överföring av domännamn är motiverad för att registraren omsorgsfullt ska kunna genomföra denna åtgärd som är viktig med tanke på användarens rättsskydd. Om någon annan än en fysisk person som registrerats som användare av ett domännamn begär överföring av domännamnet, ska registraren be om en ändamålsenlig fullmakt som getts av användaren. Om en juridisk person som registrerats som användare av ett domännamn begär överföring av domännamnet, ska registraren försäkra sig om att den som lämnat begäran är berättigad att handla på användarens vägnar. Med detta avses begäran om nödvändiga ytterligare

uppgifter, om de uppgifter som lämnats i anslutning till begäran om överföring av domännamn inte stämmer överens med registrarens uppgifter eller om registraren av något annat skäl har anledning att misstänka exempelvis existensen av användarens viljeuttryck.

Efter att registraren har fått begäran om överföring ska registraren begära att den myndighet som förvaltar domännamnsregistret sänder domännamnets överföringskod till användaren. Domännamnets överföringskod definieras i 3 § 1 punkten i föreskriften. Enligt definitionen avses med domännamnets överföringskod en av den myndighet som förvaltar domännamnsregistret angiven kod med vilken ett domännamn kan överföras från en användare till en annan. Därför kan registraren inte själv skapa någon kod. Syftet med förfarandet är att säkerställa att registraren inte utan användarens begäran kan överföra domännamn till en annan användare. Den myndighet som förvaltar domännamnsregistret sänder överföringskoden till användaren som i sin tur kan ge koden till registraren för överföring av domännamnet. Syftet med förfarandet är att säkerställa att användaren av ett domännamn uttryckligen framfört sitt viljeuttryck, när domännamnet överförs till en annan användare.

10.1 Domännamnets överföringstid

Enligt 10 § 2 mom. i föreskriften ska registraren överföra domännamnet till den nya användaren inom fem vardagar från det att domännamnsanvändaren har lämnat domännamnets överföringskod och uppgifterna om den nya användaren till registraren. Denna tidsfrist anses vara ett rimligt krav för servicenivå, även om det inte finns något hinder för en snabbare överföring. Enligt 168 § 1 mom. i informationssamhällsbalken ska registraren göra överföringen inom rimlig tid från mottagandet av begäran.

10.2 Rollen för den myndighet som förvaltar domännamnsregistret vid förfarandet för överföring av domännamn

Om domännamnet inte har överförts inom rimlig tid kan den myndighet som förvaltar domännamnet göra överföringen. I praktiken innebär det t.ex. att Kommunikationsverket sänder domännamnets överföringskod till användaren på användarens begäran. Avsikten är att rollen för den myndighet som förvaltar domännamnsregistret ska vara sekundär när den nya registry-registrarmodellen införs i enlighet med informationssamhällsbalken. Det är emellertid nödvändigt att säkerställa möjligheten att överföra domännamn i situationer där en registrar av något skäl inte sörjer för sina lagstadgade skyldigheter.

Kommunikationsverkets uppgift är att övervaka att lagen iakttas när det gäller fi-domäner, och vid behov kan verket ingripa i registrarernas verksamhet. Vid tillsynen kan Kommunikationsverket vidta åtgärder enligt 171 § 2 mom. i informationssamhällsbalken. Kommunikationsverket kan ge en registrar en anmärkning, ett bindande beslut eller i sista hand ett förbudsbeslut, om registraren bryter mot bestämmelserna i informationssamhällsbalken eller bestämmelser, föreskrifter och beslut som utfärdats med stöd av den. Förbudsbeslutet innebär att registraren för en tid av högst ett år

förbjuds att registrera domännamn eller göra anteckningar som gäller domännamn i domännamnsregistret. För ax-domäner skulle tillsynsmyndigheten enligt nuvarande praxis vara Ålands landskapsregering.

10.3 Ett anhängigt tvistemåls inverkan på överföringsförfarandet

Enligt 168 § 1 mom. i informationssamhällsbalken kan ett domännamn inte överföras om ett ärende som gäller avregistrering av domännamnet är anhängigt vid Kommunikationsverket. Detta beror på att Kommunikationsverket vid behandling av ett pågående tvistemål ska fatta beslut som gäller parterna, vilket inte skulle vara möjligt om parterna kunde bytas under processen. När ett tvistemål anhängiggörs *suspenderar* Kommunikationsverket domännamnet, vilket innebär att detta inte kan överföras till någon annan. Suspenderingen påverkar inte annan användning av domännamnet och t.ex. till domännamnet anslutna tjänster, såsom webbsidor, kan fungera normalt.

10.4 Att återföra ett domännamn

Enligt 168 § 2 mom. i informationssamhällsbalken kan Kommunikationsverket återföra domännamnet till dess ursprungliga användare om domännamnet har överförts till någon annan utan användarens samtycke och denne begär att registreringen ska korrigeras, och mottagaren av överföringen inte inom utsatt tid anför en godtagbar grund för överföringen. Enligt motiveringen till momentet skyddar bestämmelsen domännamnsanvändaren mot överföringar som uppsåtligen eller av vårdslöshet är felaktiga. Kommunikationsverkets möjlighet att korrigera en överföring av ett domännamn som inte gjorts i god tro förutsätter enligt motiveringen till momentet starka bevis för att domännamnet har överförts utan den ursprungliga användarens samtycke. Registrarerna ska sörja för en tillräcklig dokumentering av sina överföringsrutiner så att det med tanke på domännamnsanvändarens rättsskydd är möjligt att utreda ärenden i efterhand.

11 § Byte av registrar

I 11 § i föreskriften fastställs det förfarande som ska tillämpas när en domännamnsanvändare vill byta registrar. I princip har användaren två alternativa sätt att göra det. Användaren kan begära att den nya registraren skaffar koden för registrarbyte från den gamla registraren. Alternativt kan användaren också begära koden för registrarbyte från sin avtalspart, eller den gamla registraren, och sända den till den nya registraren. Med andra ord får den nya registraren koden antingen av den gamla registraren eller av användaren, vartefter den kan börja förvalta domännamnet.

Koden för registrarbyte definieras i 3 § 2 punkten i föreskriften. Enligt definitionen avses med kod för registrarbyte en kod med vilken förvaltningen av ett domännamn kan överföras från en registrar till en annan. I regel skapas koden av den gamla registraren. Begreppen *gammal registrar* och *ny registrar* definieras också i 3 och 4 punkten i samma paragraf. Med gammal registrar avses en registrar som avstår från förvaltningen av ett

domännamn vid registrarbyte, och med ny registrar en registrar som tar emot förvaltningen av ett domännamn vid registrarbyte.

Enligt bestämmelsen i föreskriften ska den gamla registraren säkerställa att användaren eller den nya registraren har rätt att begära koden för registrarbyte. I praktiken krävs ändamålsenlig och tillräcklig noggrannhet av den gamla registraren för att säkerställa att ingen annan än den som har registrerats som användare av domännamnet ber om byte av registrar. Om någon annan framställer begäran, ska denne visa upp en tillräcklig fullmakt för att kunna vidta rättshandlingen. Vid behov kan registraren exempelvis kontakta användaren för att kontrollera ärendet.

11.1 Tidsfrist för byte av registrar och skriftlig begäran

I 11 § 2 mom. i föreskriften meddelas att den gamla registraren ska sända koden för registrarbyte till den som begärt den inom fem vardagar från den berättigade begäran. Om den gamla registraren inte har sänt koden för registrarbyte till den nya registraren eller till användaren inom utsatt tid, kan den nya registraren begära att den myndighet som förvaltar domännamnsregistret sänder koden för registrarbyte till användaren.

