FINLANDS FÖRFATTNINGSSAMLING

2009 Utgiven i Helsingfors den 19 augusti 2009 **Nr 617—625**

INNEHÅLL

Nr 617

Lag

om stark autentisering och elektroniska signaturer

Given i Nådendal den 7 augusti 2009

I enlighet med riksdagens beslut föreskrivs:

1 kap.

Allmänna bestämmelser

1 §

Tillämpningsområde

I denna lag föreskrivs om stark autentisering och elektroniska signaturer samt om tillhandahållande av tjänster i anslutning till dem för tjänsteleverantörer som använder tjänsterna och för allmänheten.

Lagen tillämpas inte på tillhandahållande av tjänster avsedda för identifiering eller elektroniska signaturer internt inom en sammanslutning.

Lagen tillämpas inte heller om en sammanslutning tillämpar en egen metod för identifiering för att i samband med sina egna tjänster identifiera sina egna kunder.

Lagen tillämpas inte på tillverkning, import eller försäljning av identifieringsverktyg eller verktyg för elektroniska signaturer.

2 §

Definitioner

I denna lag avses med

1) *stark autentisering* identifiering av en person och verifiering av identifikatorns autenticitet och riktighet genom tillämpning av en elektronisk metod där identifieringen och verifieringen grundar sig på minst två av följande tre alternativ:

a) ett lösenord eller någonting annat som en innehavare av ett identifieringsverktyg vet,

b) ett smartkort eller någonting annat som en innehavare av ett identifieringsverktyg har i sin besittning, eller

RP 36/2009
KoUB 12/2009
RSv 90/2009

94—2009

c) fingeravtryck eller någon annan egenskap som identifierar en innehavare av ett identifieringsverktyg,

2) *identifieringsverktyg* föremål och specificerande uppgifter eller egenskaper som tillsammans utgör de identifikatorer, verktyg för identifiering och verktyg för verifiering som behövs för stark autentisering,

3) *identifieringsmetod* den helhet som bildas av identifieringsverktyget tillsammans med det system som behövs för att genomföra en enskild identifieringstransaktion baserad på stark autentisering,

4) *leverantör av identifieringstjänster* en tjänsteleverantör som tillhandahåller tjänster för stark autentisering till tjänsteleverantörer som använder sådana tjänster eller som ger ut identifieringsverktyg till allmänheten eller bådadera,

5) *innehavare av identifieringsverktyg* en fysisk person som på basis av avtal har fått ett identifieringsverktyg av en leverantör av identifieringstjänster,

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

7) *certifikat* ett intyg i elektronisk form som verifierar identiteten eller verifierar identiteten och kopplar ihop signaturverifieringsdata med en undertecknare och som kan användas vid stark autentisering och elektroniska signaturer,

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

9) *elektronisk signatur* data i elektronisk form som är fogade eller logiskt knutna till andra elektroniska data och som används som ett instrument för verifiering av undertecknarens identitet,

10) *avancerad elektronisk signatur* en elektronisk signatur som

a) entydigt är knuten till undertecknaren,

b) gör det möjligt att identifiera undertecknaren,

c) är skapad med en metod som endast undertecknaren kontrollerar, och

d) är knuten till andra elektroniska data på ett sådant sätt att eventuella senare förvanskningar av dessa data kan upptäckas,

11) *signaturframställningsdata* unika data, såsom koder eller privata nycklar, som undertecknaren använder för att skapa en elektronisk signatur,

12) *anordning för signaturframställning* programvara eller maskinvara för användning av signaturframställningsdata då en elektronisk signatur skapas, och

13) *signaturverifieringsdata* data, såsom koder eller öppna nycklar, som används för att verifiera en elektronisk signatur.

2 kap.

Rättsverkningar och behandling av personuppgifter

3 §

Bestämmelsernas tvingande natur

Ett avtalsvillkor som avviker från bestämmelserna i denna lag till konsumentens nackdel är utan verkan, om inte något annat föreskrivs nedan.

4 §

Elektroniska signaturer som skapas med identifieringsverktyg

Elektroniska signaturer och avancerade elektroniska signaturer kan skapas med identifieringsverktyg på det sätt som verktygens egenskaper tillåter, om inte något annat föreskrivs på något annat ställe i lag eller i 18 §.

5 §

Rättshandlingar

Identifieringsverktyg får användas vid rättshandlingar, om inte något annat föreskrivs på något annat ställe i lag eller i 18 §.

Om en rättshandling enligt lag kräver underskrift, uppfylls detta krav åtminstone genom en sådan avancerad elektronisk signatur som baserar sig på ett kvalificerat certifikat och har skapats med en säker anordning för signaturframställning. Elektroniska signaturer ska dock inte förvägras rättslig verkan enbart på den grunden att de har skapats på något annat sätt än vad som anges ovan.

I fråga om användningen av elektroniska signaturer inom förvaltningen föreskrivs särskilt.

6 §

Behandling av personuppgifter

De personuppgifter som behövs när identifieringsverktyg ges ut och tjänster upprätthålls och för identifieringstransaktioner får leverantörer av identifieringstjänster behandla på de grunder som anges i 8 § 1 mom. 1 och 2 punkten i personuppgiftslagen (523/1999). På samma grunder får certifikatutfärdare som tillhandahåller elektroniska signaturer behandla de personuppgifter som behövs vid utfärdandet och upprätthållandet av certifikat. I det syfte som anges ovan får leverantörer av identifieringstjänster och certifikatutfärdare som tillhandahåller elektroniska signaturer dessutom inhämta personuppgifter från personen själv.

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

När leverantörer av identifieringstjänster och certifikatutfärdare som tillhandahåller elektroniska signaturer kontrollerar sökandens identitet får de kräva att han eller hon uppger sin personbeteckning. Leverantörerna och certifikatutfärdarna får behandla personbeteckningar i sina register i de syften som nämns i 1 mom. Identifieringsverktyg och certifikat får innehålla personbeteckning om verktygets eller certifikatets innehåll är tillgängligt endast för dem som nödvändigt behöver den för att tillhandahålla tjänsten. Personbeteckningen får inte vara tillgänglig i en offentlig katalog.

I övrigt föreskrivs det om behandlingen av personuppgifter i 19, 24, 30, 37 och 38 § och i personuppgiftslagen.

7 §

Användning av uppgifter i befolkningsdatasystemet

Leverantörer av identifieringstjänster och certifikatutfärdare som tillhandahåller elektroniska signaturer får på de grunder som avses i 8 § 1 mom. 1 och 2 punkten i personuppgiftslagen och för de syften som nämns i 6 § 1 mom. i denna lag inhämta personuppgifter ur befolkningsdatasystemet och i systemet kontrollera de personuppgifter som en sökande eller innehavare har uppgett.

En uppgift som lämnas ut ur befolkningsdatasystemet är en offentligrättslig prestation. I fråga om avgiften för en prestation föreskrivs i lagen om grunderna för avgifter till staten (150/1992).

3 kap.

Stark autentisering

8 §

Krav som gäller identifieringsmetoden

Identifieringsmetoden ska uppfylla följande krav:

1) metoden ska grunda sig på en inledande identifiering enligt 17 § så att uppgifterna om den kan kontrolleras i efterskott i enlighet med 24 §,

2) metoden ska medge entydig identifiering av innehavaren av identifieringsverktyget,

3) det ska med tillräckligt hög tillförlitlighet gå att säkerställa att endast innehavaren av identifieringsverktyget kan använda verktyget, och

4) metoden ska vara tillräckligt säker och tillförlitlig med tanke på de informationssäkerhetsrisker som är förknippade med den teknik som används.

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.

Kommunikationsverket kan utfärda närmare tekniska föreskrifter om de krav som avses i 1 mom.

