FINLANDS FÖRFATTNINGSSAMLING

Utgiven i Helsingfors den 1 juli 2016

533/2016

Lag
om ändring av lagen om stark autentisering och elektroniska signaturer

I enlighet med riksdagens beslut

upphävs i lagen om stark autentisering och elektroniska signaturer (617/2009) 4 och 5,

ändras lagens rubrik, 1 och 2 §, rubriken för 2 kap., 6 §, 7 § 1 mom., 8 §, 9 § 1 mom., 10 §, 13 § 1 mom., 14 §, rubriken för 15 §, det inledande stycket i 15 § 1 mom., 16 §, rubriken för 17 §, 17 § 1 och 2 mom., den svenska språkdräkten i 19 § 1 mom. 8 punkten, rubriken för 20 §, 20 § 3 mom., 21, 22 och 24 §, 25 § 1—3 mom., 26 §, rubriken för 4 kap., 28—42 §, 43 § 1 mom., 44 § 1 mom., 45 § 1 mom. samt 46, 47 och 49 §,

av dem 2 och 6 § sådana de lyder delvis ändrade i lag 139/2015, 7 § 1 mom., rubriken för 17 § och 17 § 1 och 2 mom. sådana de lyder i lag 139/2015 samt 49 § sådan den lyder i lag 997/2015, och

fogas till lagen nya 7 a, 7 b, 8 a och 17 a §, en ny kapitelrubrik före 39 § och till lagen nya 42 a—42 c, 45 a och 49 a § som följer:

Lag
om stark autentisering och betrodda elektroniska tjänster

1 §

Tillämpningsområde

Denna lag innehåller bestämmelser om stark autentisering och om tillhandahållande av identifieringstjänster till tjänsteleverantörer, till allmänheten och till andra leverantörer av identifieringstjänster.

Lagen innehåller bestämmelser om tillsynen över efterlevnaden av Europaparlamentets och rådets förordning (EU) nr 910/2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG, nedan *EU:s förordning om elektronisk identifiering*, samt bestämmelser som kompletterar den förordningen. Dessutom innehåller lagen bestämmelser om bedömning av överensstämmelsen med kraven när det gäller identifieringstjänster och betrodda tjänster.

På gränsöverskridande identifieringssystem som anmäls till Europeiska kommissionen tillämpas denna lag endast om inte något annat följer av EU:s förordning om elektronisk identifiering.

Lagen tillämpas inte på tillhandahållande av tjänster avsedda för identifiering internt inom en sammanslutning. Lagen tillämpas inte heller på en sammanslutning som använder en egen metod för identifiering av egna kunder i samband med egna tjänster.

RP 74/2016
KoUB 18/2016
RSv 103/2016

Europaparlamentets och rådets förordning (EU) nr 910/2014 (32014R0910); EUT L 257, 28.8.2014, s.73

2 §

Definitioner

I denna lag avses med

1) *stark autentisering* identifiering av en person, av en juridisk person eller av en fysisk person som företräder en juridisk person och verifiering av identifikatorns autenticitet och riktighet genom tillämpning av en elektronisk metod som motsvarar tillitsnivån väsentlig enligt artikel 8.2 b i EU:s förordning om elektronisk identifiering eller tillitsnivån hög enligt artikel 8.2 c i den förordningen,

2) *identifieringsverktyg* ett sådant medel för elektronisk identifiering som avses i artikel 3.2 i EU:s förordning om elektronisk identifiering,

3) *leverantör av identifieringstjänster* en leverantör av tjänster för identifieringsförmedling eller en leverantör av identifieringsverktyg,

4) *leverantör av identifieringsverktyg* en tjänsteleverantör som tillhandahåller eller ger ut identifieringsverktyg för stark autentisering till allmänheten samt tillhandahåller sitt identifieringsverktyg till leverantörer av tjänster för identifieringsförmedling för förmedling i förtroendenätet,

5) *leverantör av tjänster för identifieringsförmedling* en tjänsteleverantör som förmedlar identifieringstransaktioner baserade på stark autentisering till en part som förlitar sig på en elektronisk identifiering,

6) *innehavare av identifieringsverktyg* en fysisk eller juridisk person som enligt avtal har fått ett identifieringsverktyg av en leverantör av identifieringstjänster,

7) *inledande identifiering* verifiering av identiteten hos den som ansöker om ett identifieringsverktyg, när verifieringen sker i samband med att verktyget skaffas,

8) *certifikat* ett intyg i elektronisk form som verifierar identiteten eller verifierar identiteten och kopplar ihop autentiseringsuppgifter för en betrodd tjänst med en användare av tjänsten och som kan användas vid stark autentisering och betrodda tjänster,

9) *certifikatutfärdare* en fysisk eller juridisk person som tillhandahåller allmänheten certifikat,

10) *förtroendenätet* de leverantörer av identifieringstjänster som har gjort en anmälan till Kommunikationsverket,

11) *organ för bedömning av överensstämmelse* ett av Kommunikationsverket godkänt organ enligt artikel 2.13 i Europaparlamentets och rådets förordning (EG) nr 765/2008 om krav för ackreditering och marknadskontroll i samband med saluföring av produkter och upphävande av förordning (EEG) nr 339/93, som är ackrediterat i enlighet med den förordningen.

Termerna elektronisk underskrift, betrodd tjänst, avancerad elektronisk underskrift, system för elektronisk identifiering och förlitande part har i denna lag samma betydelse som i artikel 3 i EU:s förordning om elektronisk identifiering.

2 kap.

Lagens tvingande natur och behandling av personuppgifter

6 §

Behandling av personuppgifter

Leverantörer av identifieringstjänster får på de grunder som anges i 8 § 1 mom. 1 och 2 punkten i personuppgiftslagen (523/1999) behandla personuppgifter som behövs när identifieringsverktyg ges ut, tjänster upprätthålls och identifieringstransaktioner genomförs. På samma grunder får certifikatutfärdare som tillhandahåller betrodda tjänster be-

handla de personuppgifter som behövs vid utfärdandet och upprätthållandet av certifikat samt inhämta personuppgifter från personen själv.

En leverantör av tjänster för identifieringsförmedling har rätt att när en sådan tjänst tillhandahålls överlåta personuppgifter till en part som förlitar sig på en elektronisk identifiering, om den förlitande parten enligt lag har rätt att behandla personuppgifter.

Personuppgifter får behandlas i andra än i 1 mom. nämnda syften endast på de grunder som anges i 8 § 1 mom. 1 punkten i personuppgiftslagen.

När leverantörer av identifieringstjänster och certifikatutfärdare som tillhandahåller betrodda tjänster kontrollerar sökandens identitet ska de kräva att sökanden uppger sin personbeteckning. Leverantörer av identifieringstjänster och certifikatutfärdare som tillhandahåller betrodda tjänster får behandla personbeteckningar i sina register i de syften som nämns i 1 mom. Identifieringsverktyg och certifikat får innehålla en personbeteckning, om verktygets eller certifikatets innehåll är tillgängligt endast för dem som nödvändigt behöver personbeteckningen för att tillhandahålla tjänsten. Personbeteckningen får inte vara tillgänglig i en offentlig katalog.

