Lagrådsremiss

Ytterligare kompletterande bestämmelser till EU:s förordning om elektronisk identifiering

Regeringen överlämnar denna remiss till Lagrådet.

Stockholm den 3 december 2020

Anders Ygeman

Pontus Söderström
(Infrastrukturdepartementet)

Lagrådsremissens huvudsakliga innehåll

I lagrådsremissen föreslås att nya kompletterande bestämmelser till Europaparlamentets och rådets förordning (EU) nr 910/2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden ska föras in i lagen (2016:561) med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering.

För att möjliggöra användningen av europeiska elektroniska legitimationer i svenska offentliga nättjänster ska offentliga organ under vissa förutsättningar ansluta sina nättjänster till den nod för inkommande gränsöverskridande elektronisk identifiering som Myndigheten för digital förvaltning tillhandahåller. Regeringen eller den myndighet som regeringen bestämmer ska få meddela föreskrifter om anslutningen till noden. Regeringen ska vidare få meddela föreskrifter om undantag från anslutningsskyldigheten i fråga om verksamhet som avser totalförsvaret eller Sveriges säkerhet i övrigt.

Regeringen eller den myndighet som regeringen bestämmer ska få meddela föreskrifter om vad som krävs för att system för elektronisk identifiering ska anmälas för gränsöverskridande elektronisk identifiering inom EU.

Lagändringarna föreslås träda i kraft den 1 juni 2021.

Innehållsförteckning

1 Beslut

Regeringen har beslutat att inhämta Lagrådets yttrande över förslag till lag om ändring i lagen (2016:561) med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering.

2 Förslag till lag om ändring i lagen (2016:561) med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering

Härigenom föreskrivs att det i lagen (2016:561) med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering ska införas tre nya paragrafer, 1 a–1 c §§, och närmast före 1 a § en ny rubrik av följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	Elektronisk identifiering
	1 a §
	Ett offentligt organ som tillhandahåller en nättjänst ska ansluta tjänsten till den svenska förbindelsepunkten (noden) för inkommande gränsöverskridande elektronisk identifiering, om nättjänsten omfattas av kravet på erkännande av medel för elektronisk identifiering som utfärdats i en annan medlemsstat enligt artikel 6 i EU:s förordning om elektronisk identifiering. Detta gäller dock inte om anslutningen medför risk för skada för totalförsvaret eller Sveriges säkerhet i övrigt.
	Regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om anslutning till noden.
	Regeringen får meddela föreskrifter om undantag från anslutningsskyldigheten i fråga om verksamhet som avser totalförsvaret eller Sveriges säkerhet i övrigt.
	1 b §
	Den som är ansluten till en svensk nod för inkommande eller utgående gränsöverskridande elektronisk identifiering ska så snart som möjligt underrätta den myndighet som ansvarar för noden om händelser som kan ha betydelse för

nodens funktionalitet eller säkerhet.

Regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om underrättelseskyldigheten.

1 c §

Regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om vilka krav som ska gälla för att ett system för elektronisk identifiering ska anmälas för gränsöverskridande elektronisk identifiering enligt EU:s förordning om elektronisk identifiering och de rättsakter som meddelas med stöd av förordningen.

Denna lag träder i kraft den 1 juni 2021.

3 Ärendet och dess beredning

Sedan september 2018 tillämpas Europaparlamentets och rådets förordning (EU) nr 910/2014 av den 23 juli 2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG (EU:s förordning om elektronisk identifiering) i sin helhet. Förordningen kompletteras med bestämmelser i lagen (2016:561) med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering och i förordningen (2016:576) med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering, vilka trädde i kraft den 1 juli 2016. I förarbetena till lagen uttalade regeringen att frågor om ömsesidigt erkännande av medel för elektronisk identifiering och processen för anmälan av ett system för elektronisk identifiering behövde analyseras i särskild ordning (prop. 2015/16:72 s. 50 f.).

Regeringen gav i mars 2016 E-legitimationsnämnden i uppdrag att utveckla en central teknisk arkitektur för hantering av europeiska e-legitimationer enligt EU:s förordning om elektronisk identifiering (N2016/02305). Regeringen beslutade i maj samma år att tillkalla en särskild utredare med uppdrag att bl.a. utreda konsekvenserna för svenska myndigheter av skyldigheten att erkänna anmälda europeiska e-legitimationer och elektroniska underskrifter i nationella digitala tjänster och lämna förslag på ytterligare åtgärder som krävs för att säkerställa att Sverige kan uppfylla sina åtaganden enligt EU:s förordning för elektronisk identifiering. Vidare skulle utredaren analysera behoven av och förutsättningarna för anmälan av svenska e-legitimationer enligt förordningen (dir. 2016:39). Utredningen, som antog namnet Utredningen om effektiv styrning av nationella digitala tjänster, överlämnade i december 2017 betänkandet reboot – omstart för den digitala förvaltningen (SOU 2017:114). En sammanfattning av betänkandet finns i *bilaga 1*. Ett utdrag av betänkandets lagförslag, i de delar som nu är aktuella, finns i *bilaga 2*. Betänkandet har remissbehandlats. En förteckning över remissinstanserna finns i *bilaga 3*. Remissvaren finns tillgängliga i Infrastrukturdepartementet (I2019/01017).