9 §

Krav som gäller leverantörer av identifieringstjänster

Fysiska personer i egenskap av leverantörer av identifieringstjänster eller fysiska per-

soner som handlar för deras räkning samt ledamöter eller suppleanter i styrelsen eller förvaltningsrådet för en sammanslutning eller stiftelse som är tjänsteleverantör, liksom dess verkställande direktör och ansvariga bolagsmän eller andra personer i motsvarande ställning ska uppfylla följande krav:

1) de ska ha uppnått myndighetsålder,

2) de får inte vara försatta i konkurs, och

3) de får inte ha begränsad handlingsbehörighet.

En leverantör av identifieringstjänster ska vara tillförlitlig. En leverantör betraktas inte som tillförlitlig om en sådan person som avses i 1 mom. genom en lagakraftvunnen dom under de senaste fem åren har dömts till fängelsestraff eller under de senaste tre åren har dömts till böter för ett brott som kan anses visa att personen i fråga är uppenbart olämplig att tillhandahålla identifieringstjänster.

En leverantör av identifieringstjänster betraktas inte heller som tillförlitlig, om en sådan person som avses i 1 mom. i övrigt genom sin tidigare verksamhet har visat sig vara uppenbart olämplig som leverantör av identifieringstjänster.

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 tjänsteleverantörer 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) uppgifter om de omständigheter som avses i 8, 9, 13 och 14 §, och

5) övriga uppgifter som behövs för tillsynen.

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

Kommunikationsverket kan utfärda för tillsynen behövliga tekniska föreskrifter om det närmare innehållet i de uppgifter enligt denna paragraf som ska anmälas och om inlämnandet av dem till Kommunikationsverket.

11 §

Leverantör av identifieringstjänster som är etablerad i en annan medlemsstat i Europeiska ekonomiska samarbetsområdet

Vad som föreskrivs i 10 § hindrar inte att en leverantör av identifieringstjänster som är etablerad i en annan medlemsstat i Europeiska ekonomiska samarbetsområdet gör en anmälan enligt nämnda paragraf.

12 §

Register över leverantörer av identifieringstjänster

Kommunikationsverket ska föra ett offentligt register över de leverantörer av identifieringstjänster som har gjort en anmälan enligt 10 § och om de tjänster som de tillhandahåller.

Efter det att anmälan enligt 10 § har inkommit ska Kommunikationsverket förbjuda en tjänsteleverantör att tillhandahålla sina tjänster som stark autentisering, om tjänsterna eller tjänsteleverantören inte uppfyller kraven i detta kapitel. Om bristfälligheten kan anses vara endast ringa, kan Kommunikationsverket uppmana tjänsteleverantören att avhjälpa bristfälligheten inom en utsatt tid.

13 §

Allmänna skyldigheter för leverantörer av identifieringstjänster

Leverantören av identifieringstjänster ska se till att de anställda har tillräcklig sakkunskap, erfarenhet och kompetens med tanke på verksamhetens omfattning.

Leverantören av identifieringstjänster ska ha med tanke på verksamhetens omfattning

tillräckliga ekonomiska resurser för att ordna verksamheten och täcka ett eventuellt skadeståndsansvar. Leverantören får också vidta andra nödvändiga åtgärder för att täcka ett eventuellt skadeståndsansvar.

Leverantören av identifieringstjänster ska dessutom ansvara för skyddet av uppgifterna enligt 32 § i personuppgiftslagen och för en tillräcklig informationssäkerhet i fråga om sina tjänster.

Leverantören av identifieringstjänster svarar för att tjänster och produkter som produceras av personer som leverantören anlitar är tillförlitliga och fungerar.

14 §

Principer för identifiering

Leverantören av identifieringstjänster ska ha principer för identifiering som närmare anger hur tjänsteleverantören uppfyller de skyldigheter som avses i denna lag. Det ska i synnerhet anges närmare hur leverantören utför den inledande identifieringen enligt 17 §.

Principerna för identifiering ska dessutom innehålla de viktigaste uppgifterna om

1) tjänsteleverantören,

2) de tjänster som tillhandahålls och priserna på dem,

3) tjänsteleverantörens viktigaste samarbetspartner,

4) de kontroller som har utförts av utomstående bedömningsorgan, och

5) andra omständigheter som är av betydelse för att tjänsteleverantörens verksamhet och tillförlitlighet ska kunna bedömas.

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

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

15 §

Skyldighet för leverantörer av identifieringstjänster att lämna uppgifter innan avtal ingås

Leverantören av identifieringstjänster ska innan ett avtal ingås informera den som ansöker om ett identifieringsverktyg om

1) tjänsteleverantören,

2) de tjänster som tillhandahålls och priserna på dem,

3) principerna för identifiering enligt 14 §,

4) parternas rättigheter och skyldigheter,

5) eventuella ansvarsbegränsningar,

6) förfarandena för klagomål och avgörande av tvister,

7) eventuella hinder för och begränsningar av användningen som avses i 18 §, och

8) övriga eventuella villkor för användning av identifieringsverktyget.

De uppgifter som avses i 1 mom. ska lämnas skriftligen eller elektroniskt så att den som ansöker om ett identifieringsverktyg kan spara och återge dem i oförändrad form. Om ett avtal på begäran av den som ansöker om ett identifieringsverktyg ingås genom distanskommunikation så att uppgifter och avtalsvillkor inte kan lämnas på det sätt som avses ovan innan avtalet ingås, ska uppgifterna utan dröjsmål lämnas på det nämnda sättet efter det att avtalet har ingåtts.

Bestämmelser om skyldigheten att lämna uppgifter vid behandlingen av personuppgifter finns i personuppgiftslagen.

16 §

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

Leverantören av identifieringstjänster ska utan onödigt dröjsmål anmäla betydande hot och störningar som riktas mot tjänsternas informationssäkerhet till de tjänsteleverantörer som använder tjänsterna, innehavarna av identifieringsverktyg och Kommunikationsverket.

Om hotet eller störningen riktas mot det skydd av uppgifter som avses i 32 § i personupppgiftslagen, ska leverantören av identifieringstjänster förutom till de aktörer som avses i 1 mom. även anmäla saken till dataombudsmannen.

I anmälan ska också redogöras för de åtgärder som de olika aktörerna kan vidta för att avvärja hoten eller störningarna, och

för de beräknade kostnaderna för dessa åtgärder.

17 §

Inledande identifiering av den som ansöker om ett identifieringsverktyg

Den inledande identifieringen ska göras personligen. Leverantören av identifieringstjänster ska noggrant identifiera den som ansöker om ett identifieringsverktyg genom att fastställa identiteten med hjälp av ett giltigt pass eller identitetskort som har utfärdats av en myndighet i en medlemsstat inom Europeiska ekonomiska samarbetsområdet, i Schweiz eller i San Marino. Vid den inledande identifieringen får leverantören, om denne så önskar, även använda ett giltigt körkort som har utfärdats efter den 1 oktober 1990 av en myndighet i en medlemsstat i Europeiska ekonomiska samarbetsområdet eller ett giltigt pass som har utfärdats av en myndighet i någon annan stat.

Den inledande identifieringen behöver inte göras personligen, om leverantörer av identifieringstjänster sinsemellan har avtalat om möjligheten att lita på varandras inledande identifieringar. Då kan ansökan om identifieringsverktyg göras elektroniskt. I avtalet ska leverantörerna av identifieringstjänster fastställa hur ansvaret fördelas mellan dem, om den ursprungliga identifieringen är felaktig. Den leverantör som litar på en inledande identifiering som gjorts av en annan leverantör bär ansvaret i förhållande till den skadelidande.

Ansökan om identifieringsverktyg kan göras elektroniskt också när sökanden har ett gällande identifieringsverktyg som har getts ut av samma leverantör av identifieringstjänster. Då behöver den inledande identifieringen inte göras på nytt.