Bestämmelser om behandlingen av personuppgifter finns dessutom i 19 och 24 § och i personuppgiftslagen.

7 §

Användning av uppgifter i befolkningsdatasystemet

Leverantörer av identifieringsverktyg och certifikatutfärdare som tillhandahåller betrodda tjänster ska hämta och uppdatera de uppgifter som de behöver för tillhandahållandet av identifieringstjänster för fysiska personer med användning av befolkningsdatasystemet. Leverantörer av identifieringstjänster ska dessutom säkerställa att de uppgifter som de behöver för tillhandahållandet av identifieringstjänster är uppdaterade enligt uppgifterna i befolkningsdatasystemet.

— — — — — — — — — — — — — — — — — — —

7 a §

Användning av uppgifter i företags- och organisationsregister

Leverantörer av identifieringsverktyg och certifikatutfärdare som tillhandahåller betrodda tjänster ska hämta och uppdatera de uppgifter som de behöver för tillhandahållandet av identifieringstjänster för juridiska personer med användning av företags- och organisationsregistren. Leverantörer av identifieringstjänster ska dessutom säkerställa att de uppgifter som de behöver för tillhandahållandet av identifieringstjänster är uppdaterade enligt uppgifterna i företags- och organisationsregistren.

7 b §

Information om giltighet för pass eller identitetskort

Leverantörer av identifieringstjänster har trots sekretessbestämmelserna rätt att med hjälp av teknisk anslutning få information ur polisens informationssystem för förvaltningsärenden om giltighet för pass eller identitetskort som används vid inledande identifiering.

8 §

Krav på system för elektronisk identifiering

Ett system för elektronisk identifiering ska uppfylla följande krav:

1) identifieringsmetoden grundar sig på en identifiering enligt 17 och 17 a § så att uppgifterna om den kan kontrolleras i efterskott i enlighet med 24 §,

2) identifieringsmetoden medger entydig identifiering av innehavaren av identifieringsverktyget så att åtminstone de villkor uppfylls som gäller för tillitsnivån väsentlig enligt avsnitten 2.1.2, 2.1.3 och 2.1.4 i bilagan till kommissionens genomförandeförordning (EU) 2015/1502 om fastställande av tekniska minimispecifikationer och förfaranden för tillitsnivåer för medel för elektronisk identifiering i enlighet med artikel 8.3 i Europaparlamentets och rådets förordning (EU) nr 910/2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden, nedan *förordningen om tillitsnivåer vid elektronisk identifiering*,

3) med hjälp av identifieringsmetoden går det att säkerställa att endast innehavaren av identifieringsverktyget kan använda verktyget på ett sådant sätt att åtminstone de villkor uppfylls som gäller för tillitsnivån väsentlig enligt avsnitten 2.2.1 och 2.3 i bilagan till förordningen om tillitsnivåer vid elektronisk identifiering,

4) identifieringssystemet är säkert och tillförlitligt på ett sådant sätt att åtminstone de villkor uppfylls som gäller för tillitsnivån väsentlig enligt avsnitten 2.2.1, 2.3.1 och 2.4.6 i bilagan till förordningen om tillitsnivåer vid elektronisk identifiering, med hänsyn till de informationssäkerhetsrisker som är förknippade med den teknik som används vid tidpunkten, och de lokaler som används för tillhandahållandet av identifieringstjänsten är säkra på det sätt som anges i avsnitt 2.4.5 i bilagan till den förordningen,

5) ledningen avseende informationssäkerheten sköts på ett sådant sätt att de villkor uppfylls som anges i det inledande stycket i avsnitt 2.4 i bilagan till förordningen om tillitsnivåer vid elektronisk identifiering och åtminstone de villkor uppfylls som gäller för tillitsnivån väsentlig enligt avsnitten 2.4.3 och 2.4.7 i bilagan till den förordningen.

Bestämmelserna i 1 mom. hindrar inte att specifika tjänster tillhandahålls så att leverantören av identifieringstjänster meddelar den tjänsteleverantör som använder en identifieringstjänst den pseudonym som innehavaren av identifieringsverktyget använder eller endast ett begränsat antal personuppgifter.

8 a §

Autentiseringsfaktorer som ska användas i identifieringsmetoden

I en identifieringsmetod ska minst två av följande autentiseringsfaktorer användas:

1) en kunskapsbaserad autentiseringsfaktor som personen måste kunna visa att den har kunskap om,

2) en innehavsbaserad autentiseringsfaktor som personen måste kunna visa att den innehar,

3) en egenskapsbaserad autentiseringsfaktor som utgår från en kroppslig egenskap hos en fysisk person.

I varje identifieringsmetod ska det i enlighet med avsnitt 2.3.1 i bilagan till förordningen om tillitsnivåer vid elektronisk identifiering användas en sådan dynamisk autentisering som ändras vid varje ny autentisering mellan en person och det system som kontrollerar personens identitet.

9 §

Krav som gäller leverantörer av identifieringstjänster

Juridiska personer som fungerar som leverantörer av identifieringstjänster och fysiska personer som handlar för deras räkning samt ledamöter eller ersättare i styrelsen eller förvaltningsrådet för en sammanslutning eller stiftelse som är tjänsteleverantör, liksom dess verkställande direktör och ansvariga bolagsmän samt andra personer i motsvarande ställning ska uppfylla följande krav:

1) de ska ha uppnått myndighetsålder,

2) de får inte vara försatta i konkurs,
3) de får inte ha begränsad handlingsbehörighet.

— — — — — — — — — — — — — — — — — — — —

10 §

Skyldighet för leverantörer av identifieringstjänster att anmäla att verksamheten inleds

En leverantör av identifieringstjänster som är etablerad i Finland ska göra en skriftlig anmälan till Kommunikationsverket innan verksamheten inleds. Anmälan kan också göras av en sådan sammanslutning av leverantörer av identifieringsverktyg som administrerar en tjänst som ska betraktas som en enda identifieringstjänst.

Anmälan ska innehålla

1) tjänsteleverantörens namn,
2) tjänsteleverantörens fullständiga kontaktuppgifter,
3) uppgifter om de tjänster som tillhandahålls,
4) utredning om att kraven i 8, 8 a, 9, 13 och 14 § uppfylls med avseende på sökanden och sökandens verksamhet,
5) en inspektionsberättelse om oberoende bedömning i enlighet med 29 § utarbetad av ett organ för bedömning av överensstämmelse, något annat utomstående bedömningsorgan eller ett internt kontrollorgan,
6) övriga uppgifter som behövs för tillsynen.