Enligt motiveringen till 168 § 3 mom. i informationssamhällsbalken om byte av registrar ska registraren, efter att domännamnsanvändaren har underrättat registraren om sin vilja att byta registrar, inom en rimlig tid vidta de åtgärder som krävs för bytet och främja bytet. Med rimlig tid avses i Kommunikationsverkets föreskrift fem vardagar, men det finns inget hinder för en snabbare service.
Om ett domännamn inte överförs för förvaltning hos en ny registrar inom rimlig tid får den myndighet som förvaltar domännamnet göra överföringen. I praktiken sänder t.ex. Kommunikationsverket koden för registrarbyte till användaren.

I 11 § i föreskriften förutsätts det att begäran om registrarbyte ska göras skriftligen, till exempel per e-post. På så sätt är det vid behov i efterhand möjligt att utreda om tidsfristen har gått ut eller inte, eller andra oklarheter vid förfarandet.

11.2 Rollen för den myndighet som förvaltar domännamnsregistret vid byte av registrar

Enligt informationssamhällsbalken är Kommunikationsverkets uppgift att vara det sista alternativet i situationer där en gammal registrar av någon anledning försummar att utföra sina lagstadgade uppgifter. Kommunikationsverkets uppgift är att övervaka att lagen iakttas när det gäller fi-domäner, och vid behov ingriper verket i registrarernas verksamhet. Vid tillsynen kan Kommunikationsverket vidta åtgärder enligt 171 § 2 mom. i informationssamhällsbalken. Kommunikationsverket kan ge en registrar en anmärkning, ett bindande beslut eller i sista hand ett förbudsbeslut, om registraren bryter mot bestämmelserna i informationssamhällsbalken eller bestämmelser, föreskrifter och beslut som utfärdats med stöd av den. För-

budsbeslutet innebär att registraren för en tid av högst ett år förbjuds att registrera domännamn eller göra anteckningar som gäller domännamn i domännamnsregistret. För ax-domäner skulle tillsynsmyndigheten enligt nuvarande praxis vara Ålands landskapsregering.

Enligt motiveringen till 168 § 3 mom. i informationssamhällsbalken om byte av registrar kan en domännamnsanvändare fritt byta registrar när som helst. Det krävs inga särskilda skäl för byte av registrar. Momentet reglerar inte domännamnsanvändarens och registrarens avtalsförhållande, utan de avtals- eller konsumenträttsliga frågor som sammanhänger med överföringen avgörs med stöd av annan lagstiftning. I motiveringen till 171 § i informationssamhällsbalken konstateras att Kommunikationsverket inte har befogenhet att avgöra avtalstvister mellan domännamnsanvändare och registrarer. Enligt 303 § 2 mom. i informationssamhällsbalken omfattar Kommunikationsverkets beslutanderätt inte frågor som gäller avtalsförhållanden eller ersättningsansvar mellan företag och abonnenter. På avtalen mellan ett företag och en konsument tillämpas konsumentskyddslagen (38/1978) som innehåller reglering t.ex. av avtalsvillkor, marknadsföring av tjänster och distansförsäljning. Behörig myndighet i konsumentreglering är Konsumentombudsmannen vars centrala uppgift är att övervaka att konsumentskyddslagen och flera andra lagar som stiftats för att skydda konsumenter följs. Konsumentombudsmannen behandlar i regel inte enstaka tvister. De behandlas av konsumenträttsrådgivare och konsumenttvistenämnden. Mer information om konsumentskyddet finns på Konkurrens- och konsumentverkets webbplats www.kkv.fi.

3 kap. Krav som gäller domännamn

Detta kapitel behandlar de förpliktelser som föreskrivs i 3 kap. i föreskriften, det vill säga de tekniska kraven för domännamn.

12 § Domännamnets form

I 12 § 1 mom. i föreskriften fastställs de tecken som är tillåtna i domännamn, nämligen bokstäverna a–z, siffrorna 0–9 och bindestreck-minus.

I tabellen i 2 mom. i föreskriften ingår främst de tecken som skiljer det svenska, finska och samiska alfabetet från det latinska. Enligt föreskriften är tillåtna tecken de nationella tecken som specificeras i listan.

Tecken	Unicode-kod	Namn
-	002D	Bindestreck-minus
á	00E1	Latinskt gement a med akut accent
â	00E2	Latinskt gement a med cirkumflex
ä	00E4	Latinskt gement a med trema (lilla ä i allmänspråket)
å	00E5	Latinskt gement a med en övre ring (lilla svenskt å i allmänspråket)

č	010D	Latinskt gement c med omvänt cirkumflex (lilla c med ett tak i allmänspråket)
đ	0111	Latinskt gement och stunget d
ǥ	01E5	Latinskt gement och stunget g
ǧ	01E7	Latinskt gement g med omvänt cirkumflex
ǩ	01E9	Latinskt gement k med omvänt cirkumflex
ŋ	014B	Latinskt gement eng
õ	00F5	Latinskt gement o med tilde
ö	00F6	Latinskt gement o med trema (lilla ö i allmänspråket)
š	0161	Latinskt gement s med omvänt cirkumflex (lilla s med ett tak i allmänspråket)
ŧ	0167	Latinskt gement och stunget t
ž	017E	Latinskt gement z med omvänt cirkumflex (lilla z med ett tak i allmänspråket)
ʒ	0292	Latinskt gement ezh
ǯ	01EF	Latinskt gement ezh med omvänt cirkumflex

Bindestreck-minus specificeras med en Unicode-kod i tabellen. Enligt 12 § i föreskriften får ett domännamn inte börja eller sluta med ett bindestreck-minus. Detta bygger på RFC-dokumentet 1035 [3]. Dessutom föreskrivs det att ett domännamn inte får börja med tecknen xn--. Detta beror på att de är reserverade som förtecken för ACE-kodade IDN- domännamn (Internationalized Domain Names) som innehåller nationella tecken. Enligt 12 § i föreskriften börjar ett domännamn som innehåller nationella tecken i ACE-format (ASCII Compatible Encoding) alltid med tecknen xn--. Kraven bygger på RFC-dokumenten RFC 3492 [4] och RFC 3490 [5].

Enligt 166 § 1 mom. i informationssamhällsbalken får ett domännamn bestå av minst två och högst 63 tecken. Denna begränsning är förenlig med RFC-dokumentet 1034 [6].

13 § Namnservrar

I 13 § i föreskriften meddelas närmare föreskrifter om konfigurationer av namnservrar med domännamn. Kravet gäller enbart domännamn som är införda tillsammans med namnservrar i domännamnsregistret. Domännamn behöver inte ha några konfigurationer av namnservrar. Namnservrar ska avregistreras i domännamnsregistret om en domännamnsanvändare fortfarande vill reservera sitt domännamn utan att det har några anslutna funktioner som en e-post eller en webbplats.

Minst två av varandra oberoende namnservrar ska konfigureras med ett domännamn. Detta säkerställer att domännamnet fungerar även om det uppstår ett fel i en av namnservrarna. Kommunikationsverket har fastställt att antalet namnservrar får vara högst tio. Namnservrarna är oberoende av varandra när namnservrarna fungerar på olika servrar och IP-adresser och bakom olika internetförbindelser.

Alla namnservrar ska kunna nås av datornätet internet och Kommunikationsverket ska kunna granska konfigurationerna med namnserverförfrågningar. Kommunikationsverket kontrollerar för alla namnservrar att de fungerar. Om en eller flera namnservrar inte fungerar eller om konfigurationerna av namnservrarna är felaktiga, skickar Kommunikationsverket ett e-postmeddelande med anmärkning till registraren eller till den av registraren uppgivna e-postadressen till den som underhåller namnservrarna.

