Uppförandekoder för förtroendenätet för identifieringstjänster

Transport- och kommunikationsverkets rekommendation

216/2022 S

Innehåll

1 Inledning och syfte med uppförandekoderna

Dessa uppförandekoder och bilagan om dataskydd kompletterar lagen, förordningen och Transport- och kommunikationsverket Traficoms lagbaserade tekniska föreskrifter om stark autentisering och förtroendenätet för leverantörer av identifieringstjänster.

Uppförandekoderna har från början tagits fram i samverkan mellan myndigheter och representanter för näringslivet i arbetsgruppen Identifiering och betrodda tjänster. Arbetsgruppen har tillsatts av Kommunikationsverket och exempelvis banker, teleföretag och Befolkningsregistercentralen (i dag Myndigheten för digitalisering och befolkningsdata) har varit representerade i gruppen. Den aktuella versionen har utfärdats i samarbetsgruppen för förtroendenätet som är tillsatt av Transport- och kommunikationsverket. Uppförandekoderna är juridiskt sett Transport- och kommunikationsverkets rekommendation.

Genom ändring (139/2015) av lagen om stark autentisering och betrodda elektroniska tjänster (617/2009, nedan benämnd autentiseringslagen) [1] utfärdades bestämmelser om uppbyggnad av ett förtroendenät för identifieringstjänster. Målet för förtroendenätet är att främja både utbudet på marknaden av allmänt tillgängliga identifieringstjänster som till användbarheten och säkerheten är avancerade och att främja säkerheten i den elektroniska ärendehanteringen. Via nätverket kan olika identifieringsverktyg förmedlas till tjänster för ärendehantering genom enhetliga tekniska och administrativa arrangemang. Närmare bestämmelser om förtroendenätets administrativa praxis, tekniska gränssnitt och administrativa ansvar finns i statsrådets förordning om förtroendenätet för leverantörer av tjänster för stark autentisering (169/2016, nedan benämnd förordningen om förtroendenätet) [2].

År 2019 gjordes betydande ändringar i bestämmelserna i autentiseringslagen (lag 412/2019) som gäller verksamheten i förtroendenätet. De nya bestämmelserna anger mera detaljerat än tidigare de leveransvillkor för tillträdesrätt som leverantören av identifieringstjänst ska upprätta och de metoder med vilka nyttjanderätten beviljas. Med anledning av dessa ändringar har uppförandekoderna och bilagan uppdaterats år 2022. I uppdateringen beaktades lagändringarna som trädde i kraft år 2019 och för bilagans del EU:s allmänna dataskyddsförordning. Syftet med uppförandekoderna är att beskriva de gemensamma målen, principerna och åtgärderna för förtroendenätets verksamhet, för att personer ska kunna identifieras i tjänsterna för ärendehantering på ett tillförlitligt och effektivt sätt oberoende av på vilket sätt företag som ingår i förtroendenätet har organiserat sin verksamhet. Syftet med uppförandekoderna är att göra det lättare att ingå avtal inom förtroendenätet.

Uppförandekoderna beskriver på en allmän nivå olika avtalsteman och den relevanta lagstiftningen om dem. Koderna innefattar också praxis som utifrån diskussioner med branschen konstaterats vara bra och som kan utnyttjas vid avtal. Uppförandekoderna och bilagan om dataskydd kan bifogas ett avtal eller hänvisas till i avtalet. Till innehållet är uppförandekoderna inte uttömmande. Dessutom kan avtalsparterna inkludera andra villkor i avtalen. I sina avtal ska parterna naturligtvis också beakta andra bestämmelser som styr verksamheten för medlemmarna i förtroendenätet, till exempel konsumentskydds- och konkurrensrätten, som på grund av den omfattande författningsmiljön inte behandlas i sin helhet i anvisningen. Det är inte Transport- och kommunikationsverket utan konsumentombudsmannen och

Konsument- och konkurrensverket som övervakar att konsumentskyddslagen och konkurrenslagen följs.

1.1 Rekommendationens versioner

Rekommendationen kompletteras och ändras vid behov. I så fall förblir rekommendationens nummer 216 oförändrat, medan datumet ändras och årtalet också vid behov. De nya versionerna av rekommendationen anges i tabellen nedan.

Version av rekommendationen och datum	Ändringar
Publicerad rekommendation 216/2017 S 3.4.2017	Den första utfärdade versionen
Korrigerad version av rekommendation 216/2017 S 3.7.2017 och den första versionen av dataskyddsbilagan	Den andra utfärdade versionen
Rekommendation 216/2022 6.6.2022 och den andra versionen av dataskyddsbilagan	Den tredje utfärdade versionen

Gällande rekommendation publiceras på Transport- och kommunikationsverkets webbplats på https://www.kyberturvallisuuskeskus.fi/sv/var-verksamhet/reglering-och-tillsyn/elektronisk-identifiering

2 Lagstiftning och föreskrifter som har samband med ämnet

Autentiseringslagens 12 a § om förtroendenätet tillämpades första gången den 1 maj 2017. Förordningen om förtroendenätet utfärdades den 10 mars 2016, och även den tillämpas från och med den 1 maj 2017. De ändringar som gjordes i autentiseringslagen med anledning av EU:s eIDAS-förordning trädde i kraft den 1 juli 2016, och Kommunikationsverkets föreskrift 72/2016 M om elektronisk identifiering och betrodda elektroniska tjänster utfärdades den 2 november 2016. Föreskriften ersattes genom föreskrift 72 A/2018 som utfärdades den 14 maj 2018 och genom föreskrift 72 B/2022 som utfärdades den första juni 2022 (nedan föreskrift 72 B eller M72 B) [3].

Den så kallade eIDAS-förordningen (EU) 910/2014 [4], som Europaparlamentet och rådet utfärdade den 23 juli 2014, ska också beaktas i den starka autentiseringen. Förordningen innefattar villkor enligt vilka medlemsstaterna erkänner de medel för elektronisk identifiering av fysiska och juridiska personer som omfattas av ett sådant system för elektronisk identifiering som en annan medlemsstat har anmält.

I eIDAS-förordningen och kommissionens genomförandeförordning (EU) 2015/1502 (nedan LoA-genomförandeförordning) [5], som preciserar eIDAS, fastställs tre tillitsnivåer för identifiering. Nivåerna beaktas i autentiseringslagen på så sätt att nivåerna väsentlig och hög anses som stark autentisering. Därutöver gäller det att i viss utsträckning beakta beredskapen till gränsöverskridande identifieringsförmedling, som behandlas i kommissionens genomförandeförordning (EU) 2015/1501 [6]. Enligt 42 c § i autentiseringslagen ska Myndigheten för digitalisering och befolkningsdata upprätthålla den nationella noden PEPS (Pan-European Proxy Server). PEPS är inte en del av förtroendenätet.

I oklara situationer kan tillämpningsordningen för normerna beskrivas på följande sätt:

1. eIDAS (i situationer där den lämpar sig för den aktuella situationen) och eventuella andra EU:s förordningar som gäller frågan
2. Autentiseringslagen och eventuella andra nationella lagar som gäller frågan
3. Statsrådets förordning om förtroendenätet
4. Transport- och kommunikationsverkets föreskrift 72 B
5. Identifieringstjänstleverantörens principer för identifiering
6. Avtal mellan leverarantören av identifieringsverktyg och leverantören av förmedlingstjänster
7. Transport- och kommunikationsverkets rekommendation om uppförandekoderna för förtroendenätet.

3 Definitioner

Definitionerna i uppförandekoderna bygger på autentiseringslagen, förordningen om förtroendenätet och eIDAS-förordningen. Nya definitioner har utarbetats om sådana saknas i bestämmelserna.