Leverantören av identifieringstjänster ska utan dröjsmål skriftligen underrätta Kommunikationsverket om ändringar i de uppgifter som avses i 2 mom. Anmälan ska också göras när verksamheten avslutas eller funktionerna överförs till en annan tjänsteleverantör.

13 §

Allmänna skyldigheter för leverantörer av identifieringstjänster

Hos leverantörer av identifieringstjänster ska lagringen av uppgifter som sammanhänger med identifieringen, personalen och de tjänster som köps av underleverantörer uppfylla åtminstone kraven för tillitsnivån väsentlig enligt avsnitten 2.4.4 och 2.4.5 i bilagan till förordningen om tillitsnivåer vid elektronisk identifiering. Leverantörer av identifieringstjänster ska dessutom ha en omfattande plan för identifieringstjänstens upphörande.

— — — — — — — — — — — — — — — — — — — —

14 §

Principer för identifiering

Leverantörer av identifieringstjänster ska ha principer för identifiering som närmare anger hur tjänsteleverantören uppfyller de skyldigheter som anges i denna lag. Det ska i synnerhet anges närmare hur leverantören av identifieringsverktyg genomför den identifiering som avses i 17 och 17 a § när identifieringsverktyg beviljas.

Principerna för identifiering ska dessutom innehålla de viktigaste uppgifterna om

1) tjänsteleverantören,
2) de tjänster som tillhandahålls och priserna på dem,
3) samtliga villkor som tillämpas,
4) de principer för informationssäkerhet som tillämpas i tjänsten,
5) tjänsteleverantörens viktigaste samarbetspartner,
6) bedömningen av överensstämmelse enligt 29 §,
7) andra omständigheter som är av betydelse för att tjänsteleverantörens verksamhet och tillförlitlighet ska kunna bedömas.

Om elektroniska underskrifter eller avancerade elektroniska underskrifter kan skapas med ett identifieringsverktyg ska leverantören av identifieringstjänster också lämna uppgifter om hur och på vilken nivå de elektroniska underskrifterna tillhandahålls samt om säkerhetsfaktorerna i fråga om underskrifterna.

Leverantören av identifieringstjänster ska hålla principerna för identifiering allmänt tillgängliga och uppdaterade.

15 §

Skyldighet för leverantörer av identifieringsverktyg att lämna uppgifter innan avtal ingås

En leverantör av identifieringsverktyg ska innan ett avtal ingås informera den som ansöker om ett identifieringsverktyg om

— — — — — — — — — — — — — — — — — — —

16 §

Skyldighet för leverantörer av identifieringstjänster att anmäla hot och störningar som riktas mot verksamheten eller skyddet av uppgifter

En leverantör av identifieringstjänster ska trots sekretessbestämmelserna utan ogrundat dröjsmål anmäla betydande hot och störningar som riktas mot tjänsternas funktion, informationssäkerheten eller användningen av en elektronisk identitet till de tjänsternas förlitande parter, till innehavarna av identifieringsverktyg, till övriga avtalsparter i förtroendenätet och till Kommunikationsverket. Kommunikationsverket får för anmälarens räkning på teknisk väg förmedla uppgifterna mellan parterna i förtroendenätet trots vad som föreskrivs i lagen om offentlighet i myndigheternas verksamhet (621/1999).

Om hotet eller störningen är riktat mot skydd av uppgifter som avses i 32 § i personuppgiftslagen, ska leverantören av identifieringstjänster även underrätta dataombudsmannen om saken.

I en anmälan enligt 1 mom. ska det redogöras för de åtgärder som olika aktörer har tillgång till för att avvärja hot eller störningar samt de beräknade kostnaderna för åtgärderna.

En leverantör av identifieringstjänster får använda sådana uppgifter om en annan leverantör av identifieringstjänster som den fått med stöd av denna paragraf endast för att skapa beredskap för de hot och störningar som avses i denna paragraf samt för att utreda störningssituationer. Hos en leverantör av identifieringstjänster får uppgifterna behandlas endast av den personal som nödvändigt behöver uppgifterna i sitt arbete. Uppgifterna ska också annars behandlas så att affärshemligheter som tillhör en annan leverantör av identifieringstjänster inte röjs.

En leverantör av identifieringstjänster som genom att handla i strid med 4 mom. vållar en annan leverantör av identifieringstjänster skada är skyldig att ersätta skadan.

17 §

Identifiering av en fysisk person som ansöker om ett identifieringsverktyg

Vid inledande identifiering ska identifieringen av en fysisk person göras personligen eller elektroniskt på ett sådant sätt att de krav uppfylls som gäller för tillitsnivån väsentlig eller hög enligt avsnitt 2.1.2 i bilagan till förordningen om tillitsnivåer vid elektronisk identifiering. Kontrollen av en persons identitet kan grunda sig på en identitetshandling som utfärdats av en myndighet eller ett sådant identifieringsverktyg för stark autentisering som avses i denna lag. Kontrollen av identiteten kan dessutom grunda sig på ett förfarande som en offentlig eller privat aktör tidigare och i annat syfte än för beviljande av ett identifieringsverktyg för stark autentisering har använt sig av och som Kommunikationsverket godkänner utifrån de bestämmelser som gäller förfarandet och utifrån myndighetstillsy-

nen eller utifrån en bekräftelse av ett i 28 § 1 punkten avsett organ för bedömning av överensstämmelse.

Dokument som godkänns vid inledande identifiering, när identifieringen endast sker utifrån en identitetshandling som utfärdats av en myndighet, är ett giltigt pass eller identitetskort som har utfärdats av en myndighet i en medlemsstat inom Europeiska ekonomiska samarbetsområdet, i Schweiz eller i San Marino. En leverantör av identifieringsverktyg som så önskar kan också vid kontrollen av identiteten använda ett giltigt pass som har utfärdats av en myndighet i någon annan stat.

— — — — — — — — — — — — — — — — — — —

17 a §

Identifiering av en juridisk person som ansöker om ett identifieringsverktyg

Den identitet som uppgetts av en juridisk person ska kontrolleras med användning av företags- och organisationsregistren eller på ett sådant sätt att åtminstone de krav på styrkande och kontroll av juridiska personers identitet uppfylls som gäller för tillitsnivån väsentlig enligt avsnitt 2.1.3 i bilagan till förordningen om tillitsnivåer vid elektronisk identifiering.

19 §

Certifikatets innehåll

Om identifieringsmetoden grundar sig på ett certifikat, ska certifikatet åtminstone innehålla

— — — — — — — — — — — — — — — — — — —

8) certifikatutfärdarens avancerade elektroniska underskrift.