Enligt 13 § i föreskriften ska namnservrarna vara försedda med NS-poster (Name Server) där alla namnservrar för ett domännamn har konfigurerats. NS-posterna ska anvisa till servrar för vilka en IP-adress har konfigurerats i A-posten eller i AAAA-posten eller båda i DNS-tjänsten. NS-posterna kan endast vara namnservrar för vilka ett domännamn de facto har konfigurerats. NS-posterna ska vara förenliga med uppgifterna i fi-roten.

Enligt 13 § i föreskriften ska den SOA-post (Start of Authority) som bestämmer konfigurationen av namnservern för ett domännamn motsvara följande krav:

1) i fältet MNAME (Master Name) ska namnet på den primära namnservern för domännamnet finnas,

2) i fältet RNAME (Responsible Name) ska en fungerande e-postadress finnas för den aktör som ansvarar för underhåll av namnservrarna. E-postadressen ska konfigureras utan tecknet @, som ersätts med punkt, till exempel hostmaster.domain.fi. Bästa sättet att konfigurera en hostmaster-adress i fältet RNAME är att följa RFC 2142. [7].

Kommunikationsverket rekommenderar att serienumren och klockorna för SOA-posten inte väsentligt avviker från de internetstandarder och -rekommendationer som publicerats. Kommunikationsverkets rekommendationer är följande:

```
example.com.  3600  SOA  dns.example.com. hostmaster.example.com. (
                         1999022301   ; serial YYYYMMDDnn
                         86400        ; refresh (  24 hours)
                         7200         ; retry   (   2 hours)
                         3600000      ; expire  (1000 hours)
                         172800 )     ; minimum (   2 days)
```

Den rekommenderade formen för serienummer är YYYYMMDDnn, där YYYY avser år, MM månad, DD dag och nn är ett löpande nummer vars värde ökar med ett vid varje uppdatering. Dagens första version är 01. Med hjälp av serienummer är det möjligt att kontrollera att domännamnets samtliga namnservrar har samma zone-poster. Ett serienummer får inte vara noll (0).

Värdena refresh och retry inverkar på hur ofta de sekundära namnservrarna kontrollerar om domännamnets namnserverinformation har ändrats på den primära namnservern. Värdet retry fastställer den tid under vilken

namnserverinformationen söks på nytt, om den föregående sökningen misslyckats.

Värdet expire anger hur lång tid en namnserver förvarar en gammal zonefil i en situation där det inte är möjligt att söka en ny fil.

Värdet Minimum TTL (time to live) fastställer en standard livslängd för RR-posterna (resource record). I vissa fall är det motiverat att fastställa ett lägre TTL-värde än det rekommenderade, till exempel vid förändringar av namnservrar.

Kommunikationsverkets rekommendationer

Kommunikationsverket rekommenderar att överföring av domännamnsinformation (AXFR, DNS zone transfer protocol) förhindras för utomstående.

Dessutom rekommenderar Kommunikationsverket att namnservrarna inte returnerar rätt information vid förfrågan om namnserverns programversion. Att återställa den rätta programversionen kan riskera informationssäkerheten, om det exempelvis finns ett känt informationssäkerhetsproblem i den version av namnserverprogrammet som används.

4 kap. Hantering av registrarens informationssäkerhet

Detta kapitel behandlar de krav för informationssäkerheten vid förmedling av domännamn som fastställs i föreskriftens kapitel 4. Kraven bygger på 170 § 1 mom. 6 punkten i informationssamhällsbalken, enligt vilken en registrar ska sörja för informationssäkerheten i sin verksamhet. Enligt motiveringen till punkten ska registraren fastställa detaljerade och tillräckliga anvisningar med tanke på hot mot informationssäkerheten. Registraren ska förvissa sig om att händelser som är relevanta för informationssäkerheten noteras. Dessutom ska registraren ingripa när det konstateras problem och avvikelser i informationssäkerhetssituationen.

Med *informationssäkerhet* avses enligt 3 § 1 mom. 28 punkten i informationssamhällsbalken administrativa och tekniska åtgärder genom vilka det säkerställs att information är tillgänglig endast för dem som har rätt att använda den, att informationen inte kan ändras av andra än dem som har rätt till detta samt att informationen och informationssystemen kan utnyttjas av dem som har rätt att använda informationen och systemen. Informationssäkerhet innebär m.a.o. åtgärder för att säkerställa informationens konfidentialitet, integritet och tillgänglighet.

I föreskriften beskrivs de minimikrav för hantering av informationssäkerheten som alla registrarer ska uppfylla i sin verksamhet. Syftet med kraven är att säkerställa en grundläggande informationssäkerhetsnivå i registrarverksamheten, som i sin tur ligger till grund för att säkerställa informationssäkerheten i servicen. Kraven fokuserar särskilt på kontinuerlig utveckling, planering, genomförande och bedömning av hantering av informations-

säkerheten. Syftet med bestämmelserna är även att minska på negativa konsekvenser av informationssäkerhetsriskerna för registrarverksamheten och användarna av domännamn.

14 § Hänsynstagande till informationssäkerheten

Informationssäkerheten utgör en viktig del av kvaliteten på den registrarverksamhet som registraren bedriver. Hänsynstagandet till de olika delområdena i informationssäkerheten vid förmedling är viktigt i alla livscykler för tjänsten: vid planering, genomförande och underhåll av tjänsten samt när tjänsten tas ur bruk. För att informationssäkerheten ska ombesörjas rutinmässigt varje dag, är det motiverat att registraren fastställer processer och rutiner för att genomföra informationssäkerheten.

Registraren ska ha dokumenterade metoder för att sörja för informationssäkerheten. De uppdaterade dokumenten skapar en grund för en systematisk utveckling och hantering av informationssäkerheten och hjälper till att rikta investeringarna i informationssäkerhet. Utifrån dokumentationen kan också Kommunikationsverket vid behov verifiera att registraren iakttar sina skyldigheter att sörja för informationssäkerheten.

14.1 Delområden som ska beaktas

Det finns flera olika faktorer som ska beaktas vid genomförandet av informationssäkerheten och i de dokument som beskriver det. Paragrafen räknar upp de sakhelheter som ska beaktas, men ställer inga exakta krav på hur helheterna egentligen ska beaktas. Orsaken är att företagen genomför den ändamålsenliga informationssäkerheten på olika sätt, beroende på bl.a. vilka tjänster som företaget tillhandahåller. Minimikraven, som ingår i flera av sakhelheterna, behandlas någon annanstans i denna föreskrift. Det väsentliga i 14 § i föreskriften är att registraren ska identifiera de krav som gäller för dess verksamhet samt de rutiner som ska tillämpas för att kraven ska uppfyllas.

Nedan finns exempel enligt sakhelhet på faktorer för att sörja för informationssäkerheten. Förteckningen innehåller också hänvisningar till de minimikrav som Kommunikationsverket har ställt.