I lagrådsremissen behandlas de lagförslag som utredningen lämnar i avsnitt 17 och 18 i betänkandet (s. 297–374). Förslagen rör frågor om svenska förbindelsepunkter (noder) för gränsöverskridande elektronisk identifiering och om anmälan av svenska system för elektronisk identifiering. Utredningens förslag i övrigt bereds vidare i Regeringskansliet.

4 Elektronisk identifiering

4.1 Processen för elektronisk identifiering

För att få åtkomst till en digital tjänst, till exempel för att lämna in en skattedeklaration digitalt, krävs normalt att den som vill få åtkomst identifierar sig. Detta kan till exempel ske genom att användaren uppger

en e-postadress men oftast, för tjänster med högre krav på säkerhet, genom användning av en elektronisk legitimation (e-legitimation). En e-legitimation innehåller, liksom en fysisk identitetshandling, uppgifter som entydigt kan kopplas till en viss person. E-legitimationen innehåller alltså endast identitetsuppgifter. En e-legitimation kan finnas som en applikation i en mobiltelefon eller surfplatta eller som en fil på en dator. Den kan också finnas på en fysisk bärare, till exempel ett kort. Kortet innehåller då ett chip där informationen lagras.

I processen för elektronisk identifiering brukar normalt fyra roller förekomma: användaren, den förlitande aktören, utfärdaren och identitetsintygsutfärdaren. Användaren är den individ som vill använda sin e-legitimation för att identifiera sig elektroniskt i en digital tjänst. Den förlitande aktören är den aktör som har behov av att verifiera en användares identitetsuppgifter vid identifiering i en digital tjänst. Utfärdaren är den som utfärdar en e-legitimation till användaren. Utfärdaren tillhandahåller också en funktion för identitetskontroll åt den förlitande aktören. Utfärdaren ansvarar gentemot användaren för att utfärdandet sker på ett tillräckligt säkert sätt. Utfärdaren ansvarar även gentemot den förlitande aktören för att den elektroniska identifieringen är tillförlitlig. Detta sker genom att utfärdaren tillhandahåller en funktion för identitetskontroll åt den förlitande aktören som får ett identitetsintyg som bekräftelse på att användaren kan få tillträde till den digitala tjänsten. Utfärdare av e-legitimationer kan köpa in tjänsten att leverera identitetsintyg av en underleverantör och då blir det i stället en identitetsintygsutfärdare som utför den elektroniska identifieringen.

Vilka krav på säkerhet som ställs för tillgång till en digital tjänst bedöms av tillhandahållaren av den digitala tjänsten. Säkerhetsnivåerna, kallade tillitsnivåer, har standardiserats inom EU genom EU:s förordning om elektronisk identifiering. Enligt förordningen finns det tre tillitsnivåer: låg, väsentlig och hög.

4.2 EU:s förordning om elektronisk identifiering

EU:s förordning om elektronisk identifiering innehåller ett rättsligt ramverk för elektronisk identifiering inom EU. Med det rättsliga ramverket följer tekniska standarder och specifikationer – i huvudsak genom genomförandeakter – vilket gör att förordningen även fungerar som ett tekniskt ramverk för elektronisk identifiering. Förordningen består av två delar, där den första innehåller förordningens allmänna del samt processen för gränsöverskridande elektronisk identifiering och den andra behandlar betrodda tjänster.

I artikel 1 anges att målet med förordningen är att säkerställa en väl fungerande marknad och uppnå en lämplig säkerhetsnivå för medel för elektronisk identifiering och betrodda tjänster. I skäl 2 i förordningen anges att den syftar till att öka förtroendet för elektroniska transaktioner på den inre marknaden genom att tillhandahålla en gemensam grund för ett säkert elektroniskt samspel mellan företag, medborgare och offentliga myndigheter. Därigenom ska effektiviteten hos offentliga och privata digitala tjänster, elektronisk affärsverksamhet och e-handel i unionen öka.

Enligt artikel 2 gäller förordningen för system för elektronisk identifiering som en medlemsstat har anmält och för tillhandahållare av betrodda tjänster som är etablerade inom unionen. Det framgår också att förordningen inte gäller tillhandahållande av betrodda tjänster som till följd av nationell lagstiftning eller avtal mellan en avgränsad krets av deltagare endast används inom slutna system. Den påverkar inte heller bestämmelser i nationell lagstiftning eller unionslagstiftningen som avser ingående av avtal och deras giltighet eller andra rättsliga eller förfarandemässiga skyldigheter i fråga om formkrav.

Enligt artikel 6 ska medel för elektronisk identifiering under vissa förutsättningar omfattas av ömsesidigt erkännande. Det gäller för sådana medel för elektronisk identifiering som är utfärdade inom ramen för ett system för elektronisk identifiering som har anmälts av en medlemsstat och därefter offentliggjorts i Europeiska unionens officiella tidning (jfr skäl 14). Skyldigheten att erkänna medel för elektronisk identifiering avser enbart medel vars identifieringstillitsnivå motsvarar en nivå som är lika hög eller högre än den nivå som krävs för den aktuella digitala tjänsten. Skyldigheten gäller dessutom endast när det offentliga organet i fråga använder tillitsnivån väsentlig eller hög i samband med åtkomst till den digitala tjänsten (jfr skäl 15).