— — — — — — — — — — — — — — — — — — —

20 §

Beviljande av identifieringsverktyg

— — — — — — — — — — — — — — — — — — —

Identifieringsverktyg beviljas endast fysiska och juridiska personer. Bindningen mellan en fysisk persons och en juridisk persons identifieringsverktyg ska genomföras i enlighet med avsnitt 2.1.4 i bilagan till förordningen om tillitsnivåer vid elektronisk identifiering. Ett identifieringsverktyg ska vara personligt. Till ett identifieringsverktyg kan det vid behov fogas en uppgift om att innehavaren av identifieringsverktyget i enskilda fall även får företräda en annan fysisk person eller en juridisk person.

21 §

Överlåtelse av identifieringsverktyg till sökande

Leverantören av ett identifieringsverktyg ska överlåta identifieringsverktyget till sökanden på det sätt som anges i avtalet. Leverantören ska säkerställa att verktyget inte obehörigt kommer i någon annans besittning vid överlåtelsen, på ett sådant sätt att åtminstone de krav uppfylls som gäller för tillitsnivån väsentlig enligt avsnitt 2.2.2 i bilagan till förordningen om tillitsnivåer vid elektronisk identifiering.

22 §

Förnyande av identifieringsverktyg

En leverantör av identifieringsverktyg får leverera ett nytt verktyg till en innehavare av identifieringsverktyg utan en uttrycklig begäran endast om ett verktyg som tidigare har tillhandahållits ska ersättas med ett nytt. När identifieringsverktyg förnyas ska de krav uppfyllas som gäller för tillitsnivån väsentlig enligt avsnitt 2.2.4 i bilagan till förordningen om tillitsnivåer vid elektronisk identifiering.

24 §

Registrering och användning av uppgifter om identifieringstransaktioner och identifieringsverktyg

Leverantörer av identifieringstjänster ska registrera

1) de uppgifter som behövs för att verifiera en enskild identifieringstransaktion eller elektronisk underskrift,

2) uppgifter om i 18 § avsedda hinder och begränsningar som gäller användningen av identifieringsverktyg,

3) i fråga om certifikat, uppgifter om certifikatets innehållet i certifikat enligt 19 §.

Leverantörer av identifieringsverktyg ska registrera behövliga uppgifter om den inledande identifiering av sökande som avses i 17 och 17 a § och om de handlingar eller den elektroniska identifiering som använts i den inledande identifieringen.

De uppgifter som avses i 1 mom. 1 punkten ska lagras i fem år från identifieringstransaktionen. De övriga uppgifter som avses i 1 och 2 mom. ska lagras i fem år från det att ett fast kundförhållande har upphört.

Personuppgifter som har uppkommit i samband med en identifieringstransaktion ska förstöras efter transaktionen, om det inte är nödvändigt att registrera dem för att verifiera en enskild identifieringstransaktion.

Leverantören av identifieringstjänster får behandla registrerade uppgifter endast för att tillhandahålla och upprätthålla tjänsterna, fakturera, trygga sina rättigheter vid tvister och utreda missbruk samt på begäran av en tjänsteleverantör som använder identifieringstjänster eller en innehavare av ett identifieringsverktyg. Leverantören av identifieringstjänster ska registrera uppgifter om när och varför uppgifterna behandlats och vem som gjort det.

Om en tjänsteleverantör endast ger ut identifieringsverktyg

1) tillämpas inte 1 mom. 1 punkten och 4 mom. på tjänsteleveratören,

2) räknas den registreringstid på fem år som avses i 3 mom. från det att identifieringsverktyget upphörde att gälla.

25 §

Anmälan om återkallande eller förhindrande av användning av identifieringsverktyg

Innehavaren av ett identifieringsverktyg ska göra en anmälan till leverantören av identifieringsverktyget, eller någon annan aktör som denne har utsett, om verktyget har förkommit, obehörigen har kommit i någon annans besittning eller obehörigen har använts. Anmälan ska göras utan obefogat dröjsmål efter det att saken har upptäckts.

Leverantören av identifieringsverktyg ska se till att det är möjligt att när som helst göra en anmälan enligt 1 mom. Leverantören ska utan dröjsmål återkalla identifieringsverktyget eller förhindra dess användning efter det att anmälan har mottagits.

Leverantören av ett identifieringsverktyg ska på lämpligt sätt och utan dröjsmål i systemet registrera uppgifter om tidpunkten för återkallandet eller förhindrandet av användningen. Innehavaren av identifieringsverktyget har rätt att på begäran få ett intyg över att

innehavaren har gjort den anmälan som avses i 1 mom. Intyget ska begäras inom 18 månader från anmälan.

— — — — — — — — — — — — — — — — — — —

26 §

Rätten för leverantörer av identifieringsverktyg att återkalla eller förhindra användning av identifieringsverktyg

Utöver vad som föreskrivs i 25 § får leverantören av ett identifieringsverktyg återkalla eller förhindra användningen av identifieringsverktyget, om

1) leverantören har skäl att misstänka att identifieringsverktyget används av någon annan än den som det har beviljats till,

2) identifieringsverktyget innehåller ett uppenbart fel,

3) leverantören har skäl att misstänka att säkerheten vid användningen av identifieringsverktyget har äventyrats,

4) innehavaren av identifieringsverktyget använder det på ett sätt som väsentligt strider mot avtalsvillkoren,

5) innehavaren av identifieringsverktyget har avlidit.

Leverantören av identifieringsverktyget ska så snart som möjligt underrätta innehavaren av identifieringsverktyget om att identifieringsverktyget har återkallats eller användningen av det förhindrats samt om tidpunkten för och orsakerna till detta.

Leverantören av identifieringsverktyget ska erbjuda en ny möjlighet att använda identifieringsverktyget eller tillhandahålla innehavaren ett nytt verktyg omedelbart efter det att en sådan orsak som avses 1 mom. 2 eller 3 punkten inte längre föreligger.

4 kap.

Bedömning av överensstämmelse

28 §

Organ för bedömning av överensstämmelse

Överensstämmelsen hos en tjänst enligt detta kapitel kan bedömas av följande bedömningsorgan så som föreskrivs nedan:

1) ett organ för bedömning av överensstämmelse,

2) ett annat utomstående bedömningsorgan som är verksamt enligt en allmänt använd metod (*annat utomstående bedömningsorgan*), eller

3) ett oberoende bedömningsorgan inom tjänsteleverantörens organisation som uppfyller en allmänt använd standard (*internt kontrollorgan*).

29 §

Bedömning av överensstämmelse hos en elektronisk identifieringstjänst

En leverantör av identifieringstjänster ska regelbundet låta ett sådant bedömningsorgan som nämns i 28 § bedöma om identifieringstjänsten uppfyller kraven på interoperabilitet, informationssäkerhet, dataskydd och annan tillförlitlighet enligt denna lag.

Bestämmelser om bedömning av överensstämmelse hos system för elektronisk identifiering som ska anmälas till Europeiska kommissionen finns i EU:s förordning om elektronisk identifiering och i förordningen om tillitsnivåer vid elektronisk identifiering.