Begrepp	***Källa och förklaring***
Tjänster för ärendehantering	En part som förlitar sig på en elektronisk identifiering
Tillitsnivån hög	Tillitsnivå hög ska inom ramen för ett system för elektronisk identifiering avse ett medel för elektronisk identifiering som ger en högre grad av tillförlitlighet avseende en persons påstådda eller styrkta identitet än tillitsnivån väsentlig, och definieras med hänvisning till tekniska specifikationer, standarder och förfaranden som avser detta, inbegripet tekniska kontroller, vilkas syfte är att förhindra risken för missbruk eller ändring av identiteten. (Artikel 8.2 i eIDAS-förordningen och kommissionens LoA-genomförandeförordning (EU) 2015/1502)
Tillitsnivån väsentlig	Tillitsnivå väsentlig avser inom ramen för ett system för elektronisk identifiering ett medel för elektronisk identifiering som ger en väsentlig grad av tillförlitlighet avseende en persons påstådda eller styrkta identitet, och definieras med hänvisning till tekniska specifikationer, standarder och förfaranden som avser detta, inbegripet tekniska kontroller, vilkas syfte är att väsentligt minska risken för missbruk eller ändring av identiteten. (Artikel 8.2 i eIDAS-förordningen och kommissionens LoA-genomförandeförordning (EU) 2015/1502)

Förtroendenät	Ett nät av de leverantörer av identifieringstjänster som har gjort en anmälan till Transport- och kommunikationsverket. (2 § i autentiseringslagen)
Den tekniska helheten för förtroendenätet	En teknisk verksamhetsmiljö, som utgörs av identifieringstjänster tillhandahållna av de leverantörer av identifieringstjänster som har gjort en anmälan till Transport- och kommunikationsverket, och där en elektronisk identifiering som bygger på förtroendenätet genomförs.
Tekniskt gränssnitt	Gränssnitt avser specifikationer och implementeringar som gäller dataöverföring mellan två olika system eller delar av systemen. (punkt 3.1 i M72 B) Tekniska gränssnitt är 1) gränssnittet mellan leverantörer av identifieringsverktyg, 2) gränssnittet mellan en leverantör av identifieringsverktyg och en leverantör av tjänster för förmedling av identifiering, 3) gränssnittet mellan en leverantör av tjänster för förmedling av identifiering och en part som förlitar sig på identifieringstjänsterna. (1 § i förordningen om förtroendenätet)
Identifieringstjänst	Varje avtalsparts tjänst som avtalspartens kunder ansluter sig till och som är kompatibel med den tekniska helheten för förtroendenätet. Avtalsparten underhåller sin identifieringstjänst och kan fungera som leverantör av identifieringsverktyg och/eller som tjänst för identifieringsförmedling för sina egna kunder. Avtalsparten kommersialiserar och prissätter på egen hand sin tjänst som använder den tekniska helheten för förtroendenätet till tjänsterna för ärendehantering och ingår egna avtal med dessa.
Leverantör av identifieringstjänster	Leverantör av tjänster för identifieringsförmedling eller leverantör av identifieringsverktyg (2 § i autentiseringslagen)
Principer för identifiering	Leverantörer av identifieringstjänster ska ha principer för identifiering som närmare anger hur tjänsteleverantören uppfyller de skyldigheter som anges i denna lag. (14 § i autentiseringslagen)
Identifieringstransaktion	Transaktionskedja, där innehavare av ett identifieringsverktyg identifierar sig i den förlitande partens tjänst (tjänst för ärendehantering) och där tjänsten för ärendehantering använder en eller flera avtalsparters identifieringstjänst för att utreda identiteten

	eller någon annan egenskap hos innehavaren av identifieringsverktyget.
Identifieringsverktyg	Ett medel för elektronisk identifiering enligt artikel 3.2 i eIDAS-förordningen, det vill säga en materiell och/eller immateriell enhet som innehåller person-identifieringsuppgifter och som används för autentisering för nättjänster. (2 § i autentiseringslagen)
Innehavare av identifieringsverktyg	En fysisk person som enligt avtal har fått ett identifieringsverktyg av en leverantör av identifieringstjänsten. (2 § i autentiseringslagen)
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. (2 § i autentiseringslagen)
Leverantör av tjänster för identifieringsförmedling	En tjänsteleverantör som förmedlar identifieringstransaktioner baserade på stark autentisering till en part som förlitar sig på en elektronisk identifiering. (2 § i autentiseringslagen)
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 eIDAS-förordningen eller tillitsnivån hög enligt artikel 8.2 c i den förordningen. (2 § i autentiseringslagen och artikel 8 i eIDAS)

4 Förtroendenätets ömsesidiga avtal

4.1 Avtalsparter

Avtalsparter kan vara de leverantörer av identifieringstjänster som i enlighet med 10 § och 12 § i autentiseringslagen är införda i Transport- och kommunikationsverkets register över leverantörer av tjänster för stark autentisering.

Uppförandekoderna fastställer inga villkor för avtal om användning av den tekniska helheten för förtroendenätet mellan avtalsparternas innehavare av identifieringsverktyg och tjänsterna för ärendehantering.

Leverantörer av identifieringstjänster, dvs. leverantörer av identifieringsverktyg och leverantörer av tjänster för identifieringsförmedling, ingår sinsemellan avtal om verksamheten i förtroendenätet samt om sammankopplingen av inledande identifiering.

4.2 Skyldighet att ingå avtal

Enligt 3 § 1 mom. i förordningen om förtroendenätet (ändrad genom statsrådets förordning 1212/2018) ska en leverantör av identifieringstjänster som hör till förtroendenätet i enlighet med samarbetsskyldigheten enligt 12 a § 2 och 4 mom. i autentiseringslagen förhandla och avtala med andra leverantörer av identifieringstjänster om omständigheter som är nödvändiga för genomförande av förtroendenätet.

Enligt 2 § 1 mom. 5 punkten i förordningen om förtroendenätet svarar en leverantör av identifieringstjänster som hör till förtroendenätet i förtroendenätet för utarbetandet och förvaltningen av sådana avtal i anslutning till förtroendenätet som avses i 3 § 1 mom.

Enligt 12 a § 2 mom. i autentiseringslagen ska en leverantör av identifieringsverktyg erbjuda leverantörer av tjänster för identifieringsförmedling tillträdesrätt till sina identifieringstjänster (avtalstvång) så att leverantörerna kan förmedla identifieringstransaktioner till en part som förlitar sig på en elektronisk identifiering. En leverantör av identifieringsverktyg ska upprätta leveransvillkor för tillträdesrätt till sin identifieringstjänst och tillämpa dem vid ingående av avtal med leverantörer av tjänster för identifieringsförmedling. Villkoren för tillträdesrätten ska vara förenliga med autentiseringslagen samt rimliga och icke-diskriminerande. När man bedömer rimlighet och icke-diskriminering är det väsentliga att leverantörer av tjänster för identifieringsförmedling som befinner sig i en liknande situation behandlas lika i villkoren (RP 264/2018). Såsom det framgår av regeringens proposition RP 264/2018 bör samma villkor tillhandahållas alla i förtroendenätet, vilket i praktiken innebär att bara en uppsättning villkor upprättas.

Leverantören av identifieringsverktyg ska godkänna en begäran av leverantören av tjänster för identifieringsförmedling om att ingå ett avtal enligt leveransvillkoren samt bevilja tillträdesrätt till identifieringstjänsten utan dröjsmål och senast inom en månad efter att begäran har gjorts. Leverantören av identifieringsverktyg kan vägra ingå avtal endast om leverantören av tjänster för identifieringsförmedling handlar i strid med denna lag eller de bestämmelser eller föreskrifter som utfärdats med stöd av den eller om det finns andra vägande skäl för vägran. Ett exempel på vägande skäl är att en leverantör av förmedlingstjänster på ett väsentligt sätt agerar i strid med något syfte som anges i leverantörens principer för identifiering (förmedlingsprinciper) (RP 264/2018). Giltiga grunder för vägran kan också bestå av andra synnerligen vägande och motiverade skäl, t.ex. allvarlig överträdelse av ett avtal mellan parterna eller sanktioner.

Innan leverantören av identifieringsverktyget helt avstår från ett avtal ska man först utreda om det finns andra rimliga mekanismer som tryggar parternas rättigheter så att de kan ingå avtal.

> Om en leverantör av identifieringsverktyg till exempel av giltigt skäl tvivlar på betalningsförmågan för tjänsterna för identifieringsförmedling på grund av en tidigare försummelse av betalning, kan en skälig säkerhet krävas i syfte att säkerställa att avtalsskyldigheterna uppfylls.

Vid vägran att ingå ett avtal ska leverantören av identifieringsverktyg agera jämlikt och icke-diskriminerande. Skälet till vägran ska vara vägande för att det giltigt ska kunna anses gå före avtalstvånget, som regleringen utgår från.

Avtalsparterna kan kontakta Transport- och kommunikationsverket om de har för avsikt att vägra ingå avtal eller om de inte kan nå enighet om avtalets innehåll.