Medel för elektronisk identifiering definieras i artikel 3.2 som en materiell och/eller immateriell enhet som innehåller personidentifieringsuppgifter och som används för autentisering för nättjänster. För e-legitimationer utfärdade i Sverige är det normalt en persons personnummer som är personidentifieringsuppgiften. Artikeln innebär att en elektronisk legitimation som uppfyller kraven enligt förordningen och som utfärdats i en annan medlemsstat ska kunna användas för identifiering till nättjänster som tillhandahålls av offentliga organ i Sverige.

System för elektronisk identifiering ska för att omfattas av förordningen anmälas till Europeiska kommissionen enligt ett särskilt förfarande som framgår av artiklarna 7–9. Där anges vilka system som får anmälas, hur anmälan ska gå till och vilka krav som ställs på de anmälda systemen och de medel för elektronisk identifiering som utfärdas inom dessa. Förordningen innehåller i artikel 10 bestämmelser om hantering av säkerhetsincidenter i anmälda system. I artikel 11 finns regler om skadeståndsansvar för den anmälande medlemsstaten, den som har utfärdat medel för elektronisk identifiering och den part som har hand om autentiseringsförfarandet, om de inte uppfyller sina skyldigheter enligt förordningen.

4.3 Gränsöverskridande elektronisk identifiering

För att identifiera sig för åtkomst till en digital tjänst i en annan medlemsstat än den där individens e-legitimation har utfärdats kan det system för gränsöverskridande identifiering som upprättas med anledning av EU:s förordning om elektronisk identifiering användas. Medlet, som är bärare av personidentifieringsuppgifterna i e-legitimationen, kan färdas i systemet mellan förbindelsepunkter, kallade noder. En nod i den avsändande staten verifierar medlet i det nationella systemet och skickar det vidare till den mottagande noden i den mottagande staten. Den mottagande noden

verifierar i sin tur att den avsändande noden verifierat medlet för e-legitimationen och gör en form av översättning så att medlet kan fungera i den mottagande statens infrastruktur för elektronisk identifiering. När detta har skett kan individen använda sin e-legitimation för identifiering i en digital tjänst i en annan stat. Förfarandet förutsätter att medlet för e-legitimationen finns inom ett sådant system som anmälts till Europeiska kommissionen och att det även i övrigt uppfyller kraven i artikel 6.

Definitionen av noderna och de huvudsakliga reglerna för dessa framgår av kommissionens genomförandeförordning (EU) 2015/1501 av den 8 september 2015 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 (kommissionens genomförandeförordning). En nod definieras i artikel 2 som en förbindelsepunkt som utgör en del av den interoperativa arkitekturen för elektronisk identifiering, som medverkar vid gränsöverskridande autentisering av personer och som har förmågan att känna igen och behandla eller vidarebefordra överföringar till andra noder genom att bringa den nationella elektroniska identifieringsinfrastrukturen i en medlemsstat i kontakt med nationella elektroniska identifieringsinfrastrukturer i andra medlemsstater. Enligt artikel 5 i förordningen ska det i varje medlemsstat finnas minst en nod med förmåga att koppla upp sig mot noder i andra medlemsstater.

5 Svenska förbindelsepunkter för gränsöverskridande elektronisk identifiering

Regeringens bedömning: Ansvaret för de svenska förbindelsepunkterna (noderna) för gränsöverskridande elektronisk identifiering i enlighet med EU:s förordning om elektronisk identifiering och de rättsakter som meddelas med stöd av förordningen bör även i fortsättningen regleras i förordning.

Utredningens förslag överensstämmer delvis med regeringens bedömning. Utredningen föreslår att ansvaret för tillhandahållandet av noderna ska regleras i lag. Utredningen föreslår även ett bemyndigande att meddela föreskrifter om noden.

Remissinstanserna: De flesta av remissinstanserna tillstyrker förslaget eller har ingen invändning mot det.

Skälen för regeringens bedömning: I samband med att Myndigheten för digital förvaltning inrättades tog myndigheten över ansvaret för noderna för gränsöverskridande identifiering från E-legitimationsnämnden. I 3 § 4 förordningen (2018:1486) med instruktion för Myndigheten för digital förvaltning ges myndigheten i uppgift att ansvara för de svenska noderna för gränsöverskridande elektronisk identifiering i enlighet med EU:s förordning för elektronisk identifiering och de rättsakter som har meddelats med stöd av förordningen.

E-legitimationsnämnden utvecklade två noder för gränsöverskridande elektronisk identifiering: en avsedd för användningen av svenska e-legitimationer i digitala tjänster i andra medlemsstater och en annan för användning av e-legitimationer utfärdade i andra medlemsstater i svenska digitala tjänster. Regeringen anser att ansvaret för noderna numera är tydligt utpekat i instruktionen för Myndigheten för digital förvaltning. Myndighetens ansvar för noderna innefattar även tillhandahållandet av noderna. Till skillnad från utredningen anser inte regeringen att det finns behov av att reglera dessa uppgifter i lag.

Utredningen föreslår även att regeringen eller, efter regeringens bemyndigande, myndigheten ska få meddela föreskrifter om noden. Vilken typ av föreskrifter som skulle bli aktuella med anledning av tillhandahållandet av noderna behandlas dock inte närmare i betänkandet. Myndigheten för digital förvaltnings rätt att meddela föreskrifter om noderna behandlas i avsnitt 6 och 8. Det bör enligt regeringens mening inte uppstå behov för Myndigheten för digital förvaltning att därutöver meddela föreskrifter om noderna. Av den anledningen saknas det behov av ett sådant bemyndigande som utredningen föreslår.