Bestämmelser om Kommunikationsverkets rätt att meddela närmare föreskrifter om bedömningsgrunderna vid bedömningen av överensstämmelsen hos en identifieringstjänst finns i 42 §. Som bedömningsgrund kan Kommunikationsverket utöver de författningar

och rättsakter som avses i 1 och 2 mom. fastställa bestämmelser eller riktlinjer som antagits av Europeiska unionen eller något annat internationellt organ, publicerade och generellt eller regionalt tillämpade anvisningar för informationssäkerhet samt datasäkerhetsstandarder eller förfaranden som används allmänt.

30 §

Bedömning av överensstämmelse hos den nationella noden för elektronisk identifiering

Överensstämmelse hos det nationella gränssnitt som hör till EU:s interoperabilitetsramverk för elektronisk identifiering (*den nationella noden*) ska påvisas genom en bedömning som görs av ett organ för bedömning av överensstämmelse eller ett annat utomstående bedömningsorgan.

Bestämmelser om kraven på den nationella noden finns i kommissionens genomförandeförordning (EU) 2015/1501 om interoperabilitetsramverket enligt artikel 12.8 i Europaparlamentets och rådets förordning (EU) nr 910/2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden. Bestämmelser om Kommunikationsverkets rätt att meddela närmare föreskrifter om bedömningsgrunderna vid bedömningen av överensstämmelse hos den nationella noden finns i 42 §.

31 §

Inspektionsberättelse

En leverantör av identifieringstjänster och Befolkningsregistercentralen ska över bedömningen av överensstämmelse låta utarbeta en inspektionsberättelse som lämnas in till Kommunikationsverket.

Inspektionsberättelsen är i kraft den tid som anges i den standard som användes vid bedömningen, dock högst i 2 år.

32 §

Fastställande av överensstämmelse hos betrodda tjänster

Ett organ för bedömning av överensstämmelse ska inspektera en kvalificerad tillhandahållare av betrodda tjänster och överensstämmelsen hos en kvalificerad betrodd tjänst med iakttagande av bestämmelserna i EU:s förordning om elektronisk identifiering.

Bestämmelser om Kommunikationsverkets rätt att meddela närmare föreskrifter om bedömningsgrunderna vid bedömningen av överensstämmelse finns i 42 §. Som bedömningsgrund kan Kommunikationsverket fastställa bestämmelser eller riktlinjer som antagits av Europeiska unionen eller något annat internationellt organ, publicerade och generellt eller regionalt tillämpade anvisningar för informationssäkerhet samt datasäkerhetsstandarder eller förfaranden som används allmänt.

33 §

Allmänna krav på bedömningsorgan

De bedömningsorgan som nämns i 28 § omfattas av följande kompetenskrav:

1) organet ska vara funktionellt och ekonomiskt oberoende av bedömningsobjektet,

2) organets personal ska ha god teknisk och yrkesinriktad utbildning samt tillräckligt omfattande erfarenhet av de uppgifter som ingår i bedömningsverksamheten,

3) organet ska förfoga över den utrustning och de lokaler, redskap och system som behövs för bedömningsverksamheten,

4) organet ska ha ändamålsenliga riktlinjer för verksamheten och uppföljningen av den.

Bestämmelser om Kommunikationsverkets rätt att meddela närmare föreskrifter om de krav som anges i 1 mom. finns i 42 §.

Ett organ för bedömning av överensstämmelse ska visa att kraven i 1 mom. 1—3 punkten är uppfyllda genom en ackreditering beviljad av den nationella ackrediteringsenheten med iakttagande av bestämmelserna i Europaparlamentets och rådets förordning (EG) nr 765/2008 om krav för ackreditering och marknadskontroll i samband med saluföring av produkter och upphävande av förordning (EEG) nr 339/93 och i lagen om konstaterande av tillförlitligheten hos tjänster för bedömning av överensstämmelse med kraven (920/2005).

En leverantör av identifieringstjänster ska i den anmälan som avses i 10 § lämna en redogörelse för att ett annat utomstående bedömningsorgan eller ett internt kontrollorgan som bedömt dess överensstämmelse uppfyller kraven enligt 1 mom. Att kraven i 1 mom. 1—3 punkten är uppfyllda ska visas genom en ackreditering enligt 3 mom. eller genom ett annat oberoende förfarande som grundar sig på en allmänt använd standard.

En ackreditering som beviljas av en utländsk ackrediteringsenhet motsvarar ett ackrediteringsbeslut enligt 3 och 4 mom.

34 §

Godkännande av organ för bedömning av överensstämmelse

Organ för bedömning av överensstämmelse godkänns av Kommunikationsverket. Ett organ kan godkännas för viss tid, om det finns särskilda skäl till detta. Kommunikationsverket kan förena ett beslut om godkännande med begränsningar och villkor rörande organets kompetensområde, tillsynen över organet och organets verksamhet.

35 §

Ansökan om att bli organ för bedömning av överensstämmelse

Organ för bedömning av överensstämmelse godkänns efter ansökan. Ansökan ska innehålla sådana uppgifter om sökanden och sökandens verksamhet utifrån vilka det kan avgöras om kraven i 33 § är uppfyllda.

När Kommunikationsverket behandlar en ansökan kan verket skaffa utlåtanden samt anlita utomstående experter för att bedöma ansökan och de uppgifter som ges i ansökan.

36 §

Certifiering av anordningar för skapande av kvalificerade elektroniska underskrifter eller kvalificerade elektroniska stämplar

Kommunikationsverket får efter ansökan utse offentliga eller privata certifieringsorgan enligt artiklarna 30 och 39.2 i EU:s förordning om elektronisk identifiering som har i uppgift att certifiera anordningar för skapande av kvalificerade elektroniska underskrifter eller kvalificerade elektroniska stämplar. Certifieringsorganet kan utses för viss tid. I sin ansökan ska certifieringsorganet ange de uppgifter som Kommunikationsverket begär och som behövs för behandlingen av ansökan.

Certifieringsorganet ska vara funktionellt och ekonomiskt oberoende av tillverkarna av anordningar för skapande av elektroniska underskrifter eller elektroniska stämplar. Organet ska ha en ansvarsförsäkring som är tillräcklig med hänsyn till verksamhetens omfattning, eller något annat motsvarande arrangemang, och det ska ha tillgång till en tillräckligt stor yrkeskunnig personal och de system, den utrustning och de redskap som behövs för verksamheten.

37 §

Verksamheten vid organ för bedömning av överensstämmelse och certifieringsorgan

Ett organ för bedömning av överensstämmelse och ett certifieringsorgan får i sitt uppdrag anlita personer som inte hör till organisationen. Organen ansvarar också för det arbete som utförts av personer de anlitat.