Transport- och kommunikationsverket kan kalla avtalsparterna för en förhandling. Avsikten är att i första hand lösa meningsskiljaktigheter genom förhandling. Transport- och kommunikationsverket deltar inte i prisförhandlingar.

I sista hand kan Transport- och kommunikationsverket som myndighet som utövar tillsyn över autentiseringslagen genom ett tillsynsbeslut fastslå om de villkor eller krav som avtalsparterna har fastställt genom förhandlingar till vissa delar står i strid med skyldigheterna i reglerna eller praxisen i branschen. Riktlinjerna i denna rekommendation används, om det fattas ett tillsynsbeslut om frågan. Transport- och kommunikationsverket kan genom sitt beslut ålägga avtalsparterna att avstå från de krav som strider mot reglerna eller från andra oskäliga krav som inte har ett motiverat samband med genomförandet av identifieringstjänsten (12 a § och 12 b § i autentiseringslagen och 3 § i förordningen om förtroendenätet). Transport- och kommunikationsverkets beslut kan förenas med tvångsmedel enligt 45 § i autentiseringslagen. Ändring i Transport- och kommunikationsverkets tillsynsbeslut kan sökas i förvaltningsdomstolen. Dessutom kan Konkurrens- och konsumentverket utgående från konkurrenslagstiftningen utvärdera vägran att ingå avtal.

Tjänster för identifieringsförmedling har inget lagstadgat tvång att förmedla alla identifieringsverktyg, men syftet med lagen är att aktörer som tillhandahåller tjänster för ärendehantering ska kunna anskaffa identifieringstjänster från en enda tjänst för identifieringsförmedling.

En och samma tjänsteleverantör kan fungera som både leverantör av identifieringsverktyg och leverantör av tjänster för identifieringsförmedling.

> Om en leverantör av identifieringsverktyg också fungerar som leverantör av tjänster för identifieringsförmedling i fråga om sitt eget verktyg, till exempel tillhandahåller verktyget vidare till en tjänst för ärendehantering utifrån ett gammalt avtal, är det fråga om förmedlingsverksamhet. Även då ska verktyget tillhandahållas för förmedling till alla andra tjänster för identifieringsförmedling, men aktören är inte tvungen att förmedla andra identifieringsverktyg utöver sitt eget verktyg.

En ny leverantör av identifieringstjänster kan be en annan leverantör av identifieringstjänster ingå avtal på de villkor som beskrivs i autentiseringslagen, förordningen om förtroendenätet och dessa uppförandekoder, när den nya leverantören har förts in i Transport- och kommunikationsverkets register enligt autentiseringslagen och när dess identifieringstjänst är tekniskt färdig så att den kan anslutas till förtroendenätets tekniska helhet. Avtalsförhandlingar kan vid behov också inledas före registreringen.

4.3 Frågor som tillhör identifieringstjänstleverantörernas ansvar och förtroendenätets samarbetsansvar

Förtroendenätets administrativa ansvar fastställs i 2 § i förordningen om förtroendenätet och i 12 a § i autentiseringslagen (speciellt 3 och 4 mom.).

Avtalsparterna skapar tillsammans med andra leverantörer av identifieringstjänster en teknisk helhet för förtroendenätet via vilken innehavare av identifieringsverktyg kan identifiera sig i tjänsterna för ärendehantering.

Avtalsparterna svarar själva för utveckling av de tjänster som ska anslutas till den tekniska helheten och fastställer på egen hand användarvillkoren och andra villkor samt priserna för sina egna kunder i de avtal som de ingår med kunderna.

4.4 Principer för identifiering och information om ändringar i dem

Enligt 14 § i autentiseringslagen ska leverantörer av identifieringstjänster ha principer för identifiering vars minimiinnehåll specificeras i 14 § 2 mom.

Enligt 10 § 3 mom. i autentiseringslagen ska leverantören av identifieringstjänster utan dröjsmål skriftligen underrätta Transport- och kommunikationsverket om ändringar i principerna för identifiering.

Transport- och kommunikationsverket för ett offentligt register över leverantörer av identifieringstjänster på sina webbsidor. I registret finns en länk till varje leverantörs principer för identifiering samt uppgift om det datum då principerna har trätt i kraft.

Leverantörerna av identifieringstjänster underrättar Transport- och kommunikationsverket om ändringar i principerna för identifiering när de fattat beslutet om ändringen, eller senast när principerna för identifiering har publicerats.

4.5 Tillitsnivåer för identifiering

Leverantörer av identifieringsverktyg och leverantörer av tjänster för identifieringsförmedling kan i förtroendenätet tillhandahålla identifieringstjänster på tillitsnivån väsentlig eller hög eller på båda nivåerna.

Vid förmedling av en identifieringstransaktion specificerar identifieringsförmedlingstjänsten för leverantören av identifieringsverktyg på vilken nivå identifieringen ombes. Tjänsten för ärendehantering beslutar om identifieringsnivån och ber om en förmedlingstjänst på den nivån. Identifieringen på tillitsnivån väsentlig kan också ske genom en identifieringstjänst på tillitsnivån hög.

4.6 Tekniska gränssnitt och minimiuppsättning identifieringsuppgifter

Förtroendenätets tekniska gränssnitt fastställs i 1 § 1 mom. i förordningen om förtroendenätet. Enligt 1 § 2 mom. i förordningen ska en leverantör av identifieringstjänster som hör till förtroendenätet i vartdera av de gränssnitt som avses i 1 mom. 1 punkten (gränssnittet mellan leverantörer av identifieringsverktyg) och 2 punkten (gränssnittet mellan en leverantör av identifieringsverktyg och en leverantör av tjänster för förmedling av identifiering) tillhandahålla minst ett tekniskt gränssnitt som baserar sig på en allmänt tillämpad standard.

Minimiuppsättningen uppgifter som ska förmedlas i förtroendenätet fastställs i punkt 12 i Transport- och kommunikationsverkets föreskrift 72 B.

Enligt föreskrift 72 B kan leverantörer av identifieringsverktyg, leverantörer av tjänster för identifieringsförmedling och leverantörer av tjänster för ärendehantering avtala om sådana övriga egenskaper för gränssnitten mellan dem och sådana tillämpliga protokoll som inte fastställs i denna föreskrift (punkt 14.2).

De tillgängliga tekniska gränssnitten anges i leveransvillkor för tillträdesrätt till identifieringstjänsten. Avtalsparterna ska avtala om vilka fastställda gränssnitt de ska använda. Enligt promemorian Motivering till och tillämpning av föreskrift 72 B bör förtroendenätet använda SAML 2.0- eller Open ID Connect-protokollet och deras nationella profiler som Kommunikationsverket har publicerat som separata rekommendationer [7][8].

Avtalsparterna kan också fritt avtala om andra gränssnitt såvida det inte hindrar andra medlemmar i förtroendenätet från att bedriva verksamhet på de fastställda gränssnitten. I så fall får de gränssnitt som har fastställts i förtroendenätet inte

diskrimineras i förhållande till de övriga gränssnitt som tillhandahålls. Samarbetsgruppen för förtroendenätet bör informeras om ibruktagande av andra gränssnitt.

4.7 Information om störningar i informationssäkerheten, felsituationer, serviceavbrott och ändringar i förtroendenätet

4.7.1 Vilka situationer ska anmälas?

Enligt 16 § 1 mom. i autentiseringslagen *ska en leverantör av identifieringstjänster 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 Transport- och kommunikationsverket*.

Med stöd av 16 § 2 mom. i autentiseringslagen får leverantören av identifieringstjänster trots sekretessbestämmelserna underrätta alla medlemmar i förtroendenätet om hot och störningar som avses i 1 mom. samt om tjänsteleverantörer som skäligen kan misstänkas för att eftersträva orättmätig ekonomisk vinning, lämna betydelsefull osann eller vilseledande information eller behandla personuppgifter på ett olagligt sätt.

Enligt 2 § 1 mom. 4 punkten i förordningen om förtroendenätet *svarar en leverantör av identifieringstjänster som hör till förtroendenätet i förtroendenätet för att andra leverantörer av identifieringstjänster som hör till förtroendenätet utan ogrundat dröjsmål informeras om sådana störningar eller hot mot informationssäkerheten som inverkar på sådana tjänster som de tillhandahåller samt för utredningen av störningssituationer i förtroendenätet*.