6 Offentliga organs anslutning till den svenska noden för inkommande gränsöverskridande identifiering

Regeringens förslag: Ett offentligt organ som tillhandahåller en nättjänst som omfattas av kravet på erkännande av medel för elektronisk identifiering som utfärdats i en annan medlemsstat enligt artikel 6 i EU:s förordning om elektronisk identifiering ska ansluta tjänsten till den svenska förbindelsepunkten (noden) för inkommande gränsöverskridande elektronisk identifiering. Skyldigheten ska dock inte gälla om anslutningen medför risk för skada för totalförsvaret eller Sveriges säkerhet i övrigt. Regeringen eller den myndighet som regeringen bestämmer ska få meddela föreskrifter om anslutning till noden. Regeringen ska få meddela föreskrifter om undantag från anslutningsskyldigheten i fråga om verksamhet som avser totalförsvaret eller Sveriges säkerhet i övrigt.

Regeringens bedömning: Även aktörer som inte omfattas av kravet på anslutning bör anslutas till noden om de begär det. Myndigheten för digital förvaltning bör få ta ut avgifter av de privata aktörer som frivilligt har anslutit sig till noden.

Utredningens förslag överensstämmer delvis med regeringens förslag och bedömning. Utredningen föreslår att det i lag ska införas bestämmelser om att även offentliga organ som inte omfattas av EU-förordningens krav och privata aktörer ska få ansluta till den svenska noden. Utredningen föreslår även ett bemyndigande för regeringen eller, efter regeringens bemyndigande, digitaliseringsmyndigheten att meddela föreskrifter om skyldighet för privata aktörer att betala avgift för att ansluta till noden.

Utredningen föreslår inte några undantag från anslutningsskyldigheten. Den föreslår inte heller ett bemyndigande att meddela föreskrifter om anslutningen till noden.

Remissinstanserna: De flesta av remissinstanserna tillstyrker förslaget eller har ingen invändning mot det. *Sjöfartsverket* påpekar vikten av att de lösningar som föreslås möjliggör utländska medborgares användning av myndigheternas digitala tjänster, för att undvika att särskilda system för sådan användning tas fram. *Tillväxtverket* påpekar att erkännandet av utländska elektroniska identitetshandlingar även bör omfatta den slutliga åtkomsten till den digitala tjänsten i linje med målsättningarna om att sådana tjänster ska bli helt tillgängliga online. *Försäkringskassan* avstyrker förslaget. *Försvarsmakten* anser att det är svårt att uttyda vilka myndigheter som bör omfattas av de föreslagna författningskraven. Försvarsmakten påpekar att det saknas en nationell informationsvärdering i utredningens förslag vilket innebär att realiserbarheten i förslagen kan ifrågasättas. Med anledning av detta föreslår Försvarsmakten att en nationell informationsvärdering genomförs innan kraven på digitalisering lagregleras. Försvarsmakten anser vidare att myndigheten bör undantas från tvingande krav på digitalisering eftersom de operativa uppgifter som den utför kräver att myndigheten har full rådighet och handlingsfrihet i hur uppgifter och information hanteras för att kunna verka i hela konfliktskalan, dvs. fred, kris och krig.

Skälen för regeringens förslag och bedömning: Det följer av bestämmelserna om ömsesidigt erkännande i artikel 6 i EU:s förordning om elektronisk identifiering att en medlemsstats offentliga organ under vissa omständigheter i sina nättjänster ska acceptera medel för elektronisk identifiering som utfärdats i en annan medlemsstat. Offentligt organ definieras i artikel 3.7. Till sådana organ hör statliga, regionala eller lokala myndigheter, organ som lyder under offentlig rätt eller sammanslutningar som bildats av en eller flera sådana myndigheter eller ett eller flera sådana offentligrättsliga organ. Hit hör också privata enheter som av minst en av dessa myndigheter, enheter eller sammanslutningar har bemyndigats att tillhandahålla offentliga tjänster när de agerar i enlighet med ett sådant bemyndigande.

För att ett offentligt organ ska omfattas av kravet på erkännande ska det för åtkomst till nättjänsten krävas elektronisk identifiering enligt nationell rätt eller på grund av ett administrativt förfarande. Nättjänsten ska vidare kräva att identifieringen sker på tillitsnivån väsentlig eller hög. För medlet krävs att dess tillitsnivå ska motsvara en nivå som är minst lika hög som den som används i den digitala tjänsten och att medlet ska vara utfärdat inom ramen för ett system som anmälts och ingår i den förteckning som Europeiska kommissionen offentliggjort i Europeiska unionens officiella tidning, se avsnitt 8. I skäl 14 förtydligas att principen om ömsesidigt erkännande endast avser autentisering för en nättjänst. Den ger inte en rätt till åtkomst till tjänsten. Åtkomsten till tjänsterna och deras slutliga leverans till den sökande är kopplad till rätten att ta emot sådana tjänster enligt villkoren i nationell lagstiftning. Varje offentligt organ får inom ramen för den tillämpliga nationella lagstiftningen avgöra vilka krav som ska ställas för åtkomst till tjänsterna.