1. Administrativ informationssäkerhet
   - Styrdokument för informationssäkerhet (vanligen t.ex. informationssäkerhetspolicy och -arkitektur), genom vilka organisationens ledning visar de övergripande målen och de allmänna principerna för informationssäkerheten samt sitt engagemang i att genomföra informationssäkerheten.
   - Processer och hantering av dessa
   - Riskhantering och kontinuitet (se 15 § i denna föreskrift)
   - Dokumentationsrutiner och -system
   - Auditerings- och övningsförfaranden

2. Personalsäkerhet

- Ansvar och skyldigheter i anslutning till personalens informationssäkerhet
- Personalens informationssäkerhetskompetens och utveckling av den
- Bakgrundskontroller
- Nyckelpersonsrisker
- Förebyggande av farliga ansvars- och uppgiftshelheter
- Arbetsrotation i syfte att upptäcka missbruk
- Anvisningar för förfarandet när arbetsförhållandet slutar
- Missbruk och underlåtenhet att iaktta instruktioner från personalens sida

3. Maskinvaru-, programvaru- och telekommunikationssäkerhet
   - Hantering av sårbarheter
   - Observation av kränkningar av informationssäkerheten (se 17–18 § i denna föreskrift)
   - Hantering av ändringar (se 19 § i denna föreskrift)

4. Datamaterial- och driftsäkerhet
   - Säkerställande av informationens konfidentialitet, integritet och tillgänglighet
   - Klassificering av datamaterial och behandling enligt klassificeringen (se 16 § i denna föreskrift)
   - Ansvar för registret för användarrättigheter: delning, ändring och radering av användarrättigheter
   - Förebyggande av att användarrättigheter samlas på hög
   - Förhindrande av att utomstående kommer åt den hanterings- och konfigurationsinformation som anknyter till förmedling av domännamn samt kundernas fakturerings-, kund- och logguppgifter
   - Förvaring och förstöring av datamaterial

5. Fysisk säkerhet
   - Fysiskt läge för lokaler och omgivningens säkerhet
   - Åtkomsthantering
   - Strukturellt skydd

Föreskriften förutsätter att ovan angivna sakhelheter (1–5) ska beaktas i de olika skedena av livscykeln för förmedling av domännamn. Det innebär att registraren ska beakta informationssäkerheten när den planerar, genomför och underhåller tjänsten samt när den tar tjänsten ur bruk.

14.2 Informationssäkerhetsdokument

Föreskriften förutsätter att registraren ska ha uppdaterade dokument om på vilket sätt den genomför informationssäkerheten i sin verksamhet. Föreskriften fastställer inte vilka alla olika dokument registraren ska ha, utan registraren får själv bedöma det. Det viktiga är att dokumentationen är uppdaterad och att det utifrån dokumentationen är möjligt att fastslå att alla de delområden av informationssäkerheten som räknas upp i paragrafen har beaktats i verksamheten.

15 § Riskhantering

Med *säkerhetsrisk* avses sannolikhet för en viss olägenhet eller skada och dess konsekvenser. Med informationssäkerhetsrisker avses en sådan oavsiktlig eller avsiktlig faktor som äventyrar konfidentialitet, integritet eller tillgänglighet vid förmedlingen av domännamn. Informationssäkerhetsrisker skiljer sig från informationssäkerhetshot genom att informationssäkerhetsriskernas sannolikhet och verkningar har bedömts.

Informationssäkerhetsrisker kan t.ex. orsakas av

- mänskliga misstag
- brister i eller underlåtenhet att iaktta instruktioner till personalen
- stölder eller skadegörelser
- fel eller funktionsstörningar i apparater, system eller program
- spridning av skadliga program
- förstöring av datamaterial
- eldsvåda eller vattenskada
- fel och försummelser begångna av en underleverantör eller en aktör som ingår i samarbetsnätverket.

Med riskhantering avses en process som syftar till att identifera risker, minska sannolikheten för risker och/eller konsekvenser av risker till en godtagbar nivå och bibehålla den uppnådda nivån. Syftet med riskhanteringen är att skydda organisationen och dess förmåga att utföra sina funktioner med beaktande av ekonomiska omständigheter.

Genom kraven på riskhanteringen strävar man efter att säkerställa att registraren är medveten om följderna om riskerna realiseras och huruvida de riskminskande åtgärderna är tillräckliga. Målsättningen för riskhanteringen är bland annat att

- snabba upp återhämtningen efter informationssäkerhetsproblem
- minska kostnader och skador som förorsakas av informationssäkerhetsproblem
- rikta investeringar som förbättrar informationssäkerheten vid förmedlingen av domännamn
- förbättra kvaliteten och produktiviteten i förmedlingen av domännamn
- ekonomiskt optimera de risker som hänför sig till förmedlingen av domännamn
- förebygga riskerna mot förmedling av domännamn.

15.1 Riskidentifiering och -hantering

Bland annat följande standarder och publikationer om riskhantering har getts ut: ISO/IEC 27005 [21], NIST 800- 30 Risk Management Guide [22] och OCTAVE [23].

Denna föreskrift ålägger ingen skyldighet att iaktta en viss standard. Riskhanteringsmodeller skiljer sig i olika företag, och en enda modell som skulle passa för alla finns inte.

Föreskriften förutsätter att registraren ska identifiera riskerna i sin verksamhet och verksamhetens kontinuitet och att den ska hantera riskerna. Med riskhantering avses att registraren fastställer en godtagbar risknivå för sin verksamhet och genomför nivån med ändamålsenliga metoder (ofta genom s.k. kontroller). I praktiken ska registraren fastställa ansvar och tidsscheman för riskhantering. Dessutom ska den följa upp hur riskhanteringen genomförs och vilka konsekvenser riskerna medför.

Föreskriften förutsätter också att riskhanteringen ska vara regelbunden, dvs. risker och metoder för hantering av risker ska bedömas regelbundet. Registraren kan själv fastställa lämpliga uppföljningscykler. Normalt görs riskbedömningar i företag när nya tjänster eller funktioner definieras, årligen och alltid efter att en eventuell risk har realiserats.

15.2 Dokumentation av process och resultat

För att övervaka att kraven på riskhanteringen iakttas, ska registraren dokumentera den fastställda processen för riskhantering och resultaten från riskhanteringen.

16 § Datamaterial

För att information med anknytning till förmedlingen av domännamn ska vara tillgänglig endast för dem som har rätt att använda den, ska registraren ha ett klassificeringssystem och hanteringsförfaranden för sådant datamaterial som är viktigt för förmedlingen av domännamn.

16.1 Klassificering och hantering av material

Registraren ska fastställa sådana kriterier för klassificeringen av datamaterial som lämpar sig för dess verksamhet. Materialet kan exempelvis klassificeras på följande sätt: offentligt, konfidentiellt och sekretessbelagt.

Dessutom ska registraren fastställa på vilket sätt företaget hanterar (skyddar) materialet som har indelats i olika klasser.

16.2 Materialdokument

Klassificeringen och den tillhörande anvisningen för hantering av datamaterial ska dokumenteras. Faktorer som ska beaktas när klassificeringen fastställs och dokumenteras är exempelvis följande:

- allmänna principer för bedömning av datamaterialets säkerhetsklass och konfidentialitet samt hemlighållandet av datamaterial
- hanterings- och ändringsrättigheter vad gäller fördelningen av läsrättigheter till datamaterialet, ändringsrättigheter och fördelningen av dessa rättigheter
- fastställande av konfidentialitetsklass
- offentlighet av uppgifter eller dokument: till exempel rätten att tala om ett ärende offentligt
- dokumentets egenskaper: papper, stämpel och andra märkningar
- förvaring och kryptering
- utskrifter och kopiering

- säkerhetskopiering
- mottagning, distribution, sändning och transport
- dokumentering av hanteringen av uppgifter och dokument
- arkivering och hantering av dokument eller upphörande av hanteringsrätten samt förstörande av uppgifter och dokument.

17 § Övervakning av informationssäkerheten

I 17 § i föreskriften preciseras delvis informativt registrarens skyldighet enligt 170 § 1 mom. 6 punkten i informationssäkerhetsbalken att sörja för informationssäkerheten i sin verksamhet. Enligt motiveringen till punkten ska registraren förvissa sig om att händelser som är relevanta för informationssäkerheten noteras. En förutsättning är sålunda att kränkningar av och hot mot informationssäkerheten vid registrarverksamheten ska kunna upptäckas. I praktiken innebär detta att registraren ska underhålla systemet för administration av sin tjänst.