Organ för bedömning av överensstämmelse och certifieringsorgan ska följa bestämmelserna i förvaltningslagen (434/2003), lagen om offentlighet i myndigheternas verksamhet, lagen om elektronisk kommunikation i myndigheternas verksamhet (13/2003), språklagen (423/2003) och samiska språklagen (1086/2003) när de utför offentliga förvaltningsuppgifter som avses i denna lag. På personalen vid organ för bedömning av överensstämmelse och vid certifieringsorgan och vid dotterbolag och underentreprenörer som anlitas av sådana organ tillämpas bestämmelserna om straffrättsligt tjänsteansvar när den sköter uppgifter som avses i denna paragraf. Bestämmelser om skadeståndsansvar finns i skadeståndslagen (412/1974).

Organ för bedömning av överensstämmelse och certifieringsorgan ska underrätta Kommunikationsverket om varje ändring som har betydelse för uppfyllandet av villkoren för att godkännas eller utses.

38 §

Återkallande av godkännande som organ för bedömning av överensstämmelse eller utseende till certifieringsorgan

Om Kommunikationsverket konstaterar att ett organ för bedömning av överensstämmelse eller ett certifieringsorgan inte uppfyller föreskrivna villkor eller att organet i väsentlig grad handlar i strid med gällande bestämmelser, ska Kommunikationsverket sätta ut en tillräcklig tidsfrist inom vilken saken ska rättas till.

Kommunikationsverket kan återkalla ett beslut att godkänna ett bedömningsorgan eller utse ett certifieringsorgan om organet inte har korrigerat sin verksamhet inom den tid som satts ut enligt 1 mom. och det är fråga om en väsentlig förseelse eller försummelse.

4 a kap.

Betrodda tjänster

39 §

Återkallande av certifikat

En undertecknare eller en innehavare av en elektronisk stämpel ska utan dröjsmål begära att den certifikatutfärdare som har utfärdat ett kvalificerat certifikat ska återkalla det, om undertecknaren eller innehavaren har grundad anledning att misstänka att framställningsdata för undertecknings eller den elektroniska stämpeln används på obehörigt sätt.

En certifikatutfärdare som tillhandahåller kvalificerade certifikat ska utan dröjsmål återkalla ett kvalificerat certifikat, om undertecknaren eller innehavaren av den elektroniska stämpeln begär det. En begäran om återkallande av ett certifikat anses ha kommit in till certifikatutfärdaren när den har stått till utfärdarens förfogande så att begäran har kunnat behandlas.

40 §

Ansvar för obehörig användning av framställningsdata för en underteckning eller elektronisk stämpel

En undertecknare och en innehavare av en elektronisk stämpel ansvarar för skada som orsakats av obehörig användning av framställningsdata för en avancerad elektronisk underskrift eller elektronisk stämpel som är baserad på ett kvalificerat certifikat tills en begäran om återkallande av certifikatet har kommit in till certifikatutfärdaren så som anges i 39 § 2 mom.

En konsument har dock ansvar enligt 1 mom. endast om

1) konsumenten har överlåtit framställningsdata till någon annan,

2) någon som är obehörig att använda framställningsdata kommit åt dem på grund av att konsumenten varit vårdslös på ett sätt som inte är lindrigt, eller

3) konsumenten på annat sätt än det som nämns i 2 punkten har förlorat besittningen till framställningsdata och därefter har underlåtit att begära att det certifikatet ska återkallas så som anges i 39 § 1 mom.

41 §

Det ansvar som vilar på tillhandahållare av betrodda tjänster

Bestämmelser om det ansvar som vilar på tillhandahållare av betrodda tjänster finns i artikel 13 i EU:s förordning om elektronisk identifiering.

Den certifikatutfärdare som tillhandahållit ett kvalificerat certifikat är ansvarig för skada som den som förlitat sig på det kvalificerade certifikatet orsakats genom att certifikatutfärdaren eller en person som denne anlitat inte har återkallat certifikatet på det sätt som anges i 39 §. Certifikatutfärdaren är fri från ansvar, om den visar att skadan inte har berott på oaktsamhet hos certifikatutfärdaren eller en person som denne anlitat.

42 §

Allmän styrning och Kommunikationsverkets föreskrifter

Kommunikationsministeriet svarar för den allmänna styrningen och utvecklingen av stark autentisering och betrodda tjänster.

Kommunikationsverket får meddela närmare föreskrifter om

1) kraven enligt 8 § 1 mom. 4 och 5 punkten på säkerhet och tillförlitlighet hos identifieringssystemet,

2) innehållet i de uppgifter som ska anmälas enligt 10 § och inlämnandet av dem till Kommunikationsverket,

3) egenskaperna enligt 12 a § 2 mom. hos förtroendenätets gränssnitt,

4) när störningar som avses i 16 § är betydande och om innehållet i anmälningar enligt 16 § 1 mom. samt anmälningarnas form och inlämnandet av dem,

5) grunderna för bedömningen enligt 29, 30 och 32 § av överensstämmelsen hos en identifieringstjänst, en betrodd tjänst och den nationella noden,

6) kompetenskraven enligt 33 § för organ för bedömning av överensstämmelse med beaktande av vad som föreskrivs i EU:s förordning om elektronisk identifiering,

7) de uppgifter som ska ingå i en ansökan enligt 35 § och inlämnandet av dem till Kommunikationsverket,

8) de krav som ställs på certifieringsorgan som avses i 36 §, förfarandet vid certifiering och kraven på anordningar för skapande av elektroniska underskrifter och elektroniska stämplar med beaktande av vad som föreskrivs i EU:s förordning om elektronisk identifiering.

42 a §

Kommunikationsverkets uppgifter

Kommunikationsverket ska utöva tillsyn över efterlevnaden av denna lag, om inte något annat föreskrivs i denna lag.

Kommunikationsverket ska i enlighet med EU:s förordning om elektronisk identifiering

1) delta i samarbetet mellan Europeiska unionens medlemsstater i det interoperabilitetsramverk för elektronisk identifiering som avses i artikel 12 i förordningen och i det samarbetsnätverk som upprättats för detta ändamål,

2) anmäla system för elektronisk identifiering till Europeiska kommissionen i enlighet med artiklarna 7—10 i förordningen,

3) vara tillsynsorgan enligt artikel 17 i förordningen och sköta tillsynsorganets uppgifter enligt förordningen,

4) i enlighet med artikel 22 i förordningen föra och publicera förteckningar över kvalificerade tillhandahållare av betrodda tjänster i Finland och över de kvalificerade betrodda tjänster som dessa tillhandahåller.

Kommunikationsverkets beslutanderätt omfattar inte avtalsförhållanden mellan parter eller frågor om ersättningsskyldighet.

42 b §

Dataombudsmannens uppgifter

Dataombudsmannen ska övervaka att bestämmelserna om personuppgifter i denna lag iakttas.

42 c §

Befolkningsregistercentralens uppgifter

Befolkningsregistercentralen ska upprätthålla den nationella nod som avses i 30 §.