Den gränsöverskridande elektroniska identifieringen möjliggörs genom ett tekniskt system med noder som har utvecklats för ändamålet. De

svenska noderna tillhandahålls av Myndigheten för digital förvaltning, se avsnitt 4.3 och avsnitt 5. I maj 2020 var knappt 25 procent av de 470 offentliga organ som uppskattas vara berörda av förordningens krav anslutna till den svenska noden för inkommande gränsöverskridande elektronisk identifiering. För att Sverige ska uppfylla de krav på ömsesidigt erkännande som ställs i förordningen behöver alla aktörer som omfattas av kravet ansluta sig till den nod för inkommande elektronisk identifiering som Myndigheten för digital förvaltning tillhandahåller.

Det finns vidare tillkommande faktorer som stöder ett införande av en obligatorisk anslutning till noden. Europaparlamentets och rådets förordning (EU) 2018/1724 av den 2 oktober 2018 om inrättande av en gemensam digital ingång för tillhandahållande av information, förfaranden samt hjälp- och problemlösningstjänster och om ändring av förordning (EU) nr 1024/2012 (EU:s förordning om en gemensam digital ingång) ställer krav på att medlemsstaterna säkerställer att digitala tjänster finns för vissa förfaranden, till exempel att lämna in en inkomstskattedeklaration, och att dessa tjänster kan nås digitalt av invånare i andra medlemsstater. Förordningen har antagits med utgångspunkt i att individen ska identifiera sig med stöd av den tekniska infrastruktur som upprättats med anledning av EU:s förordning om elektronisk identifiering. Den aviserade översyn av EU:s förordning om elektronisk identifiering som ska presenteras under fjärde kvartalet 2020 kan resultera i ökade krav på tillgång till medlemsstaternas digitala tjänster. Det är viktigt att svenska offentliga aktörer är förberedda för sådana krav. Den fråga som *Tillväxtverket* lyft, om huruvida kravet på erkännande av utländska elektroniska identitetshandlingar – på grund av EU:s förordning om en gemensam digital ingång – inte bara avser autentiseringen utan även omfattar åtkomst till den digitala tjänsten blir föremål för behandling i samband med översynen.

Vidare har Sverige genom Nordiska ministerrådet för digitalisering och deklarationen Digital North förbundit sig till att arbeta för utvecklingen av en sammanhängande digital infrastruktur i regionen till nytta för medborgare, företag och offentliga förvaltningar. Det arbetet bygger i stor utsträckning på att svenska aktörer kan hantera elektronisk identifiering via noderna och att digitala tjänster i linje med EU-förordningen om en gemensam digital ingång kan fungera gränsöverskridande.

Det är mot denna bakgrund motiverat att införa en skyldighet för de offentliga organ som omfattas av förordningens krav på erkännande av utländska e-legitimationer att ansluta sig till den nod för inkommande gränsöverskridande identifiering som Myndigheten för digital förvaltning tillhandahåller.

Försäkringskassan avstyrker förslaget om obligatorisk anslutning och framhåller att en oberoende säkerhetsgranskning av det tekniska systemet för gränsöverskridande elektronisk identifiering behöver genomföras. Regeringen konstaterar dock att systemet numera har varit i drift i över två år. Dessutom har flera externa säkerhetsgranskningar genomförts, vilka har gett systemet ett mycket gott omdöme. Myndigheten för digital förvaltning, som ansvarar för tillhandahållandet av noderna, kommer även i fortsättningen att genomföra återkommande säkerhetsgranskningar av systemet.

Försvarsmakten föreslår att en nationell informationsvärdering genomförs innan lagreglering sker. Regeringen konstaterar att noden för gränsöverskridande elektronisk identifierings funktion i legitimeringsprocessen

är att möjliggöra interoperabilitet vid överföring av identitetsintyg. Den kan liknas vid en katalogtjänst som dirigerar identitetsintygets passage. Som behandlas i avsnitt 9 är det uppgifter om namn, födelsedatum och en unik identitetsbeteckning för den person identifieringen gäller som passerar noden. Noden fungerar inte som en s.k. gateway. Annan information än den som hänför sig till identitetsintyget passerar därför inte vidare in i de anslutna aktörernas system via noden. Noden fungerar inte heller som en brandvägg. De säkerhetsrisker som aktualiseras är de som följer av tillhandahållandet av digitala tjänster genom internet och påverkas inte av en anslutning till noden. Vilka användare som får åtkomst till nättjänsten och den säkerhetsnivå som krävs för åtkomst avgörs i nättjänsten. Det är därför viktigt att berörda aktörer bedriver ett systematiskt informationssäkerhetsarbete. Regeringen vill betona att alla aktörer som tillhandahåller nättjänster som ansluts till noden är ansvariga för att deras informationssäkerhetssystem uppfyller de krav som kan ställas på dem inom deras respektive verksamhetsområde. För utövare av säkerhetskänslig verksamhet finns bestämmelser om säkerhetsskydd i säkerhetsskyddslagen (2018:585) och säkerhetsskyddsförordningen (2018:658). För leverantörer av samhällsviktiga tjänster och digitala tjänster finns särskilt reglerade skyldigheter i lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster. Det finns även bestämmelser om krav på informationshanteringssystem i förordningen (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap. Det är mot denna bakgrund inte motiverat att genomföra en nationell informationsvärdering innan ett krav på anslutning till noden lagregleras.

Sammantaget bedömer regeringen att det i lagen (2016:561) med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering bör införas en skyldighet för de offentliga organ som omfattas av kravet i förordningen att ansluta sina nättjänster till den nod för inkommande gränsöverskridande elektronisk identifiering som Myndigheten för digital förvaltning tillhandahåller.