Om identiteten hos den som ansöker om ett identifieringsverktyg inte kan verifieras på ett tillförlitligt sätt, ska polisen utföra den inledande identifiering som gäller ansökan. De kostnader som polisens identifiering orsakar den som ansöker om ett identifieringsverktyg är en offentligrättslig prestation. I fråga om avgiften för en sådan prestation föreskrivs i lagen om grunderna för avgifter till staten.

18 §

Hinder och begränsningar när det gäller att utföra rättshandlingar

Användningen av identifieringsverktyg för att utföra rättshandlingar får förhindras genom avtal mellan leverantörer av identifieringstjänster, tjänsteleverantörer som använder tjänsterna och innehavare av identifieringsverktyg. Dessutom får utförandet av rättshandlingar begränsas både när det gäller användningsändamål och transaktionernas värde i pengar.

Leverantören av identifieringstjänster ska se till att alla parter känner till hindren eller begränsningarna eller att de är lätta upptäcka. Leverantören får även införa hinder eller begränsningar med tekniska medel. Leverantören svarar inte för de åtgärder som har vidtagits i strid med hindren eller begränsningarna trots att leverantören har handlat på ett omsorgsfullt sätt.

Leverantören av identifieringstjänster ska se till att en tjänsteleverantör som använder identifieringstjänsterna har möjlighet att dygnet runt kontrollera de hinder och begränsningar som gäller identifieringsverktyget. Denna skyldighet föreligger dock inte om användning av identifieringsverktyget i strid med hindren och begränsningarna har förhindrats med hjälp av tekniska medel.

En tjänsteleverantör som använder identifieringstjänster ska i samband med användningen av ett identifieringsverktyg kontrollera eventuella hinder eller begränsningar i de system och register som leverantören av identifieringstjänsterna har. Detta behöver dock inte göras om användning av identifieringsverktyget i strid med hindren och begränsningarna har förhindrats med hjälp av tekniska medel.

19 §

Certifikatets innehåll

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

1) uppgifter om certifikatutfärdaren,

2) uppgifter om innehavaren av certifikatet,

3) innehavarens identifieringskod,

4) certifikatets giltighetstid,
5) certifikatets identifieringskod,
6) uppgifter om eventuella hinder och begränsningar som gäller användningen av certifikatet,
7) certifikatinnehavarens öppna nyckel och uppgifter om nyckelns användningsändamål, och
8) certifikatutfärdarens avancerade elektroniska signatur.

Den som tillhandahåller certifikattjänster ska för sin del försäkra sig om att en tjänsteleverantör som använder identifieringstjänster har tillgång till certifikatets innehåll om det är nödvändigt för identifieringen.

20 §

Utgivning av identifieringsverktyg

Utgivningen av identifieringsverktyg grundar sig på ett avtal mellan den som ansöker om verktyget och leverantören av identifieringstjänster. Avtalet ska ingås skriftligen. Avtalet kan även ingås elektroniskt om dess innehåll inte kan ändras ensidigt och det hålls tillgängligt för parterna. Leverantören av identifieringstjänster ska bemöta sina kunder på ett icke-diskriminerande sätt och dem som ansöker om identifieringsverktyg jämlikt när avtalet ingås.

Avtalet kan gälla tills vidare eller för viss tid. Ett identifieringsverktyg kan ha en giltighetstid som är kortare än avtalets giltighetstid.

Identifieringsverktyg tillhandahålls endast fysiska personer. Identifieringsverktyg ska vara personliga. Till ett verktyg kan vid behov fogas en uppgift om att en person i enskilda fall även kan företräda en annan fysisk person eller en juridisk person.

21 §

Överlåtelse av identifieringsverktyg till sökande

Leverantören av identifieringstjänster ska överlåta identifieringsverktyget till den sökande på det sätt som anges i avtalet. Leverantören ska på ett tillräckligt sätt säkerställa att verktyget inte obehörigt kommer i någon annans besittning vid överlåtelsen.

22 §

Förnyande av identifieringsverktyg

Leverantören av identifieringstjänster får leverera ett nytt verktyg till en innehavare av ett identifieringsverktyg utan en uttrycklig begäran endast om ett verktyg som tidigare har tillhandahållits ska ersättas med ett nytt. Vid leveransen ska bestämmelserna i 21 § iakttas.

23 §

Skyldigheter för innehavare av identifieringsverktyg

Innehavaren av ett identifieringsverktyg ska använda verktyget i enlighet med villkoren i avtalet. Innehavaren ska förvara identifieringsverktyget omsorgsfullt. Innehavaren är skyldig att ansvara för verktyget efter att ha tagit emot det.

Innehavaren av ett identifieringsverktyg får inte överlåta verktyget för att användas av någon annan.

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 och elektronisk signering,
2) de uppgifter som behövs om den inledande identifiering av en sökande som avses i 17 § och om den handling som anlitats för identifieringen,
3) uppgifter om sådana eventuella hinder och begränsningar för användningen av verktyget som avses i 18 §, och
4) i fråga om certifikat, uppgifter om certifikatets innehåll enligt 19 §.

De uppgifter som avses i 1 mom. 1 punkten ska förvaras i fem år från identifieringstransaktionen. De uppgifter som avses i 1 mom. 2—4 punkten ska förvaras i fem år från det att kundförhållandet mellan leverantören av identifieringstjänster och innehavaren av ett identifieringsverktyg upphörde.

De personuppgifter som har samlats in 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, utföra fakturering och trygga sina rättigheter vid tvister 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.

Vad som föreskrivs i 1 mom. 1 punkten och 3 mom. gäller inte tjänsteleverantörer som endast ger ut identifieringsverktyg. Den förvaringstid på fem år som avses i 2 mom. räknas då från det att identifieringsverktyget upphörde att gälla.

25 §

Anmälan om återkallande eller förhindrande av användning av identifieringsverktyg

Innehavaren av ett identifieringsverktyg ska anmäla till leverantören av identifieringstjänster eller någon annan aktör som denne har utsett att verktyget har försvunnit, obehörigt har kommit i någon annans besittning eller obehörigt har använts. Anmälan ska göras utan obefogat dröjsmål efter det att saken har upptäckts.

Leverantören av identifieringstjänster ska se till att det är möjligt att när som helst göra en anmälan enligt 1 mom. Leverantören ska utan dröjsmål återkalla verktyget eller förhindra att det används efter det att anmälan har mottagits.

Leverantören av identifieringstjänster ska på lämpligt sätt och utan dröjsmål i systemet registrera uppgift om tidpunkten för återkallandet eller förhindrandet av användningen. Innehavaren av ett identifieringsverktyg har rätt att på begäran få ett intyg över att han eller hon har gjort anmälan enligt 1 mom. Intyget ska begäras inom 18 månader från anmälan.

Systemet ska vara sådant att en tjänsteleverantör som använder identifieringstjänster lätt kan kontrollera uppgifterna i systemet vilket tid på dygnet som helst. Skyldighet att ordna möjlighet att kontrollera uppgifterna föreligger dock inte, om användning av identifieringsverktyget kan förhindras med hjälp av tekniska medel eller om verktyget kan spärras.

En tjänsteleverantör som använder identifieringstjänster ska i samband med användningen av ett identifieringsverktyg kontrollera uppgifterna om eventuella återkallanden och hinder i de system och register som leverantören av identifieringstjänster har. Detta behöver dock inte göras om användning av identifieringsverktyget kan förhindras med hjälp av tekniska medel eller om verktyget kan spärras.

Om en identifieringstjänst grundar sig på certifikat och uppgifter om återkallade certifikat ges med hjälp av en spärrlista, får den som tillhandahåller certifikattjänster registrera uppgifter om sådan kontroll av certifikatens giltighet som gjorts på spärrlistan. Certifikatutfärdaren kan alternativt lagra spärrlistan.