43 §

Rätt till information

När Kommunikationsverket fullgör sina uppgifter enligt denna lag har verket trots sekretessbestämmelserna rätt att få den information som behövs för skötseln av uppgifterna av dem vars rättigheter och skyldigheter denna lag gäller och av dem som handlar för dessas räkning.

— — — — — — — — — — — — — — — — — — — —

44 §

Myndighetssamarbete och rätt att lämna information

Utöver vad som föreskrivs i lagen om offentlighet i myndigheternas verksamhet har Kommunikationsverket och dataombudsmannen trots sekretessbestämmelserna och andra begränsningar som gäller utlämnande av uppgifter rätt att lämna Finansinspektionen och Konkurrens- och konsumentverket den information som de behöver för skötseln av sina uppgifter. Finansinspektionen och Konkurrens- och konsumentverket har motsvarande rätt att trots sekretessbestämmelserna lämna Kommunikationsverket och dataombudsmannen de uppgifter som behövs för skötseln av deras uppgifter enligt denna lag.

— — — — — — — — — — — — — — — — — — — —

45 §

Administrativa tvångsmedel

Kommunikationsverket kan ge en anmärkning till den som bryter mot denna lag eller bestämmelser som utfärdats eller föreskrifter eller beslut som har meddelats med stöd av den, eller mot EU:s förordning om elektronisk identifiering eller bestämmelser som har utfärdats med stöd av den, samt ålägga denne att avhjälpa felet eller försummelsen inom skälig tid. Beslutet kan förenas med vite eller med hot om att verksamheten kommer att avbrytas helt eller delvis eller att den försummade åtgärden kommer att vidtas på den försumliges bekostnad. Bestämmelser om vite, hot om avbrytande och hot om tvångsutförande finns i viteslagen (1113/1990).

— — — — — — — — — — — — — — — — — — —

45 a §

Interimistiska beslut

Om ett fel eller en försummelse som gäller EU:s förordning om elektronisk identifiering, denna lag eller bestämmelser som utfärdats eller föreskrifter som meddelats med stöd av dem, eller en störning i datasäkerheten, omedelbart och i väsentlig grad äventyrar tillförlitligheten hos en identifieringstjänst eller betrodd tjänst, får Kommunikationsverket omgående besluta om behövliga interimistiska åtgärder oberoende av den tidsfrist som avses i 45 §.

Kommunikationsverket ska innan det beslutar om interimistiska åtgärder ge den som är föremål för beslutet tillfälle att bli hörd, utom när detta inte kan ordnas så snabbt som ärendets brådskande natur nödvändigtvis kräver.

Som interimistisk åtgärd kan Kommunikationsverket förbjuda eller avbryta

1) tillhandahållandet av en identifieringsmetod som stark autentisering,

2) tillhandahållandet av en sådan kvalificerad betrodd tjänst som avses i artikel 3.17 i EU:s förordning om elektronisk identifiering,

3) tillhandahållandet av ett system för elektronisk identifiering som anmälts enligt artikel 9.1 i EU:s förordning om elektronisk identifiering,

4) tillhandahållandet av autentisering enligt artikel 7 f i EU:s förordning om elektronisk identifiering.

De interimistiska åtgärderna kan vara i kraft i högst tre månader. Beslut om interimistiska åtgärder får överklagas separat, på samma sätt som beslut som avses i 45 § 1 mom.

46 §

Inspektionsrätt

Kommunikationsverket har rätt att utföra inspektioner av leverantörer av identifieringstjänster och av leverantörernas tjänster, av organ för bedömning av överensstämmelse som avses i 28 §, av certifieringsorgan enligt 36 § för anordningar för skapande av kvalificerade elektroniska underskrifter och elektroniska stämplar och dessa organs verksamhet, av certifikatutfärdare som tillhandahåller kvalificerade certifikat samt av tillhandahållare av betrodda tjänster och deras tjänster. En inspektion kan genomföras för att övervaka fullgörandet av skyldigheter enligt denna lag och EU:s förordning om elektronisk identifiering samt bestämmelser som utfärdats och föreskrifter och beslut som har meddelats med stöd av dem. Bestämmelser om inspektioner finns i 39 § i förvaltningslagen.

Kommunikationsverket förordnar en inspektör att utföra de inspektioner som avses i 1 mom. Den som utför inspektionen har rätt att hos en leverantör av identifieringstjänster, hos en certifikatutfärdare som tillhandahåller kvalificerade certifikat och hos en tillhanda-

hållare av betrodda tjänster samt hos personer som dessa anlitar granska sådan maskinvara och programvara som kan vara av betydelse vid tillsynen över efterlevnaden av denna lag och de bestämmelser som utfärdats och de föreskrifter som meddelats med stöd av den.

Leverantörer av identifieringstjänster, certifikatutfärdare som tillhandahåller kvalificerade certifikat, tillhandahållare av betrodda tjänster och de personer som dessa anlitar ska för inspektionen ge en inspektör som avses i 2 mom. tillträde till alla andra utrymmen än sådana som används för boende av permanent natur.

Dataombudsmannen har vid fullgörandet av sina uppgifter den rätt att utföra inspektioner som anges i personuppgiftslagen.

47 §

Avgifter till Kommunikationsverket

En leverantör av identifieringstjänster och en sammanslutning av tjänsteleverantörer som har gjort en anmälan enligt 10 § ska betala Kommunikationsverket en registreringsavgift på 5 000 euro. Leverantören av identifieringstjänster och sammanslutningen ska dessutom betala Kommunikationsverket en årlig tillsynsavgift på 14 000 euro.

En kvalificerad tillhandahållare av betrodda tjänster som gjort en anmälan enligt artikel 21 i EU:s förordning om elektronisk identifiering och en certifikatutfärdare som tillhandahåller kvalificerade betrodda tjänster ska betala Kommunikationsverket en registreringsavgift på 5 000 euro för varje betrodd tjänst de tillhandahåller. Dessutom ska de betala Kommunikationsverket en årlig tillsynsavgift på 14 00 euro för den första kvalificerade betrodda tjänst som de tillhandahåller och en årlig tillsynsavgift på 9 000 euro för varje därpå följande kvalificerade betrodda tjänst som de tillhandahåller. Om en certifikatutfärdare som tillhandahåller betrodda tjänster även gör en anmälan enligt 10 §, ska certifikatutfärdaren dessutom betala den registreringsavgift som anges i 1 mom.

Ett organ för bedömning av överensstämmelse som godkänts enligt 34 § ska betala Kommunikationsverket en utnämningsavgift på 10 000 euro. Dessutom ska organet betala Kommunikationsverket en årlig tillsynsavgift på 15 000 euro.

Ett certifieringsorgan som utsetts enligt 36 § ska betala Kommunikationsverket en utnämningsavgift på 10 000 euro. Dessutom ska organet betala Kommunikationsverket en årlig tillsynsavgift på 15 000 euro.