Försvarsmakten anför vidare att det av utredningens förslag är svårt att uttyda vilka myndigheter som omfattas av författningskraven. Regeringens förslag är utformat med utgångspunkt i att kravet på ömsesidigt erkännande i artikel 6 i EU:s förordning om elektronisk identifiering är direkt tillämpligt. Kravets innebörd bör därför inte vara föremål för tolkning i nationell lagstiftning. En aktör som tillhandahåller nättjänster måste själv ta ställning till om tjänsterna omfattas av förordningens tillämpningsområde och om de omfattas av lagens bestämmelser om skyldighet att ansluta till noden. Myndigheten för digital förvaltning har i uppgift att lämna stöd och information till myndigheter i frågor som rör gränsöverskridande elektronisk identifiering enligt EU:s förordning om elektronisk identifiering.

Skyldigheten att ansluta till noden bör inte gälla om detta skulle medföra risk för skada för totalförsvaret eller Sveriges säkerhet i övrigt. Det ankommer på varje berörd aktör att bedöma huruvida en anslutning till noden medför en sådan risk. Det bör dock understrykas att undantaget från skyldigheten att ansluta till noden inte påverkar giltigheten av det krav på erkännande av medel för elektronisk identifiering som följer av artikel 6 i EU:s förordning om elektronisk identifiering. Om en aktör som omfattas av kravet bedömer att en anslutning till noden inte bör ske eller att en

befintlig anslutning bör avbrytas med hänsyn till risk för skada för totalförsvaret eller Sveriges säkerhet i övrigt, får alltså aktören ordna tillgång till de tekniska lösningar som krävs för erkännande på ett annat sätt.

Myndigheter som bedriver sådan verksamhet som avser totalförsvaret eller Sveriges säkerhet i övrigt bör helt undantas från skyldigheten att ansluta till noden. Avgränsningen av vilka myndigheter som ska undantas görs lämpligen i förordning. Regeringen bör därför få meddela föreskrifter om undantag från anslutningsskyldigheten i fråga om verksamhet som avser totalförsvaret eller Sveriges säkerhet i övrigt.

Som *E-legitimationsnämnden* påpekar kräver obligatorisk anslutning till noden att den ansvariga myndigheten kan reglera villkoren för anslutningen. Den ansvariga myndigheten bör bl.a. få ställa krav på säkerhet som en aktör ska uppfylla för att ansluta sina nättjänster till noden. I lagen bör det därför anges att regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om anslutning till noden. Regeringen avser att ge Myndigheten för digital förvaltning rätt att meddela sådana föreskrifter.

Övriga offentliga organ och privata aktörer får ansluta till noden

Som utredningen anför kan även privata aktörer och offentliga organ som inte omfattas av förordningens krav på erkännande ha ett intresse av att kunna ta emot användare från andra medlemsstater i sina nättjänster. Det gäller sådana offentliga organ som inte kräver elektronisk identifiering på tillitsnivå väsentlig eller hög för inloggning i sina nättjänster utan där det räcker med en lägre tillitsnivå. Regeringen anser att det är angeläget att varje medlemsstat bidrar till att underlätta gränsöverskridande elektronisk identifiering. Utländska personer ska på ett tillförlitligt sätt kunna använda sitt lands godkända e-legitimation vid användning av svenska tjänster, under förutsättning att det finns ett regelverk som garanterar säkerhetsnivå och ansvar (se prop. 2014/15:1 utgiftsområde 22 s. 150 f.). För att uppfylla de kommande kraven på att digitala tjänster för vissa förfaranden ska kunna nås av invånare i andra medlemsstater i EU:s förordning om en gemensam digital ingång behöver identifiering med utländska medel som har blivit godkända för gränsöverskridande elektronisk identifiering vara möjlig. De kommande kraven kan i vissa fall avse offentliga digitala tjänster som inte omfattas av den anslutningsskyldighet som föreslås här.

De utländska medel som har blivit godkända för gränsöverskridande elektronisk identifiering enligt förfarandet i EU:s förordning om elektronisk identifiering bör i ljuset av detta även kunna användas för identifiering i övriga offentliga nättjänster och i privata aktörers tjänster. För att möjliggöra det bör Myndigheten för digital förvaltning på begäran även ansluta offentliga aktörer som inte omfattas av förordningens krav och privata aktörer till noden för inkommande gränsöverskridande elektronisk identifiering. Regeringen avser att i förordning ge Myndigheten för digital förvaltning en sådan uppgift. Som anges ovan avser regeringen att ge Myndigheten för digital förvaltning rätt att meddela föreskrifter om anslutning till noden. Genom sådana föreskrifter kan det bl.a. ställas krav på säkerhet som en aktör som inte omfattas av anslutningsskyldigheten ska uppfylla för att få ansluta sina nättjänster till noden.

De svenska nodernas utveckling och drift finansieras med offentliga medel, och anslutning av aktörer till noderna kräver arbetsinsatser av

Myndigheten för digital förvaltning. Det är därför motiverat med ett avgiftssystem som säkerställer att det offentliga inte belastas med kostnader för de privata aktörernas användning av noden. Myndigheten bör därför ges rätt att ta ut avgifter av de privata aktörer som har anslutit sig till noden för inkommande gränsöverskridande elektronisk identifiering som myndigheten tillhandahåller. Regeringen avser att ge Myndigheten för digital förvaltning rätt att ta ut sådana s.k. frivilliga avgifter från de privata aktörerna.