26 §

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

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

1) leverantören av identifieringstjänster har skäl att misstänka att verktyget används av någon annan än den som identifieringsverktyget har getts ut till,

2) verktyget innehåller ett uppenbart fel,

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

4) innehavaren av ett identifieringsverktyg använder verktyget på ett sätt som väsentligt strider mot avtalsvillkoren, eller

5) innehavaren av identifieringsverktyget har avlidit.

Leverantören av identifieringstjänster ska så snart som möjligt underrätta innehavaren om att identifieringsverktyget har återkallats eller användningen av det förhindrats och ange när och varför återkallandet eller förhindrandet skett.

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

27 §

Begränsningar av ansvaret för innehavaren vid obehörig användning av ett identifieringsverktyg

Innehavaren av ett identifieringsverktyg ansvarar för obehörig användning av verktyget endast om

1) innehavaren har överlåtit identifieringsverktyget till någon annan,

2) identifieringsverktyget har försvunnit, kommit i någon annans besittning obehörigt eller använts obehörigt på grund av innehavarens vårdslöshet, som inte är lindrig, eller

3) innehavaren har försummat att utan obefogat dröjsmål efter det att saken har upptäckts anmäla till leverantören av identifieringstjänster eller någon annan aktör som denne har angett att identifieringsverktyget har försvunnit, kommit i någon annans besittning obehörigt eller använts obehörigt.

Innehavaren av ett identifieringsverktyg ansvarar dock inte för obehörig användning av verktyget

1) till den del identifieringsverktyget har använts efter det att innehavaren har anmält till leverantören av identifieringstjänster att identifieringsverktyget har försvunnit, kommit i någon annans besittning obehörigt eller använts obehörigt,

2) om innehavaren av identifieringsverktyget inte har kunnat göra en anmälan utan obefogat dröjsmål efter det att saken har upptäckts om att verktyget har försvunnit, kommit i någon annans besittning obehörigt eller använts obehörigt på grund av att leverantören av identifieringstjänster har åsidosatt skyldigheten enligt 25 § 2 mom. att se till att innehavaren av ett identifieringsverktyg har möjlighet att när som helst göra en sådan anmälan, eller

3) om en tjänsteleverantör som använder identifieringstjänster har åsidosatt sin skyldighet enligt 18 § 4 mom. och 25 § 5 mom. att kontrollera om det finns begränsningar för användningen av identifieringsverktyget eller uppgift om hinder för användningen av eller spärrning av verktyget.

4 kap.

Elektroniska signaturer

28 §

Säkra anordningar för signaturframställning

En säker anordning för signaturframställning ska på ett tillräckligt tillförlitligt sätt säkerställa att

1) signaturframställningsdata i praktiken kan förekomma endast en gång och att de förblir konfidentiella,

2) signaturframställningsdata inte kan härledas ur andra data,

3) signaturen är skyddad mot förfalskning,

4) undertecknaren kan skydda signaturframställningsdata så att andra inte kan använda dem, och

5) anordningen inte förändrar de uppgifter som ska signeras eller hindrar att de presenteras för undertecknaren före signeringen.

En anordning för signaturframställning anses alltid uppfylla kraven i 1 mom., om

1) den överensstämmer med de allmänt erkända standarder som Europeiska gemenskapernas kommission har fastställt och som har offentliggjorts i Europeiska unionens officiella tidning, eller

2) ett kontrollorgan, beläget i Finland eller i en annan stat inom Europeiska ekonomiska samarbetsområdet, som har utsetts för att bedöma om kraven uppfylls har godkänt anordningen.

29 §

Kontrollorgan

Kommunikationsverket kan utse kontrollorgan med uppgift att bedöma om anordningar för signaturframställning uppfyller kraven i 28 § 1 mom. Kontrollorganen kan vara privata eller offentliga inrättningar.

En inrättning kan utses till kontrollorgan under förutsättning att

1) den är oberoende i fråga om sin verksamhet och ekonomi,

2) dess verksamhet är tillförlitlig, ändamålsenlig och icke-diskriminerande,

3) den har tillräckliga ekonomiska resurser för att ordna verksamheten ändamålsenligt och täcka ett eventuellt ersättningsansvar,

4) den har tillgång till yrkeskunnig och opartisk personal i den omfattning som behövs, och

5) den har tillgång till sådana lokaler och sådan utrustning som verksamheten kräver.

Kommunikationsverket utser kontrollorganen på ansökan. Ansökan ska utöver sökandens kontaktuppgifter och handelsregisterutdrag eller motsvarande utredning innehålla uppgift om huruvida sökandens verksamhet uppfyller kraven i 2 mom. Kommunikationsverket meddelar vid behov anvisningar om de uppgifter som ska ingå i ansökan och om inlämnandet av dem till Kommunikationsverket.

Kommunikationsverket övervakar kontrollorganens verksamhet. Om ett kontrollorgan inte uppfyller fastställda krav eller om det bryter mot bestämmelserna, ska Kommunikationsverket återkalla beslutet genom vilket det utsett kontrollorganet. Kontrollorganen ska underrätta Kommunikationsverket om sådana ändringar i verksamheten som inverkar på förutsättningarna för att bli utsedd till kontrollorgan.

Vid bedömningen av anordningar kan kontrollorganet anlita utomstående personer. Kontrollorganet svarar också för det arbete som dessa utför.

30 §

Kvalificerade certifikat

Med kvalificerat certifikat avses ett certifikat som uppfyller kraven i 2 mom. och som har utfärdats av en certifikatutfärdare som uppfyller kraven i 33—38 §.

Ett kvalificerat certifikat ska innehålla

1) uppgift om att certifikatet är ett kvalificerat certifikat,

2) uppgift om certifikatutfärdaren och dennes etableringsstat,

3) undertecknarens namn eller pseudonym med uppgift om att det är en pseudonym,

4) signaturverifieringsdata som motsvarar de signaturframställningsdata som undertecknaren innehar,

5) det kvalificerade certifikatets giltighetstid,

6) det kvalificerade certifikatets identifieringskod,

7) certifikatutfärdarens avancerade elektroniska signatur,

8) eventuella begränsningar av användningen av det kvalificerade certifikatet, och

9) särskilda uppgifter om undertecknaren, om de behövs med tanke på ändamålet med det kvalificerade certifikatet.

Om en certifikatutfärdare som tillhandahåller kvalificerade certifikat även tillhandahåller identifieringstjänster enligt 3 kap., anses kraven i 1 mom. alltid också uppfylla de krav på certifikatets innehåll som avses i 19 § 1 mom.

31 §

Kvalificerade certifikat som tillhandahålls av en certifikatutfärdare som inte är etablerad i Finland

Ett certifikat som anges vara kvalificerat och som tillhandahålls av en certifikatutfärdare som inte är etablerad i Finland anses uppfylla kraven på kvalificerat certifikat i denna lag, om

1) certifikatutfärdaren är etablerad i en stat inom Europeiska ekonomiska samarbetsområdet och certifikatet uppfyller etableringsstatens krav på kvalificerat certifikat,

2) certifikatutfärdaren har anslutit sig till ett frivilligt ackrediteringssystem i en stat inom Europeiska ekonomiska samarbetsområdet och uppfyller de nationella krav som i denna stat föreskrivits för genomförande av Europaparlamentets och rådets direktiv 1999/93/EG om ett gemenskapsramverk för elektroniska signaturer, nedan *direktivet om elektroniska signaturer*,

3) certifikatet garanteras av en certifikatutfärdare som är etablerad i en stat inom Europeiska ekonomiska samarbetsområdet och uppfyller de nationella krav som i denna stat föreskrivits för genomförande av direktivet om elektroniska signaturer, eller

4) certifikatet eller certifikatutfärdaren har erkänts enligt ett bilateralt eller multilateralt avtal mellan Europeiska gemenskapen och ett eller flera tredjeländer eller internationella organisationer.