Informationsskyldigheten mellan aktörerna i förtroendenätet gäller hot och störningar i informationssäkerheten, fel som påverkar funktionen och serviceavbrott samt ändringar som kan orsaka avbrott eller störningar. När informationströskeln fastställs ska hänsyn tas till på vilket sätt störningar, hot eller ändringar eventuellt påverkar den tjänst som den andra aktören i förtroendenätet tillhandahåller.

> Tröskeln bör vara låg till exempel när det gäller hot mot informationssäkerheten, såsom sårbarheter i programvaran, phishing-kampanjer eller överbelastningsangrepp, så att andra aktörer kan förbereda sig för situationen. Information om fel i funktionen ska lämnas åtminstone då de påverkar avtalsparternas tjänster.

I leveransvillkoren ska anges hur leverantören på förhand informerar om underhålls- och ändringsarbeten, såsom serviceavbrott, eller om att det finns ett på förhand fastställt tidsschema för serviceavbrotten. Information om ändringar i identifieringstjänsterna bör lämnas på samma sätt som för serviceavbrott, beroende på vilken risk för avbrott eller störningar eller oförväntade följder ändringen medför för andra aktörer i förtroendenätet. Serviceåtgärder och ändringar orsakar vanligen avbrott.

Avtalsparterna bör avtala om information om hot och störningar i informationssäkerheten, felsituationer och serviceavbrott så att övriga aktörer i förtroendenätet kan förbereda sig för situationerna och vidta nödvändiga förberedande eller korrigerande åtgärder.

4.7.2 Informationsrutiner

Avtalsparterna ska avtala om förfaranden för utlämnande av information, bland annat kontaktpersoner, kommunikationskanaler och informationstidpunkter. Informationssäkerheten i kommunikationskanalerna ska vara hög.

Avtalsparterna kan avtala om att kontaktuppgifter för information om störningar (också) ska lämnas i en sammanställning som är gemensam för förtroendenätet, som uppdateras gemensamt och som har avgränsats för detta ändamål.

Informationstidpunkterna bör sättas i relation till problemets art, allvar, omfattning och följder. God praxis är information om

- hot och störningar i informationssäkerheten, till exempel dataintrång, massiva överbelastningsangrepp, sårbarheter i informationssäkerheten, elektroniska identifieringsverktyg som har beviljats fel personer och motsvarande situationer som äventyrar integriteten i identifieringssystemet, omedelbart efter att problemet blivit känt, dock senast inom 24 timmar
- störningar eller hot mot informationssäkerheten, till exempel dataintrång som äventyrar sekretessen för personuppgifter, omedelbart efter att problemet blivit känt, dock senast inom 48 timmar
- fel som stör användningen av tjänsten, så snart som möjligt efter att felet har upptäckts
- serviceavbrott och ändringar, senast en vecka i förväg eller, om det senare blir känt när arbetet ska utföras, senast när det blir känt när arbetet ska utföras.

Inom ramen för samarbetsgruppen för förtroendenätet är det möjligt att utfärda gemensamma kommunikationsförfaranden som förtroendenätet följer i olika hot- och störningssituationer. Det rekommenderas starkt att förfarandena följs. I leveransvillkoren kan det bestämmas att man ska följa de gemensamma kommunikationsförfarandena.

4.7.3 Behandling av uppgifter om störningar, ändringar och transaktioner i förtroendenätet

Enligt 12 b § 5 mom. i autentiseringslagen *får en leverantör av identifieringstjänster använda sådan information om en annan leverantör av identifieringstjänster som den erhållit med stöd av 16 § endast för det ändamål för vilket informationen har lämnats till leverantören av identifieringstjänster. Uppgifterna får behandlas endast av den som arbetar hos eller för en leverantör av identifieringstjänster och som nödvändigt behöver uppgifterna i sitt arbete. Uppgifterna ska också annars behandlas så att affärshemligheter som tillhör en annan leverantör av identifieringstjänster inte röjs*.

De ovan beskrivna principerna om information om störningar gäller endast internt informationsutbyte i förtroendenätet. Avtalsparterna har inte rätt att till tjänster för ärendehantering, innehavare av identifieringsverktyg eller andra tredje parter lämna sådana konfidentiella uppgifter som parterna har fått som medlemmar i förtroendenätet.

Endast allmän information om att tjänsten inte är tillgänglig får förmedlas till tjänster för ärendehantering eller allmänheten när det gäller övriga aktörer i förtroendenätet.

Avtalsparterna kan avtala om att de på varandras vägnar informerar om störningar till tjänster för ärendehantering eller allmänheten, och till exempel om att de i anslutning till det ömsesidiga meddelandet specificerar vilka uppgifter som kan lämnas ut till tjänster för ärendehantering eller allmänheten. I så fall ska hänsyn dock tas till den tvingande lagstiftningen om informationsskyldigheten, bland annat 16 § i autentiseringslagen och dataskyddsförordningen.

Sekretessen mellan avtalsparterna får inte ha en negativ inverkan på konsumentens rätt att få information om vilken aktör konsumenten kan vända sig till för att åberopa sina lagstadgade rättigheter.

4.7.4 Samarbete för att utreda fel

Enligt 2 § 1 mom. 4 punkten i förordningen om förtroendenätet *svarar en leverantör av identifieringstjänster som hör till förtroendenätet i förtroendenätet för att andra leverantörer av identifieringstjänster som hör till förtroendenätet utan ogrundat dröjsmål informeras om sådana störningar eller hot mot informationssäkerheten som inverkar på sådana tjänster som de tillhandahåller samt för utredningen av störningssituationer i förtroendenätet*.

Enligt 24 § 5 mom. i autentiseringslagen *får leverantören av identifieringstjänster 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.*

Avtalsparterna ska samarbeta för att utreda fel och missbruk vid identifieringstransaktioner. Vid akuta störningar i informationssäkerheten eller fel skiljer sig utredningsförfarandet från utredning av fel och missbruk i efterhand. Avtalsparterna bör åtminstone avtala om kontaktuppgifter vid utredning av fel och missbruk om uppgifterna skiljer sig från dem som gäller vid skötsel av akuta situationer.

> Det gäller till exempel att utreda situationer där en person har både korrekta och inkorrekta identifieringsverktyg, eftersom personen har identifierats korrekt vid en inledande identifiering för en del verktyg och inkorrekt för andra verktyg. Fel identifieringsverktyg bör kunna tas bort från personen så att de korrekta identifieringsverktygen kan gälla fortsättningsvis. Enbart spärrning av identifieringsverktyg som bygger på personbeteckning fungerar inte i en sådan situation, utan det behövs samarbete i hela förtroendenätet.

4.7.5 Störningsanmälningar till myndigheten

Bestämmelser om störningsanmälningar till Transport- och kommunikationsverket finns i 16 § 1 mom. i autentiseringslagen, och närmare bestämmelser om sådana anmälningar finns i punkt 11 i Transport- och kommunikationsverkets föreskrift 72 B. Motiveringen till föreskriften innehåller tillämpningsanvisningar om anmälan. På ämbetsverkets webbplats finns en elektronisk blankett för anmälan om störningar.

Transport- och kommunikationsverket behandlar de uppgifter som verket har fått på anmälningarna i enlighet med lagen om offentlighet i myndigheternas verksamhet. Enligt 24 § 1 mom. i offentlighetslagen är bland annat affärshemligheter och uppgifter om säkerheten på nätet sekretessbelagda. Utlämnande av sekretessbelagda uppgifter kräver alltid samråd med och samtycke av den berörda personen eller att de lagstadgade kriterierna för utlämnande uppfylls. Vid intressekonflikter ska ärendet avgöras genom ett överklagbart förvaltningsbeslut.

4.8 Användbarhet

Autentiseringslagen och de bestämmelser som har utfärdats med stöd av autentiseringslagen varken föreskriver eller fastställer särskilda krav på tjänsternas användbarhet, med undantag för kravet i 25 § 2 mom. i autentiseringslagen gällande spärrtjänst. Enligt momentet *ska leverantören av identifieringsverktyg se till att det är möjligt att när som helst göra en anmälan enligt 1 mom*.

Enligt 12 b § 5 punkten i autentiseringslagen ska leverantören i leveransvillkoren ange vilken servicenivå som erbjuds. Vid genomförande av avtalspartens identifieringstjänst har användbarheten i den tekniska helheten av förtroendenätet stor betydelse.