7 Underrättelse om händelser av betydelse för funktionaliteten och säkerheten i noderna

Regeringens förslag: Den som är ansluten till en svensk nod för inkommande eller utgående gränsöverskridande elektronisk identifiering ska så snart som möjligt underrätta den myndighet som ansvarar för noden om händelser som kan ha betydelse för nodens funktionalitet eller säkerhet.

Regeringen eller den myndighet som regeringen bestämmer ska få meddela föreskrifter om underrättelseskyldigheten.

Utredningens förslag: Överensstämmer i huvudsak med regeringens förslag. Utredningen föreslår inte något bemyndigande.

Remissinstanserna: De flesta av de remissinstanser som kommenterar förslaget tillstyrker det eller har ingen invändning mot det. *Försvarets radioanstalt*, *Myndigheten för samhällsskydd och beredskap* och *Säkerhetspolisen* anser att underrättelseskyldigheten inte bör gälla i de fall en sådan skyldighet följer av annan författning.

Skälen för regeringens förslag: De noder som upprättats med anledning av EU:s förordning om elektronisk identifiering är en del av den svenska digitala infrastrukturen och möjliggör gränsöverskridande elektronisk identifiering. Noderna är dock inte att betrakta som samhällsviktiga enligt Europaparlamentets och rådets direktiv (EU) 2016/1148 av den 6 juli 2016 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen. För att Myndigheten för digital förvaltning ska kunna upprätthålla en god informationssäkerhetsnivå är det av vikt att de aktörer som använder sig av noderna rapporterar händelser som kan ha betydelse för nodernas funktionalitet eller säkerhet till myndigheten.

Försvarets radioanstalt, *Myndigheten för samhällsskydd och beredskap* och *Säkerhetspolisen* påpekar att det finns flera författningar som ställer krav på rapportering vid it-relaterade incidenter, bl.a. säkerhetsskyddslagen (2018:585). Myndigheterna framhåller att det är viktigt att det inte sker en fragmentering av rapporteringsskyldigheten vid incidenter i it-system, eftersom det skulle göra det svårt att överblicka informationssäkerhetsområdet. Vidare påpekar de att det förhållandet att samma incident kan rapporteras till flera tillsynsmyndigheter kan försämra möjlig-

heten till en tillbörlig reaktion. Regeringen instämmer i att det är viktigt att det inte sker en fragmentering av informationssäkerhetsområdet. Myndigheten för digital förvaltning behöver dock som ansvarig för infrastrukturen för gränsöverskridande elektronisk identifiering snabbt få kännedom om brister i säkerheten eller funktionaliteten i noderna. Att samma händelse i vissa fall kan komma att rapporteras till olika myndigheter bör därför inte leda till en mindre tillförlitlig hantering av incidenten inom myndigheternas egna ansvarsområden.

Bestämmelser som närmare preciserar vad underrättelseskyldigheten avser blir både detaljerade och av teknisk karaktär. De är därför mindre lämpliga att regleras i lag. I lagen bör det i stället anges att regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om underrättelseskyldigheten. Regeringen avser att i förordning ge Myndigheten för digital förvaltning rätt att meddela föreskrifter om den.

8 Anmälan av system för elektronisk identifiering

Regeringens förslag: Regeringen eller den myndighet som regeringen bestämmer ska få meddela föreskrifter om vilka krav som ska gälla för att system för elektronisk identifiering ska anmälas för gränsöverskridande elektronisk identifiering enligt EU:s förordning om elektronisk identifiering och de rättsakter som meddelas med stöd av förordningen.

Regeringens bedömning: Myndigheten för digital förvaltning bör ansvara för anmälan av system för elektronisk identifiering enligt EU:s förordning om elektronisk identifiering och de rättsakter som meddelas med stöd av förordningen.

Myndigheten bör också ansvara för åtgärder vid säkerhetsincidenter enligt artikel 10 i EU:s förordning om elektronisk identifiering.

Utredningens förslag: Överensstämmer i huvudsak med regeringens förslag. Utredningen föreslår att kraven ska anges direkt i lagen.

Remissinstanserna: Remissinstanserna tillstyrker förslaget eller har ingen invändning mot det.

Skälen för regeringens förslag och bedömning: För att en svensk e-legitimation ska kunna användas inom infrastrukturen för EU:s förordning om elektronisk identifiering måste ett svenskt system för elektronisk identifiering, där minst ett medel för elektronisk identifiering (e-legitimation) ingår, anmälas enligt det förfarande som framgår av artiklarna 7–9 i förordningen och de rättsakter som meddelats med stöd av den. Kraven är i huvudsak av teknisk karaktär och processen bygger på att en eller flera aktörer som den anmälande medlemsstaten har pekat ut utför granskningar på begäran av den utfärdare som vill få sin e-legitimation anmäld. Är utfallet av granskningen positiv, kan systemet för elektronisk identifiering anmälas till Europeiska kommissionen. Systemet tas därefter upp i den förteckning över system för elektronisk identifiering som anmälts, vilken

offentliggörs i Europeiska unionens officiella tidning. Därefter kan e-legitimationen användas för åtkomst till nättjänster i andra medlemsstater.