32 §

Anmälan om inledande av verksamhet

En certifikatutfärdare som tillhandahåller kvalificerade certifikat ska göra en skriftlig anmälan till Kommunikationsverket innan verksamheten inleds. Anmälan ska innehålla certifikatutfärdarens namn och kontaktuppgifter samt de uppgifter som behövs för att säkerställa att kraven i 30 och 33—38 § uppfylls. Kommunikationsverket kan utfärda föreskrifter om det närmare innehållet i de uppgifter som ska lämnas och om inlämnandet av dem till Kommunikationsverket.

Kommunikationsverket ska utan dröjsmål efter det att anmälan inkommit förbjuda certifikatutfärdaren att tillhandahålla sina certifikat som kvalificerade certifikat, om certifikaten inte uppfyller kraven i 30 § 2 mom. eller om certifikatutfärdaren inte uppfyller kraven i 33—38 §.

Certifikatutfärdaren ska utan dröjsmål skriftligen underrätta Kommunikationsverket, om de uppgifter som avses i 1 mom. har förändrats.

Kommunikationsverket för ett offentligt register över certifikatutfärdare som utfärdar kvalificerade certifikat.

Certifikatutfärdare som tillhandahåller kvalificerade certifikat kan också göra en anmälan enligt 10 §, om de utöver kvalificerade certifikat även vill tillhandahålla identifieringstjänster.

33 §

Allmänna skyldigheter för certifikatutfärdare som tillhandahåller kvalificerade certifikat

Certifikatutfärdaren ska ha tillräckliga tekniska kunskaper och ekonomiska resurser med tanke på verksamhetens omfattning. Certifikatutfärdaren svarar för alla delområden av certifikatverksamheten, även för att tjänster och produkter som produceras av personer som certifikatutfärdaren eventuellt anlitar är tillförlitliga och fungerar.

Certifikatutfärdaren ska

1) säkerställa att personalen har tillräcklig sakkunskap, erfarenhet och kompetens,

2) förfoga över tillräckliga ekonomiska resurser för att ordna verksamheten och täcka ett eventuellt skadeståndsansvar,

3) hålla sådana uppgifter om certifikaten och certifikatverksamheten allmänt tillgängliga som behövs för bedömande av certifikatutfärdarens verksamhet och tillförlitlighet, och

4) sörja för att signaturframställningsdata är konfidentiella då certifikatutfärdaren själv framställer dem.

Certifikatutfärdaren får inte lagra eller kopiera de signaturframställningsdata som överlåtits till en undertecknare.

34 §

Tillförlitlig maskinvara och programvara

En certifikatutfärdare som tillhandahåller kvalificerade certifikat ska se till att de system samt den maskinvara och programvara som används är tillräckligt säkra och tillförlitliga samt skyddade mot ändringar och mot förfalskning.

Maskinvara eller programvara avsedd för elektroniska signaturer anses alltid uppfylla kraven i 1 mom., om den överensstämmer med de allmänt erkända standarder som Europeiska gemenskapernas kommission har fastställt och som har offentliggjorts i Europeiska unionens officiella tidning.

35 §

Utgivning av kvalificerade certifikat

En certifikatutfärdare som tillhandahåller kvalificerade certifikat ska omsorgsfullt och på ett tillförlitligt sätt kontrollera identiteten hos den som ansöker om kvalificerat certifikat och andra uppgifter som gäller sökandens person och som är relevanta för utfärdandet och upprätthållandet av det kvalificerade certifikatet. Certifikatutfärdare som tillhandahåller kvalificerade certifikat ska identifiera sökanden personligen. Utfärdaren ska bemöta sin kunder på ett icke-diskriminerande sätt och de som ansöker om certifikat jämlikt när avtalet ingås.

En certifikatutfärdare som tillhandahåller kvalificerade certifikat ska innan ett avtal ingås informera sökanden om villkoren för användning av det kvalificerade certifikatet, inbegripet eventuella begränsningar av användningen, om frivilliga ackrediteringssystem, myndighetstillsynen över verksamheten

samt förfarandena för klagomål och avgörande av tvister. Informationen ska ges skriftligen i sådan form att sökanden kan förstå den utan svårighet.

36 §

Återkallande av kvalificerade certifikat

Undertecknaren ska utan dröjsmål begära att den certifikatutfärdare som utfärdat ett kvalificerat certifikat ska återkalla det, om undertecknaren har grundad anledning att anta att signaturframställningsdata används på obehörigt sätt.

En certifikatutfärdare som tillhandahåller kvalificerade certifikat ska utan dröjsmål återkalla ett kvalificerat certifikat, om undertecknaren begär det. Begäran om återkallande av ett kvalificerat certifikat anses ha inkommit till certifikatutfärdaren då den har stått till utfärdarens förfogande så att begäran kan behandlas.

Ett kvalificerat certifikat kan återkallas också om det annars finns särskild anledning till det. Undertecknaren ska alltid underrättas om att det kvalificerade certifikatet har återkallats och om tidpunkten för återkallandet.

37 §

Register som ska föras av certifikatutfärdare som tillhandahåller kvalificerade certifikat

En certifikatutfärdare som tillhandahåller kvalificerade certifikat ska föra register över utfärdade kvalificerade certifikat (*certifikatregister*). I registret ska införas

1) de uppgifter som det kvalificerade certifikatet ska innehålla enligt 30 § 2 mom.,

2) de uppgifter som gäller sökandens person och som avses i 35 § 1 mom., inbegripet uppgift om det förfarande för identifiering av sökanden som använts då det kvalificerade certifikatet utfärdades och behövliga uppgifter om den handling som eventuellt anlitats för identifieringen, och

3) de uppgifter som avses i 39 § om kontroll av ett certifikats giltighet som gjorts på spärrlistan, om en certifikatutfärdare som tillhandahåller kvalificerade certifikat utnyttjar rätten att registrera uppgifter enligt 39 §.

En certifikatutfärdare som tillhandahåller kvalificerade certifikat ska säkerställa att den som förlitar sig på en avancerad elektronisk signatur som är baserad på ett kvalificerat certifikat har tillgång till certifikatets i 30 § 2 mom. definierade innehåll. De uppgifter som avses ovan i 1 mom. 3 punkten behöver dock inte införas i certifikatregistret, om certifikatutfärdaren på annat sätt ser till att den som förlitar sig på certifikatet kan visa upp tillförlitligt bevis på behörig kontroll av spärrlistan.

Certifikatutfärdaren ska också föra ett register över återkallade kvalificerade certifikat (*spärrlista*) som ska vara tillgängligt för dem som förlitar sig på kvalificerade certifikat. På spärrlistan ska utan dröjsmål införas uppgift om att ett kvalificerat certifikat har återkallats och exakt tidpunkt för återkallandet.

De uppgifter som nämns i 2 och 3 mom. ska vara tillgängliga dygnet runt.

38 §

Förvaring av uppgifterna i certifikatregistret

Certifikatutfärdare som tillhandahåller kvalificerade certifikat ska på ett tillförlitligt och ändamålsenligt sätt förvara uppgifterna i certifikatregistret i 10 år från det att certifikatet upphörde att gälla.

Certifikatutfärdare som utöver kvalificerade certifikat också tillhandahåller tjänster för stark autentisering får oberoende av vad som föreskrivs i 24 § till alla delar förvara uppgifterna på det sätt som avses i 1 mom.

39 §

Registrering av uppgift om kontroll av certifikats giltighet

Certifikatutfärdare som tillhandahåller kvalificerade certifikat får registrera uppgifter om kontroll av certifikatens giltighet som gjorts på spärrlistan. De registrerade uppgifterna får användas endast för fakturering av användningen av certifikat och för verifiering av rättshandlingar som företagits med hjälp av elektroniska signaturer som är baserade på certifikat.