Det är viktigt att registraren på eget initiativ agerar snabbt om den upptäcker fel och störningar. Då kan registraren snabbt vidta åtgärder för att utreda, begränsa och avhjälpa fel och störningar i informationssäkerheten och dessutom behöver den inte vänta tills kunderna börjar klaga. Syftet med förebyggande av fel och störningar i informationssäkerheten är att man så tidigt som möjligt försöker upptäcka även de minsta kännetecknen för begynnande problem. Med hjälp av förebyggande åtgärder kan effekterna på registrarverksamheten minimeras och i bästa fall märks inga effekter alls.

Registraren ska kontinuerligt övervaka informationssäkerheten i sin registrarverksamhet. Registraren ska ha lämpliga mekanismer för hantering av förmedlingen av domännamn, med vilka den så snabbt som möjligt kan upptäcka problem i informationssäkerheten. Som exempel på sådana situationer kan nämnas blockeringsattacker, försök till dataintrång, informationsläckor och för omfattande behörigheter. Registraren ska också sträva efter att upptäcka situationer som håller på att utvecklas till problem i så tidigt skede som möjligt med hjälp av sina mekanismer för hantering av tjänsten. Indikatorer som förutspår störningar är till exempel mjukvarularm och kvalitetsmätare för tjänster som meddelar en avvikelse från det normala trots att de inte indikerar omedelbara störningar. Registraren är dock själv ansvarig för att specificera användbara mjukvarularm och kvalitetsmätare. Föregripande information som hjälper registraren att undvika problem med informationssäkerheten är bland annat anmälda observationer av sårbarheter i hårdvara eller mjukvara.

Enligt 2 mom. ska registraren dokumentera de mekanismer som den använder för att övervaka registrarverksamheten, så att registraren vid behov kan visa med vilka åtgärder den uppfyller de fastställda kraven. Registraren ska dokumentera sina system och förfaranden för mottagning och analys av olika larm- och anmälningsuppgifter och dokumentationen ska hållas uppdaterad. Med andra ord ska registraren ha en beskrivning av de tekniska system med vilka den hanterar och åtgärdar uppgifter och anmälningar om läget i sin tjänst.

18 § Hantering av situationer som stör eller hotar informationssäkerheten

I 18 § i föreskriften behandlas registrarens interna procedurer vid störningar. Syftet med procedurerna är att skapa färdigheter så att registrarer kan utreda orsaken till problemen i informationssäkerheten så snabbt som möjligt och minimera deras verkningar. Procedurerna har också praktisk betydelse när registraren t.ex. utbildar ny personal.

Enligt 18 § 1 mom. i föreskriften ska en registrar föra en uppdaterad dokumentation över procedurer för att reda ut situationer som stör eller hotar informationssäkerheten i registrarverksamheten samt för att minimera och avlägsna verkningarna utan obefogat dröjsmål.

Enligt 18 § 2 mom. ska procedurerna omfatta åtminstone
- organisering av hanteringen av informationssäkerhet, och
- ansvarsfördelning, inklusive åtminstone uppgifter som behövs för att nå de personer som svarar för informationssäkerheten.

Procedurerna ska naturligtvis också beakta eventuella speciella anvisningar för avhjälpande av betydande störningar. Sådana anvisningar kan vara till exempel arrangemang för jour eller arbetsberedskap.

Organisationen av hanteringen av informationssäkerheten beskrivs oftast i företagets interna informationssäkerhetspolicy, m.a.o. dokument som godkänts av företagets ledning och som beskriver målbilden och genomförandet av företagets informationssäkerhet.

19 § Hantering av ändringar

Föreskriftens 19 § föreskriver att en registrar ska genomföra ändringarna i nät, mjukvara, hårdvara, konfigurationer, gränssnitt och utrustningsutrymmen på ett väl avvägt och planmässigt sätt så att registrarverksamheten störs i minsta möjliga grad vid ändringarna. Enligt 2 mom. måste tillräckligt med tid reserveras för ändrings-, service- och uppdateringsåtgärder så att den planerade åtgärden kan utföras på ett behärskat sätt. Enligt 3 mom. ska registraren specificera och dokumentera de processer och förfaranden som styr ändringarna.

Paragrafen fastställer som utgångspunkt att registraren ska minimera störningar, som driftavbrott, som ändringarna orsakar. Avbrotten kan dock vara nödvändiga och de planerade ändringarna ska kunna göras så felfritt som möjligt. Därför betonar paragrafen att avbrotten ska dimensioneras så att registraren förutom behov av tjänster också tar hänsyn till det realistiska behovet av tid som ett omsorgsfullt ändringsarbete kräver. I 2 mom. i paragrafen bestäms i synnerhet om ett s.k. underhållsfönster och förutsätts att registraren reserverar tillräckligt med tid för åtgärderna.

För att hantera ändringar och minimera olägenheter ska registraren, innan den börjar genomföra ändringen, omsorgsfullt planera hur ändringsarbetet fortskrider och behövliga resurser, uppskatta ändringsarbetets inverkan och

varaktighet samt i förväg planera åtgärder som vidtas om ändringen inte sker som planerat. Om registraren t.ex. byter program för utrustningen eller gör ändringar i konfigurationerna lönar det sig att, om möjligt, simulera ändringens inverkan på förhand, till exempel för att ta reda på var felen kan finnas och avhjälpa dem i förväg.

Registraren ska i förväg definiera och dokumentera de processer och förfaringssätt som hänför sig till ändringsarbeten så att alla ändringsarbeten utförs på ett planenligt och förutsebart sätt.

För varje ändrings-, service- eller uppdateringsåtgärd ska registraren i enlighet med sina fastställda processer och förfaringssätt beräkna den tid som behövs för arbetena och reservera denna tid för att slutföra arbetet.

20 § Katakri-kraven vid användning av Kommunikationsverkets EPP-gränssnitt

I 20 § i föreskriften beskrivs de krav som en registrar av domännamn under toppdomänen fi ska uppfylla, om den använder Kommunikationsverkets EPP-gränssnitt som ett tekniskt gränssnitt. I så fall är kravet att registraren uppfyller kriterierna härledda från skyddsnivå (IV) enligt delområde I, teknisk informationssäkerhet, i den version av Katakri (verktyg för informationssäkerhetauditering) som gäller vid respektive tidpunkt, till följande delar:

1) Datakommunikationssäkerhet
2) Säkerhet i informationssystem.

Katakri är ett auditeringsverktyg för myndigheter när de bedömer den berörda organisationens förmåga att skydda myndighetens sekretessbelagda information. I Katakri har man samlat in de minimikrav som grundar sig på nationella författningar och internationella förpliktelser. Katakri 2015 auditeringsverktyget har godkänts för användning i nationella säkerhetsmyndighetens (NSA) samarbetsgrupp den 26 mars 2015. Avsikten har varit att göra Katakri mer hållbart för att undvika upprepande totalreformer.

Som sådant ställer Katakri inte några absoluta krav för informationssäkerheten, utan de insamlade kraven baserar sig på gällande lagstiftning och de informationssäkerhetsförpliktelser som är bindande för Finland. Kraven i Katakri är markerade med en källhänvisning för att säkerställa insyn.

Kraven i Katakri är uppdelade i tre delområden:

Delområde (T) som gäller säkerhetsledning vill säkerställa att organisationen har tillräckliga färdigheter och förmåga för säkerhetsledning.

Delområde (F) som gäller fysisk säkerhet beskriver säkerhetskraven för den fysiska användningsmiljön för sekretessbelagd information.

Delområde (I) som gäller teknisk informationssäkerhet beskriver säkerhetskraven för den tekniska databehandlingsmiljön. Detta delområde uppdelas i tre skyddsnivåer enligt den information som behandlas (ST IV, ST III, ST II).