Om inget annat förutsätts i bestämmelserna (bl.a. tillgänglighet till spärrlisttjänster), kan leverantören av identifieringsverktyget ange sin servicenivå närmare i sina leveransvillkor. Vid angivandet av servicenivån ska leverantören av identifieringsverktyget dock behandla alla avtalspartner jämlikt och icke-diskriminerande. Icke-diskrimineringskravet innebär att alla förmedlingstjänster, även leverantörens egen, ska tillhandahållas samma servicenivå (RP 264/2018).

Ändringar i identifieringstjänsterna kan påverka de tjänster som andra aktörer i förtroendenätet tillhandahåller. Leverantörer av identifieringstjänster ska enligt 12 a § 4 mom. genomföra underhålls-, ändrings- och informationssäkerhetsåtgärder på ett sådant sätt att åtgärderna innebär minsta möjliga olägenhet för identifieringstjänsternas övriga leverantörer, användare och förlitande parter.

Avtalsvillkoren för service- och ändringsåtgärder ska vara så rimliga som möjligt för konsumenterna. Det är inte Transport- och kommunikationsverket utan konsumentombudsmannen som övervakar att konsumentskyddslagen följs.

4.9 Avgifter för användning av den tekniska helheten för förtroendenätet

I den tekniska helheten för förtroendenätet förmedlas identifieringstransaktioner mellan avtalsparterna. Avtalsparterna betjänar sina egna innehavare av identifieringsverktyg och de ärendehanteringstjänster som är deras avtalsparter.

Mellan avtalsparterna beviljas tillträdesrätt till identifieringstjänster, och leverantören av förmedlingstjänsten förmedlar identifieringstransaktioner som baserar sig på ett identifieringsverktyg som en annan avtalspart beviljat. I så fall kan en leverantör av identifieringsverktyg ta ut en avtalad avgift av en avtalspart som tjänsten för ärendehantering är kund hos. Bestämmelser om den ersättning som tas ut för en förmedlad identifieringsuppgift finns i 12 c § i autentiseringslagen. Leverantörer av tjänster för identifieringsförmedling ska betala en ersättning på högst 3 cent per förmedlad identifieringstransaktion för tillträdesrätt till identifieringstjänsten. Ersättningen omfattar alla personidentifieringsuppgifter som gäller det elektroniska identifieringsverktyget. Grunden för prissättningen ska vara densamma för alla parter (RP 264/2018). Även avtal med ett fast pris är möjliga, om man säkerställer att medelpriset för identifieringstransaktionerna inte överskrider det lagstadgade maximipriset. Kravet på skäligt pris och icke-diskriminering gäller också denna typ av prissättning och grunderna för prissättningen ska anmälas i leveransvillkoren. Det högsta priset gäller endast en uppgift som leverantören av identifieringstjänster förmedlar till den egentliga leverantören av tjänster för identifieringsförmedling. Däremot när identifieringstjänsten levererar identifieringsdata utanför förtroendenätet, till en tjänst för ärendehantering som är direkt avtalspart till förtroendenätet, är takpriset inte i kraft, utan då tillämpas det pris som parterna har kommit överens om.

Enligt 1 § 2 mom. i förordningen om förtroendenätet kan leverantörer av identifieringstjänster som hör till förtroendenätet avtala om det gränssnitt som behövs för förmedlingen av debiteringen för en identifieringsuppgift som avses i 12 a § 3 mom. i autentiseringslagen eller om något annat gränssnitt som behövs i förtroendenätets verksamhet.

Avtalsparterna kan tillhandahålla varandra tjänster för att skapa identifieringsverktyg (s.k. kedjor av inledande identifiering). I så fall använder avtalsparten ett identifieringsverktyg som beviljats av den andra avtalsparten för att ge det nya identifieringsverktyget till innehavare av identifieringsverktyget. Det är möjligt att avtala om kedjor av inledande identifiering i samma eller olika avtal än om förmedling av identifiering.

Avtalsparterna utvecklar och kommersialiserar sina egna identifieringstjänster samt fastställer på egen hand användarvillkoren och övriga avtalsvillkor samt priserna för sina egna kunder i de avtal som de ingår med kunderna.

4.10 Begränsningar för användning av identifieringsverktyg

Leverantörer av identifieringsverktyg får införa både avtalsbaserade och tekniska begränsningar för användning av identifieringsverktyg (18 § i autentiseringslagen). Leverantören av identifieringstjänster ska dock bemöta sina kunder på ett icke-diskriminerande sätt och dem som ansöker om identifieringsverktyg jämlikt när avtalet ingås (20 § i autentiseringslagen). Avtalsparterna ska avtala om eventuella begränsningar för användning av verktyg i de avtal som de ingår sinsemellan. Leverantören av identifieringstjänster ska se till att alla parter känner till hindren eller begränsningarna eller att de är lätta att upptäcka. Hinder och begränsningar får inte gälla enskilda tjänsteleverantörer och de får inte vara beroende av vilken leverantör av tjänster för identifieringsförmedling som förmedlar identifieringstransaktionen.

Lagstiftarens strävan är att allmänt och brett tillgängliga identifieringsverktyg som lämpar sig för vilken ärendehantering och kommunikation som helst ska införas på marknaden. Identifieringsverktyg kan betraktas som basservice i informationssamhället (se bl.a. KoUB 12/2009 och KoUB 33/2014). När det gäller begränsningar som avviker från kriteriet på allmän tillgänglighet ska det finnas ett motiverat behov och begränsningarna får inte användas i större utsträckning än vad som står i rätt proportion till tillgodoseendet av det motiverade behov som berättigar till en avvikelse. Begränsningar av användningen får inte avsiktligen utgöra ett hinder för att bedriva laglig affärsverksamhet.

Principerna för behandling av personuppgifter har specificerats i bilagan om dataskydd.

4.11 Användning av varumärken

I leveransvillkoren ska man ange villkor för användning av varumärken och andra immateriella rättigheter. Tjänsterna för identifieringsförmedling har rätt att avtala med tjänsterna för ärendehantering om att de varumärken för identifieringsverktyg som används i tjänsterna för ärendehantering visas i tjänsterna för ärendehantering.

Logotyperna ska visas i samma form som innehavaren av varumärket själv visar dem i eller i den form som krävs i leveransvillkoren. Vid användning av varumärken ska all lagstiftning som gäller användning av varumärken iakttas.

Leverantörerna av identifieringsverktyg har rätt att kräva att leverantörerna av tjänster för identifieringsförmedling i sina avtal ser till att tjänsterna för ärendehantering inte på ett obehörigt och vilseledande sätt använder identifieringstjänstleverantörens varumärke för att skaffa sig mer goodwill. Ett varumärke som tillhör leverantören av identifieringsverktyg får endast användas vid identifieringstransaktioner. Varumärket får inte användas på de sätt som räknas upp i 14 § i varumärkeslagen (7/1964, ändrad genom 616/2016).

4.12 Ansvarsfördelning mellan avtalsparterna och skadestånd

Uppförandekoderna behandlar endast relationer mellan medlemmar i förtroendenätet och därför enbart de skadeståndsfrågor som gäller de relationerna. Vid genomförande av identifieringstransaktioner finns det flera olika relationer mellan olika aktörer och en stor del av relationerna omfattas inte av uppförandekoderna. Dåvarande Kommunikationsverket har låtit professor Olli Norros göra en juridisk utredning om skadeståndsjuridiska frågor gällande förtroendenätet (Kommunikationsverkets publikation 004/2016 J [9]). Avtalsparterna kan utnyttja utredningen vid upprättande av avtal.

Uppförandekoderna omfattar inte följande relationer som avtalsparterna ändå bör beakta när de planerar sin verksamhet och ingår avtal:

1. leverantör av identifieringsverktyg – innehavare av identifieringsverktyg
2. den som utför en sekundär inledande identifiering (sammankopplar den inledande identifieringen) – innehavare av identifieringsverktyg
3. leverantör av identifieringsverktyg – utomstående skadelidande
4. leverantör av tjänster för identifieringsförmedling – innehavare av identifieringsverktyg
5. leverantör av tjänster för identifieringsförmedling – tjänster för ärendehantering
6. leverantör av identifieringsverktyg – tjänster för ärendehantering

4.12.1 Avtalsparternas ansvar vid förmedling av identifiering

Avtalsparterna svarar för att de skyldigheter som fastställs i autentiseringslagen och annan lagstiftning samt parternas egna principer för identifiering fullgörs.