40 §

Ansvar för obehörig användning av signaturframställningsdata

Undertecknaren ansvarar för skada som or-

sakats av obehörig användning av signaturframställningsdata för en avancerad elektronisk signatur som är baserad på ett kvalificerat certifikat tills en begäran om återkallande av certifikatet har inkommit till certifikatutfärdaren så som anges i 36 § 2 mom.

En konsument har dock ansvar enligt 1 mom. endast om

1) konsumenten har överlåtit signaturframställningsdata till någon annan,

2) någon som är obehörig att använda signaturframställningsdata 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 signaturframställningsdata och därefter har underlåtit att begära att det kvalificerade certifikatet ska återkallas så som anges i 36 § 1 mom.

41 §

Skadeståndsansvar för certifikatutfärdare som tillhandahåller kvalificerade certifikat

En certifikatutfärdare som tillhandahåller kvalificerade certifikat är ansvarig för skada som orsakats den som förlitat sig på ett kvalificerat certifikat, om skadan uppkommit genom att

1) de uppgifter som antecknats i det kvalificerade certifikatet var felaktiga vid den tidpunkt då certifikatet utfärdades,

2) det kvalificerade certifikatet inte innehåller de uppgifter som nämns i 30 § 2 mom.,

3) den person som anges i det kvalificerade certifikatet inte vid den tidpunkt då certifikatet utfärdades var i besittning av de signaturframställningsdata som motsvarar de signaturverifieringsdata som anges eller definieras i certifikatet,

4) de signaturframställningsdata och signaturverifieringsdata som framställts av certifikatutfärdaren eller en person som denne anlitat inte kan användas som komplement till varandra, eller

5) certifikatutfärdaren eller en person som denne anlitat inte har återkallat det kvalificerade certifikatet på det sätt som anges i 36 §.

Certifikatutfärdaren är fri från ansvar enligt 1 mom., om utfärdaren visar att skadan inte har orsakats av vårdslöshet hos utfärdaren själv eller någon som denne har anlitat.

En certifikatutfärdare ansvarar inte för skada som orsakats av att ett kvalificerat certifikat har använts i strid med de begränsningar av användningen som ingår i det.

I fråga om skadeståndsansvaret för certifikatutfärdare som tillhandahåller allmänheten kvalificerade certifikat föreskrivs i övrigt i skadeståndslagen (412/1974).

Vad som föreskrivs i denna paragraf tillämpas också på en certifikatutfärdare som för allmänheten garanterar att ett certifikat är ett kvalificerat certifikat.

5 kap.

Myndighetstillsyn

42 §

Allmän styrning och tillsyn

Kommunikationsministeriet svarar för den allmänna styrningen och utvecklingen av stark autentisering och elektroniska signaturer.

Kommunikationsverket har tillsyn över efterlevnaden av denna lag med undantag av 1 § 3 mom. Kommunikationsverket utfärdar vid behov tekniska föreskrifter om kraven på tillförlitlighet och informationssäkerhet i verksamhet som bedrivs av leverantörer av identifieringstjänster och certifikatutfärdare som tillhandahåller kvalificerade certifikat.

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

43 §

Rätt till information

Trots bestämmelserna om sekretess har Kommunikationsverket rätt att av leverantörer av identifieringstjänster, certifikatutfärdare som tillhandahåller kvalificerade certifikat och kontrollorgan som avses i 29 § samt av personer som dessa anlitar få den information som behövs för att fullgöra de uppgifter som anges i 42 §.

Dataombudsmannen har i sitt uppdrag rätt att få information enligt personuppgiftslagen.

44 §

Myndighetssamarbete och rätt att lämna information

Utöver vad som föreskrivs i lagen om offentlighet i myndigheternas verksamhet (621/1999) har Kommunikationsverket och dataombudsmannen trots sekretessbestämmelserna rätt att till Finansinspektionen lämna den information som den behöver för att fullgöra sina uppgifter. Finansinspektionen har motsvarande rätt att trots sekretessbestämmelserna till Kommunikationsverket och dataombudsmannen lämna de uppgifter som de behöver för att fullgöra sina uppgifter enligt denna lag.

När Kommunikationsverket och dataombudsmannen utför uppgifter enligt denna lag ska de vid behov samarbeta på lämpligt sätt med Finansinspektionen, konkurrensverket och Konsumentverket samt med varandra.

45 §

Administrativa tvångsmedel

Om någon bryter mot denna lag eller mot föreskrifter som har utfärdats med stöd av den, kan Kommunikationsverket ålägga denne att avhjälpa felet eller försummelsen. 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).

Kostnaderna för en åtgärd som vidtagits på den försumliges bekostnad betalas av statens medel och indrivs hos den försumlige på det sätt som föreskrivs i lagen om verkställighet av skatter och avgifter (706/2007).

46 §

Inspektionsrätt

Kommunikationsverket har rätt att utföra inspektioner av leverantörer av identifieringstjänster och av leverantörernas tjänster, kontrollorgan som avses i 29 § och av deras verksamhet och certifikatutfärdare som tillhandahåller kvalificerade certifikat och av deras tjänster, om det finns skäl att misstänka att de på ett väsentligt sätt har brutit mot denna lag eller mot föreskrifter som har utfärdats med stöd av den.

Kommunikationsverket ska årligen utföra inspektioner av certifikatutfärdare som tillhandahåller kvalificerade certifikat och av deras tjänster.

Kommunikationsverket förordnar en inspektör att utföra de inspektioner som avses i 1 och 2 mom. Den som utför inspektionen har rätt att hos en leverantör av identifieringstjänster och hos en certifikatutfärdare som tillhandahåller kvalificerade certifikat samt hos personer som dessa anlitar undersöka sådan maskinvara och programvara som kan vara av betydelse vid tillsynen över att denna lag och de föreskrifter som utfärdats med stöd av den efterlevs.

Leverantörer av identifieringstjänster, certifikatutfärdare som tillhandahåller kvalificerade certifikat och de personer som dessa anlitar ska för inspektionen ge en inspektör som avses i 3 mom. tillträde till sådana produktions- och affärslokaler samt lagerutrymmen som inte omfattas av hemfriden.

Kommunikationsverket har rätt att få handräckning av polisen för att utföra inspektioner enligt denna paragraf.

Vid fullgörandet av sina uppgifter har dataombudsmannen den rätt att utöva tillsyn som anges i personuppgiftslagen.

47 §

Avgifter som ska betalas till Kommunikationsverket

En leverantör av identifieringstjänster och en sammanslutning av tjänsteleverantörer som har gjort en anmälan enligt 10 § ska betala en registreringsavgift på 5 000 euro till Kommunikationsverket. Leverantören av identifieringstjänster och sammanslutningen ska dessutom årligen betala en tillsynsavgift på 12 000 euro till Kommunikationsverket.

Certifikatutfärdare som tillhandahåller kvalificerade certifikat och som gjort en an-

mälan enligt 32 § ska betala en registreringsavgift på 5 000 euro till Kommunikationsverket. Dessutom ska en sådan certifikatutfärdare årligen betala en tillsynsavgift på 40 000 euro till Kommunikationsverket. Om en certifikatutfärdare som tillhandahåller kvalificerade certifikat även gör en anmälan enligt 10 §, ska certifikatutfärdaren betala den registreringsavgift som avses i 1 mom.

Kontrollorgan som har utsetts enligt 29 § ska betala en utnämningsavgift på 10 000 euro till Kommunikationsverket. Dessutom ska kontrollorganet årligen betala en tillsynsavgift på 15 000 euro till Kommunikationsverket.