Registreringsavgiften, utnämningsavgiften och tillsynsavgiften täcker Kommunikationsverkets kostnader för att utföra uppgifterna enligt denna lag, med undantag för de uppgifter som avses i 46 § 1 mom. Tillsynsavgiften ska betalas till fullt belopp också under det första verksamhetsåret, även om verksamheten inleds under året. Tillsynsavgiften återbetalas inte, även om tjänsteleverantören upphör med sin verksamhet under året.

Registreringsavgiften, utnämningsavgiften och tillsynsavgiften påförs av Kommunikationsverket och avgifterna är direkt utsökbara. I Kommunikationsverkets beslut om påförande av avgift får ändring sökas i enlighet med 49 § 1 mom. Närmare bestämmelser om verkställigheten av avgifterna får utfärdas genom förordning av kommunikationsministeriet.

Bestämmelser om indrivning av registreringsavgiften, utnämningsavgiften och tillsynsavgiften finns i lagen om verkställighet av skatter och avgifter. Om avgifterna inte betalas senast på förfallodagen, tas årlig dröjsmålsränta ut på det obetalda beloppet enligt den räntesats som avses i 4 § i räntelagen (633/1982). I stället för dröjsmålsränta kan myndigheten ta ut en dröjsmålsavgift på fem euro om dröjsmålsräntan är mindre än detta belopp.

För en inspektion som avses i 46 § 1 mom. tas kostnaderna för inspektionen ut av föremålet för inspektionen med iakttagande av lagen om grunderna för avgifter till staten.

6 kap.

Särskilda bestämmelser

49 §

Sökande av ändring i myndighetsbeslut

Omprövning av ett beslut som fattats av Kommunikationsverket om en avgift som ska betalas till Kommunikationsverket enligt 47 § får begäras på det sätt som anges i 7 a kap. i förvaltningslagen.

Beslut som Kommunikationsverket fattat med anledning av en begäran om omprövning samt andra beslut av Kommunikationsverket än sådana som avses i 1 mom. får överklagas genom besvär hos förvaltningsdomstolen på det sätt som anges i förvaltningsprocesslagen (586/1996).

Förvaltningsdomstolens beslut i ett ärende som gäller återkallande av ett beslut om att godkänna ett organ för bedömning av överensstämmelse eller om att utse ett certifieringsorgan får överklagas genom besvär på det sätt som anges i förvaltningsprocesslagen. Över andra beslut av förvaltningsdomstolen får besvär anföras endast om högsta förvaltningsdomstolen beviljar besvärstillstånd.

Kommunikationsverket får i sina beslut bestämma att beslutet ska iakttas innan det har vunnit laga kraft. Besvärsmyndigheten kan dock förbjuda verkställigheten av beslutet tills besvären har avgjorts.

Bestämmelser om sökande av ändring i ett beslut av dataombudsmannen finns i personuppgiftslagen.

49 a §

Sökande av ändring i beslut av organ för bedömning av överensstämmelse och beslut av certifieringsorgan

Omprövning av ett beslut som fattats av ett organ för bedömning av överensstämmelse eller av ett certifieringsorgan med stöd av denna lag får begäras hos Kommunikationsverket på det sätt som anges i 7 a kap. i förvaltningslagen.

Beslut som fattats med anledning av en begäran om omprövning får överklagas genom besvär hos förvaltningsdomstolen på det sätt som anges förvaltningsprocesslagen. Över förvaltningsdomstolens beslut får besvär anföras endast om högsta förvaltningsdomstolen beviljar besvärstillstånd.

Beslut av organ för bedömning av överensstämmelse och beslut av certifieringsorgan ska iakttas oberoende av ändringssökande, om inte den myndighet där ändring sökts bestämmer något annat.

Denna lag träder i kraft den 1 juli 2016. Lagens 7 b § tillämpas dock först från och med den 1 maj 2017.

En leverantör av identifieringsverktyg får till och med den 31 december 2018 som ett i 17 § 2 mom. i denna lag avsett godkänt dokument också använda ett giltigt körkort som har beviljats efter den 1 oktober 1990 av en myndighet i en medlemsstat i Europeiska ekonomiska samarbetsområdet.

De av Kommunikationsverket meddelade föreskrifter som gäller vid ikraftträdandet av denna lag förblir i kraft.

En leverantör av identifieringstjänster som är införd i det register som avses i 12 § ska senast två månader från ikraftträdandet av denna lag lämna Kommunikationsverket en ändringsanmälan enligt 10 § 3 mom. i denna lag, om leverantören vill fortsätta vara verksam som leverantör av identifieringstjänster för stark autentisering. De uppgifter som

krävs enligt 10 § i denna lag ska lämnas in till Kommunikationsverket senast den 31 januari 2017.

Kommunikationsverket ska behandla en ändringsanmälan enligt 4 mom. från en leverantör av identifieringstjänster och göra de anteckningar som föranleds av anmälan i det register som avses i 12 § senast tre månader efter att ha mottagit ändringsanmälan och övriga uppgifter enligt 4 mom.

Ett identifieringsverktyg för stark autentisering som har beviljats enligt de bestämmelser som gällde vid ikraftträdandet av denna lag ska betraktas som ett identifieringsverktyg för stark autentisering för åtminstone tillitsnivån väsentlig i två månader från ikraftträdandet av denna lag. Om inte något annat följer av 7 mom. och om leverantören av identifieringstjänster lämnar en ändringsanmälan enligt 4 mom. inom föreskriven tid, ska ett identifieringsverktyg som leverantören beviljat före eller efter ikraftträdandet av denna lag betraktas som ett identifieringsverktyg för stark autentisering för åtminstone tillitsnivån väsentlig tills Kommunikationsverket har gjort en anteckning om identifieringstjänsten i det register som avses i 12 § utifrån uppgifterna i ändringsanmälan.

Ett elektroniskt identifieringsverktyg som har beviljats enligt 17 § i denna lag på grundval av ett elektroniskt identifieringsverktyg som sökanden tidigare innehaft ska betraktas som ett identifieringsverktyg för stark autentisering, om

1) identifieringsverktyget har beviljats senast två månader från ikraftträdandet av denna lag, eller

2) identifieringsverktyget har beviljats efter det att två månader förflutit från ikraftträdandet av denna lag på grundval av ett sådant annat identifieringsverktyg för stark autentisering som beviljats av en leverantör av identifieringstjänster som gjort en ändringsanmälan enligt 4 mom.

Ett elektroniskt identifieringsverktyg betraktas inte längre som ett identifieringsverktyg för stark autentisering, om leverantören av identifieringstjänster inte har lämnat en ändringsanmälan enligt 4 mom. inom föreskriven tid. Kommunikationsverket ska då avföra leverantören av identifieringstjänster ur det register som avses i 12 § och underrätta leverantören om detta.

Helsingfors den 29 juni 2016

Republikens President

Sauli Niinistö

Kommunikationsminister Anne Berner

UTGIVARE: JUSTITIEMINISTERIET ISSN 1456-9663