Utgångspunkten är att skadeståndsansvaret och regressrätten i förtroendenätet bygger på avtal. Deltagandet i förtroendenätet medför inte till exempel gemensamt ansvar för skador som inträffar i nätet.

När avtal upprättas bör åtminstone följande tas upp särskilt:

1. skador i anslutning till avbrott och störningar i tjänsterna
2. skador i anslutning till identitetsmisstag eller -stölder och
3. andra skador som hänför sig till integritet eller tillförlitlighet.

I avtalet kan man avtala om ansvarsbegränsningar och maximibeloppet för skadeståndsansvar i euro inom ramen för lagstiftningen. Avtalsparterna ska beakta tillämpningen av konsumentskyddsbestämmelserna, och parternas ömsesidiga avtal får inte försvaga de lagstadgade rättigheterna för konsumenter som är innehavare av identifieringsverktyg. En konsument är inte en part i förtroendenätets avtal men avtalen kan ha en indirekt inverkan på konsumentens rättigheter och detta ska beaktas.

I avtalet kan man avtala om att ansvaret för skador, där skadevållaren inte obestridligt kan fastslås, fördelas mellan avtalsparterna i lika delar.

4.12.2 Ansvar vid sammankoppling av inledande identifiering

Enligt 17 § 5 mom. i autentiseringslagen bär den leverantör av identifieringsverktyg som litar på en tidigare inledande identifiering ansvaret i förhållande till den skadelidande om den inledande identifieringen är felaktig. I paragrafens 6 mom. sägs att om en leverantör av identifieringsverktyg som litar på en tidigare inledande identifiering blir ansvarig för en skada med stöd av 5 mom., har leverantören rätt att få ersättning för sin skada av den leverantör av identifieringsverktyg som begått felet vid den inledande identifieringen, om inte den sistnämnda leverantören visar att skadan inte har berott på uppsåt eller grov oaktsamhet.

Det är möjligt för leverantörer av identifieringsverktyg att i leveransvillkoren meddela villkor för begränsning och fördelning av ansvaret mellan leverantörerna till den del det lagen inte kräver det.

4.13 Dataskydd

Avtalsparterna iakttar gällande lagar och förordningar om dataskydd samt den bifogade bilagan om dataskydd *Behandling av personuppgifter i förtroendenätet för elektronisk identifiering.*

4.14 Sekretess

Uppförandekoderna är offentliga.

Enligt 12 b § i autentiseringslagen ska en leverantör av identifieringsverktyg offentliggöra leveransvillkoren för tillträdesrätt till sin identifieringstjänst samt annan information som är relevant för överlåtelse av tillträdesrätt och identifieringstjänsternas kompatibilitet på sin webbplats. Uppgifter som ska offentliggöras innebär bl.a. en beskrivning av de tekniska gränssnitten och testarrangemangen för förmedlingen av identifieringstransaktionerna till den del de inte innehåller affärshemligheter eller uppgifter som äventyrar informationssäkerheten.

Enligt 12 a § 5 mom. i autentiseringslagen får en leverantör av identifieringstjänster använda sådan information om en annan leverantör av identifieringstjänster som den erhållit i samband med överlåtelse av tillträdesrätt eller med stöd av 16 § (störningsanmälningar) endast för det ändamål för vilket informationen har lämnats till leverantören av identifieringstjänster.

4.15 Tillfälliga avbrott i förmedlingen av identifieringstransaktioner

En leverantör av identifieringsverktyg kan avbryta förmedlingen av identifieringstransaktioner till sina egna innehavare av identifieringsverktyg från en sådan tjänst för identifieringsförmedling som allvarligt eller trots anmärkningar underlåter att uppfylla de skyldigheter som lagstiftningen ålägger eller som fastställs i parternas ömsesidiga avtal. Ett avbrott kan också bygga på att tjänsten för identifieringsförmedling gör det omöjligt för leverantören av identifieringsverktyg att uppfylla de skyldigheter som har fastställts i lagstiftningen eller avtalet. Leverantören av identifieringsverktyg ska informera de övriga medlemmarna i förtroendenätet och Transport- och kommunikationsverket om avbrottet.

Enligt 12 b § 4 mom. andra meningen i autentiseringslagen får en leverantör av identifieringstjänster också tillfälligt utan en annan leverantörs samtycke avbryta tillhandahållandet av en identifieringstjänst eller begränsa dess användning, om det är nödvändigt för att underhålls-, ändrings- och informationssäkerhetsåtgärder ska kunna genomföras framgångsrikt.

4.16 Upphörande av avtal

Ett avtal upphör med uppsägning eller hävning eller om avtalsparterna gemensamt avtalar om upphörande av avtalet.

Skälet till uppsägning av ett avtal för en leverantör av identifieringsverktyg ska vara vägande för att det giltigt ska kunna anses gå före avtalstvånget, som regleringen utgår från. Avtal kan sägas upp av orsaker som ursprungligen kunde ha berättigat till att inte ingå avtal (se kap. 4.2) förutsatt att informationen inte fanns tillgänglig när avtalet ursprungligen träffades.

Omedelbar hävning av avtal ska endast i undantagsfall anses vara ett medel för att avsluta avtal. Ett avtal kan alltid hävas om Transport- och kommunikationsverket avregistrerar tjänsteleverantören i fråga i det register som avses i 12 § i autentiseringslagen.

I problemsituationer är det primära medlet alltid utredning av ärendet och i allvarliga situationer ett tillfälligt avbrytande av förmedlingen av identifieringstransaktioner.

Även om ett avtal mellan leverantörer av identifieringstjänster upphör, gäller avtalsvillkoren avseende skadestånd fortsättningsvis. När avtalet mellan leverantörerna av identifieringstjänster upphör, upphör inte ansvaret för skada som förorsakas av åtgärder som vidtagits eller inte vidtagits under avtalets giltighetstid.

4.17 Överföring av avtal

Om verksamhet överlåts inom en koncern eller i en annan motsvarande grupp av företag som en avtalspart hör till, kan avtalet överföras till ett koncernföretag eller till ett företag inom samma grupp av företag som anges i en ändringsanmälan till Transport- och kommunikationsverket.

Avtalsparterna ska avtala om övriga villkor och förfaranden för överföring av avtalet i sitt ömsesidiga avtal.

4.18 Tvistelösning

Transport- och kommunikationsverket och dataombudsmannen övervakar för sina delar att bestämmelserna i autentiseringslagen iakttas. De kan ge lagenliga tillsynsbeslut som ålägger berörda parter att åtgärda verksamheten till den del det finns bestämmelser om skyldigheter och rättigheter i lag, förordning eller föreskrifter. Transport- och kommunikationsverket får genom beslut förbjuda tillhandahållande av identifieringstjänster som lagstadgad stark autentisering om verksamheten inte längre uppfyller kraven i lagen.

Transport- och kommunikationsverket är inte behörig myndighet i frågor som gäller avtalsförhållanden mellan parter eller frågor om ersättningsskyldighet. Avtalsparterna kan avtala om ett behörigt organ för tvistelösning.

På avtalen tillämpas Finlands lag såvida inte avtalsparter undantagsvis avtalar något annat.

5 Ändring av upphörandekoderna

Uppförandekoderna har utfärdats som Transport- och kommunikationsverkets rekommendation och därför ansvarar Transport- och kommunikationsverket för änd-

ring och hantering av koderna. När uppförandekoderna ändras, ska en övergångsperiod som är skälig med tanke på ändringarnas art vid behov reserveras för genomförande av ändringarna.

Transport- och kommunikationsverket kan överlåta uppförandekoderna till samarbetsgruppen för förtroendenätet för hantering efter att först ha diskuterat frågan med samarbetsgruppen, som kan utses med stöd av förordningen om förtroendenätet.

Om dessa uppförandekoder ändras, ska leverantörerna av identifieringstjänster vid behov ändra sina avtal i enlighet med uppförandekoderna. Detta bör beaktas i avtalen.

Vid ändring av dessa uppförandekoder och de modellavtalsklausuler som ingår i koderna utvärderas ändringarnas inverkan på gällande avtal noggrant.