Registreringsavgiften, utnämningsavgiften och tillsynsavgiften motsvarar 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. Kommunikationsverkets beslut om att påföra avgift får överklagas i enlighet med 49 § 1 mom. Närmare bestämmelser om verkställigheten av avgifterna kan utfärdas genom förordning av kommunikationsministeriet.

Registreringsavgiften, utnämningsavgiften och tillsynsavgiften får drivas in utan dom eller beslut på det sätt som föreskrivs i lagen om verkställighet av skatter och avgifter. Om avgifterna inte betalas senast på förfallodagen, tas en årlig dröjsmålsränta ut på det obetalda beloppet enligt den räntefot som avses i 4 § 1 mom. i räntelagen (633/1982). I stället för dröjsmålsränta kan myndigheten ta ut en dröjsmålsavgift på fem euro i sådana fall då dröjsmålsräntan understiger detta belopp.

Om den verksamhet som bedrivs av en leverantör av identifieringstjänster ska inspekteras med stöd av 46 § 1 mom., tas kostnaderna för inspektionen ut av leverantören av identifieringstjänster enligt lagen om grunderna för avgifter till staten.

6 kap.

Särskilda bestämmelser

48 §

Straffbestämmelser

Bestämmelser om straff för personregisterbrott finns i 38 kap. 9 § i strafflagen (39/1889) och bestämmelser om straff för personregisterförseelse finns i 48 § 2 mom. i personuppgiftslagen.

49 §

Ändringssökande

Bestämmelser om sökande av ändring i beslut som Kommunikationsverket har fattat med stöd av denna lag finns i förvaltningsprocesslagen (586/1996).

Kommunikationsverket kan i sitt 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 dataombudsmannens beslut finns i personuppgiftslagen.

7 kap.

Ikraftträdande

50 §

Ikraftträdande

Denna lag träder i kraft den 1 september 2009.

Genom denna lag upphävs lagen av den 24 januari 2003 om elektroniska signaturer (14/2003). De föreskrifter som Kommunikationsverket har utfärdat med stöd av den lag som upphävs är dock i kraft tills nya föreskrifter utfärdas med stöd av denna lag.

Åtgärder som verkställigheten av lagen förutsätter får vidtas innan lagen träder i kraft.

51 §

Övergångsbestämmelse

Leverantörer av identifieringstjänster ska

göra en anmälan enligt 10 § till Kommunikationsverket inom sex månader från lagens ikraftträdande. Som tjänster för stark autentisering och leverantörer av identifieringstjänster betraktas under denna tid sådana tjänster för elektronisk identifiering och sådana leverantörer av tjänster för elektronisk identifiering som omfattas av tillämpningsområdet för 1 § och som motsvarar definitionerna i 2 § 1 och 4 punkten.

Identifieringsverktyg som har getts ut före ikraftträdandet av denna lag eller inom den övergångsperiod som avses i 1 mom. betraktas som verktyg för stark autentisering, om en leverantör av identifieringstjänster gör en anmälan enligt 10 § inom den tid som avses i 1 mom. Identifieringstjänsterna och leverantörerna av identifieringstjänster ska då uppfylla alla krav som i denna lag ställs på dem, med undantag för kraven i 17 §.

Om leverantörerna av identifieringstjänster har ingått ett avtal enligt 17 § 2 mom. om möjligheten att lita på varandras inledande identifieringar, och den tjänsteleverantör som har gett ut de identifieringsverktyg som använts vid den inledande identifieringen inte har gjort en anmälan enligt 10 § inom den tid som avses i 1 mom., ska den inledande identifieringen göras utan dröjsmål på det sätt som avses i 17 § i fråga om de identifieringsverktyg som getts ut på detta sätt.

En sådan certifikatutfärdare som tillhandahåller kvalificerade certifikat och som har gjort en anmälan enligt 9 § 1 mom. i lagen om elektroniska signaturer och fortsatt verksamheten utan avbrott till ikraftträdandet av denna lag, behöver inte göra en ny anmälan enligt 32 § 1 mom. Certifikatutfärdaren kan då lämna en fritt formulerad skriftlig anmälan till Kommunikationsverket om att verksamheten fortsatt oförändrad. Certifikatutfärdare som när denna lag träder i kraft tillhandahåller kvalificerade certifikat ska, oberoende av när ovan nämnda skriftliga anmälan lämnas, fram till den 31 december 2009 betala en i 12 § i kommunikationsministeriets förordning om vissa av Kommunikationsverkets avgifter (1175/2005) avsedd certifikatavgift.

Nådendal den 7 augusti 2009

Republikens President

TARJA HALONEN

Kommunikationsminister *Suvi Lindén*

Nr 618

Lag

om ändring av lagen om elektronisk kommunikation i myndigheternas verksamhet

Given i Nådendal den 7 augusti 2009

I enlighet med riksdagens beslut

ändras i lagen av den 24 januari 2003 om elektronisk kommunikation i myndigheternas verksamhet (13/2003) 3 § 2 mom., 9 § 1 mom., 16 § och 18 § 2 mom. som följer:

3 §

Annan lagstiftning

— — — — — — — — — — — — — —

Bestämmelser om elektroniska signaturer och om tillhandahållande av identifieringstjänster och kvalificerade certifikat i anslutning till dem finns i lagen om stark autentisering och elektroniska signaturer (617/2009).

9 §

Krav på skriftlig form och underskrift

Vid anhängiggörande och behandling av ärenden uppfyller också elektroniska dokument som sänts till en myndighet kravet på skriftlig form. Om det vid anhängiggörande eller behandling av ett ärende krävs en undertecknad handling, uppfylls kravet på underskrift också genom en sådan elektronisk signatur som avses i 5 § 2 mom. i lagen om stark autentisering och elektroniska signaturer.

— — — — — — — — — — — — — —

16 §

Elektronisk signering av beslutshandlingar

En beslutshandling kan signeras elektroniskt. Myndigheten ska signera dokumentet på det sätt som anges i 5 § 2 mom. i lagen om stark autentisering och elektroniska signaturer.

18 §

Bevislig elektronisk delgivning

— — — — — — — — — — — — — —

Parten eller dennes företrädare ska identifiera sig när beslutshandlingen hämtas. Vid identifieringen kan användas ett identifieringsverktyg eller ett kvalificerat certifikat som avses i lagen om stark autentisering och elektroniska signaturer eller någon annan motsvarande identifieringsteknik som är datatekniskt tillförlitlig och bevislig.

— — — — — — — — — — — — — —

Denna lag träder i kraft den 1 september 2009.

Nådendal den 7 augusti 2009

Republikens President

TARJA HALONEN

Kommunikationsminister *Suvi Lindén*

RP 36/2009
KoUB 12/2009
RSv 90/2009

3 /94

Nr 619

Lag

om ändring av 2 och 9 § i lagen om elektronisk behandling av klientuppgifter inom social- och hälsovården

Given i Nådendal den 7 augusti 2009

I enlighet med riksdagens beslut

ändras i lagen av den 9 februari 2007 om elektronisk behandling av klientuppgifter inom social- och hälsovården (159/2007) 2 § 3 mom. och 9 § som följer:

2 §

Tillämpningsområde

— — — — — — — — — — — — — —

Om inte något annat följer av denna eller någon annan lag tillämpas på behandlingen av klientuppgifter vad som bestäms i lagen om patientens ställning och rättigheter (785/1992), nedan *patientlagen*, lagen om klientens ställning och rättigheter inom socialvården (812/2000), nedan *klientlagen*, personuppgiftslagen (523/1999), lagen om offentlighet i myndigheternas verksamhet (621/1999), lagen om elektronisk kommunikation i myndigheternas verksamhet (13/2003), lagen om stark autentisering och elektroniska signaturer (617/2009) och arkivlagen (831/1994) eller med stöd av dem.