Föreskriften förutsätter att registrarer som använder Kommunikationsverkets EPP-gränssnitt uppfyller kraven på den tekniska informationssäkerhetens delområde gällande datakommunikationssäkerhet och säkerhet i informationssystem. Syftet med föreskriften är att säkerställa en hög informationssäkerhetsnivå hos registrarernas kunder.

Kommunikationsverket konstaterar också att föreskriftens krav uttryckligen gäller förmedling av domännamn, vilket har konstaterats i 2 § som gäller föreskriftens tillämpningsområde. Om den som förmedlar domännamn också utövar annan verksamhet, gäller föreskriften inte den andra verksamheten.

Kommunikationsverkets föreskrift hänvisar till gällande kriterier. Den gällande versionen av Katakri finns på försvarsministeriets webbplats på defmin.fi.

5 kap. Anmälningsskyldighet vid störningar

Detta kapitel behandlar de förpliktelser som fastställs i föreskriftens kapitel 5. Förpliktelserna preciserar kraven enligt 170 § 1 mom. 7 punkten i informationssamhällsbalken gällande anmälningar om betydande störningar i informatiossäkerheten, som ska göras till den myndighet som förvaltar domännamnsregistret.

21 § Registrarens störningsanmälan till den myndighet som förvaltar domännamnsregistret

Föreskriftens 21 § innehåller mer detaljerade bestämmelser om innehållet i registrarens anmälningsskyldighet vid störningar i informationssäkerheten.

Skyldigheten som föreskrivs i 170 § 1 mom. 7 punkten i informationssamhällsbalken är ny för registrarer. Enligt paragrafen ska en registrar utan dröjsmål meddela Kommunikationsverket om dess förmedling av domännamn är utsatt för betydande kränkningar av eller hot mot informationssäkerheten eller för någonting annat som väsentligen förhindrar eller stör den. Samtidigt ska registraren också anmäla hur länge störningen eller hotet beräknas pågå, om vilka verkningar störningen eller hotet har, om avhjälpande åtgärder samt om åtgärder för att förhindra att störningen upprepas. I motiveringen till punkten nämns exempelvis en situation där någon har gjort intrång i registrarens system. Det är nödvändigt att tillsynsmyndigheten utan dröjsmål får veta om det, emedan risken är att den som står bakom intrånget fritt kan komma åt att ändra uppgifter om domännamn som registraren i fråga förvaltar, såsom namnservrar. I motiveringen till punkten konstateras det att hotet begränsas till denna registrars kunder,

men att det ändå kan gälla en stor kundkrets. För ax-domäner skulle tillsynsmyndigheten enligt nuvarande praxis vara Ålands landskapsregering.

I en anmälan om betydande informationssäkerhetsstörning till Kommunikationsverket enligt 21 § 1 mom. i föreskriften ska en registrar, förutom de uppgifter som förutsätts i lagen, också i mån av möjlighet redogöra för orsaken till störningen eller hotet och hur störningen har framkallats. Störningsanmälan ska göras inom 24 timmar från det att registraren har fått veta om störningen. Anmälan ska kompletteras senare till den del alla de uppgifter som krävs inte finns tillgängliga vid anmälningstidpunkten.

21.1 Betydande kränkningar av informationssäkerheten

Enligt 170 § 2 mom. i informationssamhällsbalken får Kommunikationsverket meddela närmare föreskrifter om när en störning som avses i 1 mom. 7 punkten ska anses vara betydande samt om innehållet i anmälan samt anmälans utformning och hur den lämnas in.

I detta skede anser Kommunikationsverket att det inte finns någon anledning att meddela närmare föreskrifter om när en störning i informationssäkerheten är betydande. Anmälningströskeln kan senare fastställas närmare genom en ändring i föreskriften, om det utifrån tillsynserfarenheter visar sig vara nödvändigt. Enligt Kommunikationsverkets uppfattning är det emellertid nödvändigt att lyfta fram vissa synpunkter som ska beaktas vid bedömning av om en störning är betydande eller inte.

Vid bedömning av om en kränkning av informationssäkerheten eller någon annan händelse är betydande eller inte ska hänsyn tas till vilka negativa konsekvenser händelsen har eller hur allvarligt hotet mot informationssäkerheten till följd av händelsen är. Kränkningar av informationssäkerheten kan ha konsekvenser för uppgifternas eller datasystemens konfidentialitet, integritet eller tillgängliget.

Med konfidentialitet avses i detta sammanhang att uppgifter och verifieringsuppgifter om användarnamn endast är tillgängliga för dem som är berättigade att få uppgifterna. Med integritet avses att det inte är möjligt att obehörigt göra ändringar i uppgifter och att utomstående inte har möjlighet att inverka på datasystemens funktion. Med tillgänglighet avses att en tjänst eller uppgifter i tjänsten är tillgängliga för dem som är berättigade till den.

En störning i informationssäkerheten är alltid betydande om den drabbar följande objekt:

- de data- och kommunikationssystem som används för registrarens tjänster och produktion av tjänster
- informationssäkerheten, skyddet av personuppgifter eller skyddet av företagshemligheter hos registrarens kunder

- fi-roten i Finland, som administreras av Kommunikationsverket, till följd av en direkt eller indirekt kränkning av informationssäkerheten hos en registrar.

Som en betydande störning betraktas också verksamhet som är ofta återkommande eller exceptionellt långvarig eller verkar avsiktlig och som har negativa konsekvenser för en registrars förmåga att sörja för informationssäkerheten i registrarverksamheten.

Detsamma gäller också när en störning inte kan undanröjas enbart genom registrarens egna åtgärder.

21.2 Exempel på sådana typer av kränkningar i informationssäkerheten som omfattas av anmälningsskyldighet

Nedan finns exempel på sådana typer av kränkningar i informationssäkerheten som enligt Kommunikationsverkets uppfattning ska meddelas utifrån 170 § 1 mom. 7 punkten i informationssamhällsbalken. Förteckningen är inte täckande utan syftet är att beskriva allvarlighetsgraden för de fall som ska anmälas. Betydande störningar i informationssäkerheten som avses i 7 punkten och som överskrider informationströskeln är till exempel

21.2.1 Dataintrång i registrarens datasystem

- Obehörig åtkomst till registrarens system
- Sårbarheter eller konfigurationsfel som riskerar informationssäkerheten i registrarens system

21.2.2 Tredje parter får kännedom om inloggningskoder
- Utomstående kommer över de inloggningskoder som används till Kommunikationsverkets system

21.2.3 Obehöriga ändringar

- Möjlighet att obehörigt ändra uppgifter om de domännamn som registrarer förvaltar
- Ändringar som en registrars anställda obehörigt gör i Kommunikationsverkets domännamnsregister
- Obehörig åtkomst till en självbetjäningsportal som en registrar tillhandahåller sina kunder och där kunderna själva kan uppdatera uppgifterna om sina domännamn

21.2.4. Blockeringsattacker

- En registrars system lamslås och/eller kundernas åtkomst till systemet förhindras
- En systemstörning påverkar funktionen i Kommunikationsverkets system

21.3 Rekommendation om frivilliga anmälningar

Kommunikationsverket rekommenderar att registrarerna efter gottfinnande underrättar Kommunikationsverket också om kränkningar av och hot mot informationssäkerhet som är av mindre betydelse. Sådan information kan ha betydelse för att Kommunikationsverket ska kunna inleda åtgärder enligt 172 § i informationssamhällsbalken, eller för att Kommunikationsverket ska kunna sköta andra informationssäkerhetsuppgifter som föreskrivs i 304 § 1 mom. 1, 7, 8 och 10 punkten i informationssamhällsbalken.