6 Referenser

[1] Lag om stark autentisering och betrodda elektroniska tjänster (617/2009, autentiseringslag)

[2] Statsrådets förordning om förtroendenätet för leverantörer av tjänster för stark autentisering (169/2016)

[3] Transport- och kommunikationsverkets föreskrift 72 B/2022 M om elektroniska identifieringstjänster och betrodda elektroniska tjänster (M72 B, föreskrift 72 B). Promemorian MPS72B (motivering till och tillämpning av föreskrift 72) hänför sig till föreskriften.

[4] 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 (eIDAS)

[5] EU-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

[6] 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

[7] Transport- och kommunikationsverkets rekommendation 212/2021 S (SAML om förtroendenätets gränssnitt (Finnish Trust Network SAML 2.0 Protocol Profile)

[8] Transport- och kommunikationsverkets rekommendation 213/2021 S (OIDC om förtroendenätets gränssnitt(Finnish Trust Network OpenID Connect Protocol Profile)

[9] Kommunikationsverkets publikation 004/2016 J, Olli Norros: Selvitys tunnistamiseen liittyvistä vahingonkorvauskysymyksistä, Vahingonkorvausoikeudellinen selvitys

Bilaga

Behandling av personuppgifter i förtroendenätet för elektronisk identifiering

Behandling av personuppgifter i förtroende-nätet för elektronisk identifiering

Bilaga till Transport- och kommunikationsverkets rekommendation
216/2022 S

Versionshistorik

Version	Datum	Beskrivning/ändring
1.0	3.7.2017	Första publicerade versionen
2.0	6.6.2022	Omfattar ändringar som dataskyddsförordningen kräver samt andra preci-seringar

Innehåll

1 Inledning

Denna rekommendation om behandlingen av personuppgifter (dataskyddsbilagan) kompletterar lagen, förordningen och Transport- och kommunikationsverket lagbaserade tekniska föreskrifter om stark autentisering och förtroendenätet för leverantörer av identifieringstjänster.

Genom ändringen (139/2015) av lagen om stark autentisering och betrodda elektroniska tjänster (617/2009, nedan benämnd autentiseringslagen) [1] utfärdades bestämmelser om uppbyggnad av ett förtroendenät för identifieringstjänster. Regleringen som gäller förtroendenätet har sedan dess preciserats genom nya lagändringar. Målet för förtroendenätet är att främja både utbudet på marknaden av allmänt tillgängliga identifieringstjänster som till användbarheten och säkerheten är avancerade och säkerheten i den elektroniska ärendehanteringen. Via nätet kan olika identifieringsverktyg förmedlas till tjänster för ärendehantering genom enhetliga tekniska och administrativa arrangemang. Närmare bestämmelser om förtroendenätets administrativa praxis, tekniska gränssnitt och administrativa ansvar finns i statsrådets förordning om förtroendenätet för leverantörer av tjänster för stark autentisering (169/2016 jämte ändringar, nedan benämnd förordningen om förtroendenätet) [2].

I denna rekommendation specificeras de allmänna principerna för behandling av personuppgifter i förtroendenätet. Närmare bestämmelser om behandlingen av personuppgifter finns speciellt i EU:s allmänna dataskyddsförordning (2016/679, nedan benämnd dataskyddsförordningen)[1] och i dataskyddslagen (1050/2018).

Behandlingen av personuppgifter i tjänster för ärendehantering och annan behandling av personuppgifter än den som hänför sig till identifieringstransaktioner har avgränsats ur dataskyddsbilagan, även om de tangeras i anvisningarna.

Denna rekommendation om behandlingen av personuppgifter har tagits fram av experter inom personuppgiftslagen på basis av de behov som dåvarande Kommunikationsverkets arbetsgrupp för Identifiering och betrodda tjänster hade identifierat. Under beredningen av den första versionen av bilagan har dataskyddsombudsmannen konsulterats om ämnet.

Rekommendationen om behandlingen av personuppgifter är juridiskt sett Transport- och kommunikationsverkets rekommendation, inte en förpliktande föreskrift. Enligt lagen om stark autentisering och betrodda elektroniska tjänster ska dataombudsmannen övervaka att bestämmelserna om personuppgifter i lagen iakttas. Transport- och kommunikationsverket är inte myndighet som svarar för tillsynen över att personuppgifter behandlas i enlighet med lag.

2 FÖRTROENDENÄTET OCH DESS VERKSAMHET

2.1 Förtroendenät

Leverantörer av identifieringstjänster som avses i autentiseringslagen är en del av det gemensamma förtroendenätverket. Det finns två typer av medlemmar, dvs. leverantörer av identifieringstjänster, i förtroendenätet: en leverantör av identifieringsverktyg ingår ett avtal om tillhandahållande av identifieringstjänster med de

[1] Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EY.

kunder som ska identifieras och en leverantör av tjänster för identifieringsförmedling förmedlar identifieringstransaktioner till sådana leverantörer av tjänster för ärendehantering som inte hör till förtroendenätet men som anlitas av den som ska identifieras. En och samma organisation kan samtidigt vara en leverantör av identifieringsverktyg och en leverantör av tjänster för identifieringsförmedling; ansvar i dessa roller behandlas dock separat i denna handling.

2.2 Minimiuppsättningen uppgifter som ska behandlas

Som en del av identifieringstransaktioner behandlar och förmedlar medlemmarna i förtroendenätet sinsemellan uppgifter om förnamn, efternamn, födelsetid och identifikator som identifierar en person (personbeteckning eller elektronisk kommunikationskod). Medlemmarna kan också, i tillämpliga delar, hämta, säkerställa eller uppdatera de uppgifter som de behöver för tillhandahållandet av identifieringstjänster med användning av befolkningsdatasystemet. Leverantörer av identifieringsverktyg är skyldiga att hämta och uppdatera uppgifterna med användning av befolkningsdatasystemet (7 § i autentiseringslagen).

2.3 Icke-obligatoriska uppgifter som ska behandlas

Som en del av identifieringstransaktionen kan medlemmarna i förtroendenätet behandla och eventuellt förmedla sinsemellan sådana icke-obligatoriska uppgifter som anges i punkt 12.2 i Transport- och kommunikationsverkets föreskrift 72B[3]. Sådana uppgifter är förnamn och -efternamn vid födseln, födelseort, nuvarande adress och kön.

2.4 Övriga uppgifter som ska behandlas

En medlem i förtroendenätet kan också tillhandahålla sina egna mervärdestjänster där det är möjligt att behandla andra uppgifter förutom uppgifterna i 2.2 och 2.3 (för relaterade ytterligare krav, se punkt 4.2).

2.5 Förmedling av personuppgifter i förtroendenätet

Leverantörer av identifieringsverktyg, leverantörer av tjänster för identifieringsförmedling och leverantörer av tjänster för ärendehantering är i dataskyddsförordningen avsedda självständiga personuppgiftsansvariga i fråga om personuppgifter som ska behandlas, vilket ska bedömas på basis av dataskyddsförordningen. Förmedlingen av identifieringstransaktioner i förtroendenätet kan alltså omfatta utlämnande av personuppgifter mellan de personuppgiftsansvariga på de villkor som beskrivs nedan.

2.6 Definitioner

De rättsliga begrepp som används här har samma betydelse som i autentiseringslagen och i dataskyddsförordningen. Om en part som förlitar sig på elektronisk identifiering används begreppet tjänst för ärendehantering. Med detta avses en nättjänst eller en annan tjänst som den som ska identifieras använder och för vilken identifiering görs. Personuppgift och behandling av personuppgifter har samma betydelse som i dataskyddsförordningen. En identifieringstransaktion som förmedlas i förtroendenätet innehåller i princip alltid sådana personuppgifter.

3 BEHANDLING AV PERSONUPPGIFTER I FÖRTROENDENÄTET I ALLMÄNHET

3.1 Kravet på behandlingens lagenlighet och grunder

Medlemmarna i förtroendenätet behandlar personuppgifter endast på en sådan grund som lagen tillåter (se punkt 4) och endast i den omfattning som grunden i

fråga och myndigheternas föreskrifter som tillämpas tillåter. När medlemmar i förtroendenätet lämnar ut personuppgifter till andra medlemmar i förtroendenätet och till tjänster för ärendehantering är de ansvariga för att även den mottagande parten har en lagbaserad rätt att ta emot och behandla personuppgifterna i fråga.