9 §

Elektronisk signering av handlingar

Klientuppgifternas integritet, oförvanskade form och oavvislighet ska säkerställas med en elektronisk signatur vid elektronisk behandling, överföring och förvaring av uppgifterna. Vid elektronisk signering som görs av en fysisk person ska användas en avancerad elektronisk signatur enligt lagen om stark autentisering och elektroniska signaturer. Vid signering som görs av en organisation och datatekniska enheter ska användas en elektronisk signatur av motsvarande tillförlitlighet.

— — — — — — — — — — — — — —

Denna lag träder i kraft den 1 september 2009.

Nådendal den 7 augusti 2009

Republikens President

TARJA HALONEN

Kommunikationsminister *Suvi Lindén*

RP 36/2009
KoUB 12/2009
RSv 90/2009

Nr 620

Lag

om ändring av 2 § i lagen om kommunikationsförvaltningen

Given i Nådendal den 7 augusti 2009

I enlighet med riksdagens beslut

ändras i lagen av den 29 juni 2001 om kommunikationsförvaltningen (625/2001) 2 § 1 punkten, sådan den lyder i lag 520/2004, som följer:

2 §

Kommunikationsverkets uppgifter

Kommunikationsverket har till uppgift att

1) sköta de uppgifter som enligt kommunikationsmarknadslagen (393/2003), lagen om radiofrekvenser och teleutrustningar (1015/2001), lagen om posttjänster (313/2001), lagen om televisions- och radioverksamhet (744/1998), lagen om statens televisions- och radiofond (745/1998), lagen om dataskydd vid elektronisk kommunikation (516/2004), lagen om förbud mot vissa avkodningssystem (1117/2001), lagen om stark autentisering och elektroniska signaturer (617/2009) och lagen om domännamn (228/2003) ankommer på Kommunikationsverket, samt

— — — — — — — — — — — — —

Denna lag träder i kraft den 1 september 2009.

Nådendal den 7 augusti 2009

Republikens President

TARJA HALONEN

Kommunikationsminister *Suvi Lindén*

RP 36/2009
KoUB 12/2009
RSv 90/2009

Nr 621

Lag

om ändring av 18 § i lagen om förhindrande och utredning av penningtvätt och av finansiering av terrorism

Given i Nådendal den 7 augusti 2009

I enlighet med riksdagens beslut

ändras i lagen av den 18 juli 2008 om förhindrande och utredning av penningtvätt och av finansiering av terrorism (503/2008) 18 § 3 punkten som följer:

18 §

Skärpta krav på kontroll vid identifiering på distans

Om kunden inte är närvarande vid identifieringen och styrkandet av identiteten (*identifiering på distans*), ska den rapporteringsskyldiga vidta följande åtgärder för att minska risken för penningtvätt och finansiering av terrorism:

— — — — — — — — — — — — — —

3) kontrollera kundens identitet med ett identifieringsverktyg eller ett kvalificerat certifikat som avses i lagen om stark autentisering och elektroniska signaturer (617/2009) eller med hjälp av någon annan teknik för elektronisk identifiering som är informationssäker och bevislig.

Denna lag träder i kraft den 1 september 2009.

Nådendal den 7 augusti 2009

Republikens President

TARJA HALONEN

Kommunikationsminister *Suvi Lindén*

RP 36/2009
KoUB 12/2009
RSv 90/2009

Nr 622

Lag

om ändring av 56 b § i lagen om överlåtelseskatt

Given i Nådendal den 7 augusti 2009

I enlighet med riksdagens beslut

ändras i lagen av den 29 november 1996 om överlåtelseskatt (931/1996) 56 b § 2 mom., sådant det lyder i lag 1085/2005, som följer:

56 b §

Elektronisk kommunikation och signering

— — — — — — — — — — — — — —

Deklarationer och andra handlingar som får lämnas in till skattemyndigheten på elektronisk väg och som ska signeras ska certifieras med en avancerad elektronisk signatur som avses i lagen om stark autentisering och elektroniska signaturer (617/2009) eller på något annat godtagbart sätt.

— — — — — — — — — — — — — —

Denna lag träder i kraft den 1 september 2009.

Nådendal den 7 augusti 2009

Republikens President

TARJA HALONEN

Kommunikationsminister *Suvi Lindén*

RP 36/2009
KoUB 12/2009
RSv 90/2009

Nr 623

Lag

om ändring av 93 a § i lagen om beskattningsförfarande

Given i Nådendal den 7 augusti 2009

I enlighet med riksdagens beslut

ändras i lagen av den 18 december 1995 om beskattningsförfarande (1558/1995) 93 a § 2 mom., sådant den lyder i lag 1079/2005, som följer:

93 a §

Elektronisk kommunikation och signering

— — — — — — — — — — — — — —

Deklarationer och andra handlingar som får lämnas in till skattemyndigheten på elektronisk väg och som ska signeras ska certifieras med en avancerad elektronisk signatur som avses i lagen om stark autentisering och elektroniska signaturer (617/2009) eller på något annat godtagbart sätt.

— — — — — — — — — — — — — —

Denna lag träder i kraft den 1 september 2009.

Nådendal den 7 augusti 2009

Republikens President

TARJA HALONEN

Kommunikationsminister *Suvi Lindén*

RP 36/2009
KoUB 12/2009
RSv 90/2009

Nr 624

Lag

om ändring av 6 a § i lagen om förskottsuppbörd

Given i Nådendal den 7 augusti 2009

I enlighet med riksdagens beslut

ändras i lagen av den 20 december 1996 om förskottsuppbörd (1118/1996) 6 a § 2 mom., sådant det lyder i lag 1082/2005, som följer:

6 a §

Elektronisk kommunikation och signering

— — — — — — — — — — — — — —

Deklarationer och andra handlingar som får lämnas in till skattemyndigheten på elektronisk väg och som ska signeras ska certifieras med en avancerad elektronisk signatur som avses i lagen om stark autentisering och elektroniska signaturer (617/2009) eller på något annat godtagbart sätt.

— — — — — — — — — — — — — —

Denna lag träder i kraft den 1 september 2009.

Nådendal den 7 augusti 2009

Republikens President

TARJA HALONEN

Kommunikationsminister *Suvi Lindén*

RP 36/2009
KoUB 12/2009
RSv 90/2009

FÖRFS/ELEKTRONISK VERSION

Nr 625

Lag

om ändring av 11 § i blodtjänstlagen

Given i Nådendal den 7 augusti 2009

I enlighet med riksdagens beslut
ändras i blodtjänstlagen av den 1 april 2005 (197/2005) 11 § som följer:

11 §

Uppgifter som hänför sig till blodgivare

Den som ger blod och blodkomponenter ska före blodgivningen ges nödvändiga upplysningar som hänför sig till blodgivningen samt de uppgifter som avses i 24 § i personuppgiftslagen (523/1999). Blodgivaren ska informeras om sekretessen i fråga om uppgifterna. Av blodgivaren ska begäras identifieringsuppgifter, sådana uppgifter om hälsotillståndet som är av betydelse när det gäller att bedöma blodgivarens lämplighet samt blodgivarens egenhändiga underskrift eller en avancerad elektronisk signatur enligt lagen om stark autentisering och elektroniska signaturer (617/2009). Läkemedelsverket kan utfärda närmare föreskrifter om den information som ska ges till och inhämtas från blodgivare.

Denna lag träder i kraft den 1 september 2009.

Nådendal den 7 augusti 2009

Republikens President
TARJA HALONEN

Kommunikationsminister *Suvi Lindén*

RP 36/2009
KoUB 12/2009
RSv 90/2009

UTGIVARE: JUSTITIEMINISTERIET

Nr 617—625, 3 ark

EDITA PRIMA AB, HELSINGFORS 2009 EDITA PUBLISHING AB, HUVUDREDAKTÖR JARI LINHALA ISSN 1456-9663