Enligt 172 § 1 mom. i informationssamhällsbalken har Kommunikationsverket rätt att vidta nödvändiga åtgärder för att upptäcka, förhindra och utreda sådana betydande kränkningar av informationssäkerheten som innebär att fi-domännamn utnyttjas och som är riktade mot allmänna kommunikationsnät eller kommunikationstjänster eller mot användare av dem, samt för att inleda förundersökning med anledning av kränkningarna. Kommunikationsverket får vidta dessa åtgärder utan att höra domännamnsanvändaren.

Enligt 2 mom. i paragrafen kan de nödvändiga åtgärder som avses i 1 mom. utföras med avseende på namnserverinformationen i fi-roten och kan omfatta
1) åtgärder för att förhindra eller begränsa den trafik som riktas till domännamnet,
2) åtgärder för att dirigera den trafik som riktas till domännamnet till en annan webbadress, samt
3) andra med 1 och 2 punkten jämförbara åtgärder av teknisk natur.

Enligt 3 mom. ska de åtgärder som avses i 172 § utföras omsorgsfullt och de ska stå i proportion till allvaret i den kränkning av informationssäkerheten som ska avvärjas. Åtgärderna ska utföras utan att yttrandefriheten, skyddet av konfidentiella meddelanden eller integritetsskyddet begränsas mer än vad som är nödvändigt med tanke på säkerställandet av möjligheterna att uppnå målen enligt 1 mom. Åtgärderna ska avbrytas, om det inte längre finns förutsättningar enligt denna paragraf att vidta dem.

I 304 § i informationssamhällsbalken ingår bestämmelser om Kommunikationsverkets särskilda uppgifter. Enligt paragrafen ska Kommunikationsverket

- främja den elektroniska kommunikationens funktion, störningsfrihet och trygghet (1 punkten),
- samla in information om kränkningar och hot om kränkningar av informationssäkerheten för nättjänster, kommunikationstjänster och mervärdestjänster samt om fel och störningar i kommunikationsnät och kommunikationstjänster (7 punkten),
- informera om frågor som gäller informationssäkerhet samt om kommunikationsnäts och kommunikationstjänsters funktion (8 punkten),
- utreda kränkningar och hot om kränkningar av informationssäkerheten för nättjänster, kommunikationstjänster och mervärdestjänster (10 punkten).

21.4 Anmälningsförfarande

Upptäckt av en störning i informationssäkerheten ska anmälas till den myndighet som förvaltar domännamnsregistret så fort som möjligt, dock senast inom 24 timmar i enlighet med föreskriftens 21 § 2 mom. Anmälan ska i första hand skickas per e-post till cert@ficora.fi. Om störningen i informationssäkerheten är allvarlig och/eller om registraren behöver hjälp för att utreda obehöriga ändringar, bör Kommunikationsverket också kontaktas per telefon.

Om inte all information som efterfrågas i blanketten finns till handa (se punkt 21.5 nedan) och situationen kräver noggrannare utredning, ska registraren senast inom 24 timmar lämna en preliminär anmälan som kompletteras så fort som möjligt och senast inom tre (3) dagar.

Om registraren trots utredningar inte kan lämna alla uppgifter inom tre dagar efter den preliminära anmälningen, ska den inom den fastställda tidsfristen uppge de uppgifter som finns tillhanda samt motivera varför den lämnar resten av uppgifterna efter att fristen har gått ut.

Uppgifter som lämnats in ska uppdateras vid behov och så fort som möjligt om uppgifterna ändras.

21.5 Uppgifter som anmäls

Av anmälan till myndigheten ska framgå följande uppgifter:

- Uppgifter om registraren, dvs.
  - registrarens namn
  - namn på person som lämnar närmare uppgifter om händelsen samt dennes e-postadress och telefonnummer.
- tidpunkt när händelsen inträffade och upptäcktes
  - tidpunkt när händelsen inträffade och tidpunkt när den upptäcktes ska anges separat
  - tidpunkten för upptäckten ska anges med minst en dags noggrannhet
  - när det gäller tekniska systemloggar för händelsen anges också ett exakt klockslag, en tillämplig tidszon (t.ex. "UTC+2") samt ett eventuellt klockfel och dess riktning jämfört med den officiella tiden
  - tidsstämplar för tekniska systemloggar bör anges i ett format som är kompatibelt med ISO 8601 (jfr http://www.w3.org/TR/NOTE-datetime), fastän det viktigaste är att data om upptäckter överhuvudtaget finns i förvar.
- Typ av händelse, dvs. om det är fråga om till exempel

- dataintrång eller olovlig användning (t.ex. intrång i ett program som är anslutet till Kommunikationsverkets EPP-gränssnitt)
- fel i hanteringen av kunduppgifter (t.ex. oavsiktligt läckage i kund-uppgifter)
- annan händelse, som i så fall ska beskrivas med ord.

- Föremål för händelsen och åtgärder, dvs.

  - beskrivning av systemet som utsatts för händelsen
  - observationer av händelserna
  - uppgifter om orsaken till händelsen
  - åtgärder som vidtagits eller kommer att vidtas för att eliminera eller avhjälpa följderna
  - uppgift om huruvida ytterligare skador har förhindrats.

- Uppgifter om eventuella effekter för användarna, dvs.

  - beskrivning av eventuella effekter
  - uppgifter om de domännamn som har redigerats obehörigt
  - uppgift om ifall registraren inte har kännedom om vilka obehöriga ändringar som har gjorts med registrarens koder i Kommunikations-verkets system.

6 kap. Ikraftträdandebestämmelser

Detta kapitel behandlar bestämmelserna i föreskriftens kapitel 6, dvs. bestämmelserna om ikraftträdande av föreskriften.

22 § Ikraftträdande

Föreskriften träder i kraft den 5 september 2016 och gäller tills vidare.

23 § Erhållande av upplysningar och publicering

Föreskriften har publicerats i Kommunikationsverkets föreskriftssamling och kan erhållas vid Kommunikationsverkets kundtjänst.

Därtill publiceras föreskriften samt motiverings- och tillämpningspromemorian elektroniskt på Kommunikationsverkets webbplats och i Finlands elektroniska författningssamling Finlex, www.finlex.fi, myndigheternas föreskriftssamlingar.

AVDELNING C Övriga frågor som har samband med föreskriftens ämnesområde

1 Kommunikationsverkets rekommendation om ibruktagning av DNSSec-tekniken

Kommunikationsverket rekommenderar att registrarena främjar användningen av DNSSec-tekniken vid förmedlingen av domännnamn. DNSSec (Domain Name System Security Extensions) är ett standardiserat säkerhetstillägg i domännamntjänsten (Domain Name System) på Internet. Syftet med DNSSec är att öka informationssäkerheten och tillförlitligheten i namntjänsten genom digitala signaturer som läggs till i DNS-posterna.

Med de funktioner som DNSSec erbjuder är det möjligt att verifiera DNS-uppgifternas ursprung och integritet samt att de så kallade negativa svaren är genuina. För att ovan nämnda funktioner ska kunna implementeras, definierar DNSSec nya posttyper i namntjänsten, av vilka de viktigaste är posterna RRSIG, DNSKEY, DS och NSEC(3). DNSSecs funktioner bygger på så kallade förtroendekedjor där de offentliga nycklarna i signerade zoner kan verifieras med hjälp av en offentlig nyckel i den signerade överzonen. I en idealisk situation börjar förtroendekedjorna från en signerad rotzon vars offentliga nyckel på förhand definierats som tillförlitlig. För att tillförlitligheten i namntjänsten som helhet ska kunna säkerställas, är det av största vikt att varje del av förtroendekedjan är att lita på.

DNSSec ska inte ersätta krypteringstekniken TLS (Transport Layer Security), utan DNSSec kompletterar TLS och förhindrar situationer där en användare hamnar på en fel server redan innan förbindelsen har skyddats med TLS-tekniken.