3.2 Medlemsspecifik information

Förutom vad som sägs här beskrivs en medlems behandling av personuppgifter också i medlemmens egen dataskyddsbeskrivning, i principer för identifiering eller i motsvarande handling som dock aldrig får vara i strid med vad som sägs här. Den medlemsspecifika dataskyddsbeskrivningen eller motsvarande handling innehåller bl.a. medlemmens, och i tillämpliga delar medlemmens dataskyddsansvariges, namn och kontaktinformation, huruvida medlemmen översänder uppgifter utanför EU/EES-området och grunden för sådant samt övriga frågor som lagen kräver. Transport- och kommunikationsverket för på sina webbsidor en förteckning över medlemmarna i förtroendenätet som också innehåller länkar till dessa dataskyddsbeskrivningar eller medlemmens principer för identifiering som närmare anger de dataskyddsprinciper som medlemmen tillämpar.

4 GRUNDEN FÖR BEHANDLINGEN AV PERSONUPPGIFTER I FÖRTROENDENÄTET

4.1 Behandlingsgrund i förtroendenätet

Medlemmarna behandlar i regel personuppgifter för den som ska identifieras för att fullgöra ett avtal i vilket den registrerade är part eller för att vidta åtgärder på begäran av den registrerade innan ett sådant avtal ingås.

Personuppgifter kan också behandlas för att fullgöra en rättslig förpliktelse eller för att trygga en medlems eller en tredje parts berättigade intressen.

Medlemmen svarar i alla fall för att den har en tillräcklig grund för behandlingen av personuppgifter.

4.2 Mervärdestjänster

Här behandlas inte något annat än behandling av personuppgifter för genomförande av identifieringstjänster. De mervärdestjänster som en medlem i förtroendenätet eventuellt tillhandahåller (se punkt 2.4) beskrivs separat i respektive dataskyddsbeskrivning eller i motsvarande uppgifter. En leverantör av identifieringsverktyg som har en kundrelation med den som ska identifieras är på basis av vad som sägs här inte ansvarig för att personuppgifter för den som ska identifieras kan behandlas i syfte att tillhandahålla mervärdestjänster.

4.3 Personuppgiftsbiträden

Om en medlem anlitar ett biträde för behandling av personuppgifter, ska medlemmen se till att den och den personuppgiftsansvarige har ingått ett skriftligt avtal som uppfyller lagens krav och att övriga krav som hänför sig till att anlita ett biträde följs. En medlem svarar för sitt biträde i enlighet med lag.

5 BEHANDLING AV PERSONUPPGIFTER I TJÄNSTER FÖR ÄRENDEHANTERING

5.1 Behandlingsgrund i tjänster för ärendehantering

Här beskrivs varken den behandling av personuppgifter som görs av en leverantör av tjänster för ärendehantering eller en behandlingsgrund för det. En medlem i förtroendenätet som har ett avtalsförhållande eller ett motsvarande förhållande med tjänsten för ärendehantering försäkrar sig om att tjänsten för ärendehantering har en tillräcklig behandlingsgrund för att ta emot och behandla identifieringstransaktionen och tillhörande personuppgifter. Om uppgifterna i identifieringstransaktionen innehåller personbeteckningen för den som ska identifieras, kan den lämnas ut till tjänsten för ärendehantering endast om denne har en laglig grund att ta emot och behandla personbeteckningar.

5.2 Dataskyddsbeskrivning för tjänster för ärendehantering

En tjänst för ärendehantering har en egen dataskyddsbeskrivning (eller en motsvarande handling) med uppgifter om behandlingen av personuppgifterna i tjänsten. Tjänsten för ärendehantering säkerställer att den som ska identifieras har tillgång till dataskyddsbeskrivningen och att leverantören av tjänsten för ärendehantering uppfyller sina informationsskyldigheter och andra skyldigheter mot den som ska identifieras. En medlem i förtroendenätet som ingått avtal med tjänsten för ärendehantering säkerställer, om möjligt, att tjänsten för ärendehantering uppfyller dessa skyldigheter eller kan uppfylla dem för tjänsten för ärendehantering eller bistå i detta, om man har överenskommit om det.

5.3 Överlåtelse av uppgifter från tjänsten för ärendehantering

Tjänsten för ärendehantering får överlåta uppgifter som den fått i samband med identifieringstjänster endast om lagen tillåter det. En medlem i förtroendenätet som ingått avtal med tjänsten för ärendehantering säkerställer i avtalen att leverantören av tjänsten för ärendehantering har förbundit sig till detta.

6 UTLÄMNANDE AV PERSONUPPGIFTER TILL UTLANDET

6.1 Utlämnande och översändande till utlandet

Medlemmarna i förtroendenätet får inte, t.ex. som en del av utlokaliseringsarrangemang, lämna ut eller översända personuppgifter till stater utanför Europeiska unionen eller Europeiska ekonomiska samarbetsområdet (EU/EES) förutom när tillämplig lagstiftning om behandling av personuppgifter tillåter och de ytterligare förutsättningar som lagstiftningen eventuellt ställer är uppfyllda.

6.2 Information

Om man lämnar ut eller översänder uppgifter till stater utanför EU/EES, måste medlemmen informera om detta samt om grunden för utlämnande/översändande och om övriga angelägenheter som lagen kräver i en medlemsspecifik dataskyddsbeskrivning eller i en annan motsvarande handling.

7 INFORMATIONSSÄKERHET; FÖRVARING AV UPPGIFTERNA

7.1 Allmänt krav på informationssäkerhet

Med stöd av lag är alla medlemmar i förtroendenätet skyldiga att genomföra alla de tekniska och organisatoriska åtgärder som behövs för att skydda personuppgifterna mot obehörig åtkomst och mot förstöring, ändring, utlämnande och översändande som sker av misstag eller i strid med lag eller mot annan olaglig behandling.

7.2 Transport- och kommunikationsverkets föreskrifter

Alla medlemmar i förtroendenätet iakttar alltid också de föreskrifter av Transport- och kommunikationsverket som tillämpas på sådan verksamhet som beskrivs här.

7.3 Förvaring av uppgifterna

Som en del av identifieringstransaktionen får medlemmarna i förtroendenätet lagra de personuppgifter de behandlat i den tid som förutsätts i 24.3 § i autentiseringslagen, dvs. i minst fem år från identifieringstransaktionen, eller i en sådan annan tid som den lag som gäller förtroendenätets medlems verksamhet tillåter eller förutsätter.

8 TILLSYN OCH RÄTTIGHETER FÖR DEM SOM SKA IDENTIFIERAS

8.1 Tillsyn

Transport- och kommunikationsverket och dataombudsmannen utövar i tillämpliga delar tillsyn över vad som sägs här. Om den som ska identifieras har ställning som konsument kan denne också ha rätt att föra ärendet till konsumenttvistenämnden (kuluttajariita.fi).

Medlemmarna i förtroendenätverket säkerställer dessutom för sin del och i enlighet med lämpliga krav på omsorgsfullhet att uppgifterna behandlas i förtroendenätverket i enlighet med lag.

8.2 Rättigheter för den som ska identifieras

Den som ska identifieras har en lagbaserad rätt att

(1) granska sina personuppgifter som en medlem i förtroendenätet har sparat samt i vissa situationer begära en kopia av uppgifterna till sig själv och/eller eventuellt begära att uppgifterna flyttas till ett annat informationssystem,

(2) kräva att felaktiga eller bristfälliga uppgifter korrigeras,

(3) kräva att gamla eller onödiga uppgifter raderas,

(4) kräva att behandlingen av uppgifterna begränsas temporärt, till exempel tills ett annat krav som gäller personens uppgifter har avgjorts,

(5) invända mot behandlingen av sina uppgifter för direktmarknadsföring eller, om en speciell personlig situation kräver, användningen av sina uppgifter för att trygga en medlems eller en tredje parts berättigade intressen.

Dessa rättigheter kan dock begränsas i vissa situationer som fastställs i lag.

9 ÖVRIGT

9.1 Lag som tillämpas

På denna handling, på tolkningen av den samt på rättigheter och skyldigheter som följer därav tillämpas Finlands lag.

10 Referenser

[1] Lag om stark autentisering och betrodda elektroniska tjänster (617/2009, autentiseringslag)

[2] Statsrådets förordning om förtroendenätet för leverantörer av tjänster för stark autentisering (169/2016)

[3] Transport- och kommunikationsverkets föreskrift 72B/2022 M om elektroniska identifieringstjänster och betrodda elektroniska tjänster (M72 B, föreskrift 72B). Promemorian MPS 72B (motivering till och tillämpning av föreskrift 72) hänför sig till föreskriften.