Kommunikationsverket rekommenderar att registrarerna tar i bruk DNSSec för alla domännamn som de förvaltar eller erbjuder den till alla sina kunder (domännamnsanvändare), om registraren har egna namnservrar.

Ytterligare information om DNSSec-säkerhetstillägget finns bland annat på Kommunikationsverkets webbplats på https://domain.fi.

AVDELNING D Lagstiftning

1 Rättsgrund

Kommunikationsverkets föreskrift bygger informationssamhällsbalken (917/2014). Bestämmelser om domännamn ingår främst i 21 kap. i lagen samt i följande kapitel:

- 1 kap. 3 § Definitioner, 21 och 35 punkten
- 36 kap. 295 § Domännamnsavgift
- 39 kap. 312 § Elektronisk delgivning
- 43 kap. 343 § Överklagande hos marknadsdomstolen

- 45 kap. 351 § Ikraftträdande

I 21 kap. i informationssamhällsbalken föreskrivs om Kommunikationsverkets befogenheter att meddela föreskrifter enligt följande:

Kommunikationsverket får enligt 165 § 3 mom. i informationssamhällsbalken meddela närmare föreskrifter om hur anmälan ska göras och om innehållet i den. I 1 mom. i paragrafen åläggs registrar skyldighet att göra en anmälan om inledande av registrarverksamhet. I 2 mom. åläggs registrar skyldighet att informera om ändringar i de uppgifter som anmälts, nedläggning av verksamheten och förbudsbeslut som Kommunikationsverket meddelat med stöd av 171 § 2 mom.

Kommunikationsverket får enligt 166 § 3 mom. i informationssamhällsbalken meddela föreskrifter om de konfigurationer som är nödvändiga för att domännamnet ska fungera och om domännamnets form, antal tecken och tillåtna tecken. Enligt 1 mom. i paragrafen får ett domännamn bestå av minst två och högst 63 tecken. En bestämmelse om domännamnets form finns i 2 mom.i paragrafen.

Kommunikationsverket får enligt 167 § 4 mom. i informationssamhällsbalken utfärda närmare föreskrifter om hur registreringen tekniskt ska genomföras och om de uppgifter som ska lämnas i samband med registreringen. Enligt 1 mom. i paragrafen ska registraren i domännamnsregistret anteckna korrekta och uppdaterade uppgifter som identifierar domännamnsanvändaren samt den e-postadress som ska användas för hörande och delgivning.

Kommunikationsverket får enligt 168 § 4 mom. i informationssamhällsbalken utfärda föreskrifter om det tekniska genomförandet och tidsfristerna i fråga om överföring av domännamn och byte av registrar. Enligt 1 mom. paragrafen kan domännamnsanvändaren överföra domännamnet till en annan användare under domännamnets giltighetstid. Registraren ska göra överföringen inom rimlig tid från mottagandet av begäran. Enligt 2 mom. i paragrafen kan domännamnsanvändaren byta registrar under domännamnets giltighetstid. Registraren ska vidta de åtgärder som krävs för att byta registrar inom rimlig tid från mottagandet av begäran.

Kommunikationsverket får enligt 170 § 2 mom. i informationssamhällsbalken meddela närmare föreskrifter om information som ges till användare av domännamn, om informationssäkerheten i registrarens verksamhet, om när en störning som avses i 1 mom. 7 punkten ska anses vara betydande samt om innehållet i anmälan samt anmälans utformning och hur den lämnas in. Enligt 1 mom. 1 punkten i paragrafen ska en registrar innan ett domännamn registreras tillhandahålla behövlig information enligt denna lag om kraven på domännamnets innehåll och form. Enligt 1 mom. 6 punkten i paragrafen ska en registrar sörja för informationssäkerheten i sin verksamhet. Enligt 1 mom. 7 punkten i paragrafen ska en registrar utan dröjsmål meddela Kommunikationsverket om dess förmedling av domännamn är utsatt för betydande kränkningar av eller hot mot informationssäkerheten eller för någonting annat som väsentligen förhindrar eller stör den. Enligt

punkten ska registraren också anmäla hur länge störningen eller hotet beräknas pågå, om vilka verkningar störningen eller hotet har, om avhjälpande åtgärder samt om åtgärder för att förhindra att störningen upprepas.

Referenslista

[1] Informationssamhällsbalken [917/2014], uppdaterad version: www.finlex.fi

[2] Den nationella kriteriesamlingen för säkerhetsauditering, Katakri:
1) Datakommunikationssäkerhet
2) Säkerhet i informationssystem
www.defmin.fi

[3] IETF 1035 Domain names - implementation and specification: http://www.ietf.org/rfc/rfc1035.txt

[4] IETF RFC 3492 Punycode: A Bootstring Encoding of Unicode for Internationalized Domain Names in Applications (IDNA): http://www.ietf.org/rfc/rfc3492.txt

[5] IETF RFC 3490 Internationalizing Domain Names in Applications (IDNA): http://www.ietf.org/rfc/rfc3490.txt

[6] IETF RFC 1034 Domain names - concepts and facilities: http://www.ietf.org/rfc/rfc1034.txt

[7] IETF RFC 2142 Mailbox Names for Common Services, Roles and Functions: http://www.ietf.org/rfc/rfc2142.txt

RFC-dokument om Kommunikationsverkets EPP-gränssnitt:

[8] IETF RFC 3375 - Generic Registry-Registrar Protocol Requirements: https://www.ietf.org/rfc/rfc3375.txt

[9] IETF RFC 3735 - Guidelines for Extending EPP: https://tools.ietf.org/rfc/rfc3735.txt

[10] IETF RFC 5910 - Domain Name System (DNS) Security Extensions Mapping for the Extensible Provisioning Protocol (EPP): https://tools.ietf.org/rfc/rfc5910.txt

[11] IETF RFC 5730 - Extensible Provisioning Protocol (EPP): https://tools.ietf.org/rfc/rfc5730.txt

[12] IETF RFC 5731 - Extensible Provisioning Protocol (EPP) Domain Name Mapping: https://tools.ietf.org/rfc/rfc5731.txt

[13] IETF RFC 5732 - Extensible Provisioning Protocol (EPP) Host Mapping: https://tools.ietf.org/rfc/rfc5732.txt

[14] IETF RFC 5733 - Extensible Provisioning Protocol (EPP) Contact Mapping: https://tools.ietf.org/rfc/rfc5733.txt

[15] IETF RFC 5734 - Extensible Provisioning Protocol (EPP) Transport over TCP: https://tools.ietf.org/rfc/rfc5734.txt

Övriga internetstandarder och rekommendationer som har samband med föreskriften:

[16] IETF RFC 1912 Common DNS Operational and Configuration Errors: http://www.ietf.org/rfc/rfc1912.txt

[17] IETF RFC 2181Clarifications to the DNS Specification: http://www.ietf.org/rfc/rfc2181.txt

[18] RFC 2182 Selection and Operation of Secondary DNS Servers: http://www.ietf.org/rfc/rfc2182.txt

[19] RIPE 192 Simple DNS Configuration Example. RIPE DNS Working Group: http://www.ripe.net/ripe/docs/ripe-192.html

[20] RIPE 203 Recommendations for DNS SOA Values: http://www.ripe.net/ripe/docs/ripe-203.html

Standarder och publikationer om riskhantering, som har samband med föreskriften:

[21] ISO/IEC 27005:2011, Information technology - Security techniques - Information security risk management: http://www.iso.org/iso/home.htm

[22] NIST Special Publication 800-30, Risk Management Guide for Information Technology Systems: http://www.nist.gov/

[23] Software Engineering Institute (SEI) at Carnegie Mellon University, OC¬TAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation): www.cert.org/octave/