Myndigheten för digital förvaltning ansvarar för de svenska noderna för gränsöverskridande elektronisk identifiering. Som *Statskontoret* framför är det lämpligt att samma myndighet ansvarar för anmälan av svenska system för gränsöverskridande identifiering. På så sätt samlas rätt kompetens hos Myndigheten för digital förvaltning och myndigheten får möjlighet att överblicka hela den process för elektronisk identifiering som följer av EU:s förordning om elektronisk identifiering.

Myndigheten bör av samma skäl ansvara för åtgärder vid säkerhetsincidenter enligt artikel 10 i EU:s förordning om elektronisk identifiering. Det gäller bland annat att tillfälligt upphäva eller återkalla en gränsöverskridande autentisering och att informera kommissionen och andra medlemsstater om att ett system för elektronisk identifiering har dragits tillbaka på grund av säkerhetsbrister.

Utredningen föreslår att myndighetens ansvarsområde ska pekas ut i lag. Regeringen anser dock att detta med fördel regleras i förordning. Bestämmelser om Myndigheten för digital förvaltnings ansvar för anmälan av system för elektronisk identifiering och för åtgärder vid säkerhetsincidenter bör därför införas i förordning.

I EU:s förordning om elektronisk identifiering och de rättsakter som meddelas med stöd av den finns bl.a. regler för hur en anmälan ska gå till och de krav som ställs på de system för elektronisk identifiering som medlemsstater anmäler. Kraven anges särskilt i kommissionens genomförandebeslut (EU) 2015/1984 av den 3 november 2015 om förutsättningar, format och förfaranden för anmälan enligt artikel 9.5 i Europaparlamentets och rådets förordning (EU) nr 910/2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden.

Som *E-legitimationsnämnden* påpekar kan det finnas behov av att ställa ytterligare krav med hänsyn till det ansvar som medlemsstaterna tar som garant för att det anmälda systemet uppfyller förordningens krav. Utredningen föreslår ett antal lagkrav som ett svenskt medel för elektronisk identifiering bör uppfylla för att bli anmält för gränsöverskridande identifiering. Medlet ska enligt utredningens förslag bl.a. ingå i valfrihetssystem enligt lagen (2013:311) om valfrihetssystem i fråga om tjänster för elektronisk identifiering och vara utfärdat av en aktör som har tecknat försäkring som täcker ersättning för det skadeståndsansvar som följer av artikel 7 i EU:s förordning om elektronisk identifiering.

De närmare krav som ska ställas för en anmälan är av så detaljerad och teknisk karaktär att de lämpar sig mindre väl att regleras i lag. De bör i stället fastställas i förordning eller myndighetsföreskrifter. Det ger ökad flexibilitet inför eventuella ändringar av bl.a. tekniska specifikationer och standarder. I lagen bör det därför anges att regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om krav för att system för elektronisk identifiering ska anmälas för gränsöverskridande elektronisk identifiering enligt EU:s förordning om elektronisk identifiering och de rättsakter som meddelas med stöd av förordningen. Regeringen avser att ge Myndigheten för digital förvaltning rätt att meddela sådana föreskrifter.

9 Myndigheten för digital förvaltnings behandling av personuppgifter

Regeringens bedömning: Det behövs inga särskilda bestämmelser för utpekande av personuppgiftsansvaret och för behandling av personuppgifter i Myndigheten för digital förvaltnings verksamhet i frågor som rör hanteringen av noderna för gränsöverskridande elektronisk identifiering. Bestämmelserna i dataskyddsförordningen, dataskyddslagen och EU:s förordning om elektronisk identifiering och de rättsakter som har meddelats med stöd av den är tillräckliga.

Utredningens förslag och bedömning överensstämmer inte med regeringens bedömning. Utredningen föreslår att särskilda bestämmelser införs som pekar ut nodmyndigheten som personuppgiftsansvarig för behandlingen av personuppgifter i noden och som anger att myndigheten får behandla de personuppgifter som kommer till noden. Vidare föreslår utredningen att nodmyndigheten ska ha rätt att behandla tekniska uppgifter om de aktörer vars uppgifter ska behandlas av noden och de personuppgifter som är nödvändiga för att säkerställa behörigheter för aktörernas ombud.

Remissinstanserna: De remissinstanser som kommenterar förslaget tillstyrker eller har ingen invändning mot det.

Skälen för regeringens bedömning

Regelverk för skydd för behandling av personuppgifter

Den 26 april 2016 antogs Europaparlamentets och rådets förordning (EU) 2016/679 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/EG (allmän dataskyddsförordning), nedan kallad EU:s dataskyddsförordning. Dataskyddsförordningen tillämpas från och med den 25 maj 2018. Samma dag upphävdes personuppgiftslagen (1998:204), och lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning, nedan kallad dataskyddslagen, trädde i kraft.

EU:s dataskyddsförordning utgör den generella regleringen av personuppgiftsbehandling inom unionen. Den är tillämplig på sådan behandling av personuppgifter som helt eller delvis sker på automatisk väg samt på annan behandling än automatisk av personuppgifter som ingår i eller kommer att ingå i ett register. Från dataskyddsförordningens tillämpningsområde undantas bl.a. behandling av personuppgifter som utgör ett led i en verksamhet som inte omfattas av unionsrätten eller som utförs av medlemsstaterna när de bedriver verksamhet som omfattas av den gemensamma utrikes- och säkerhetspolitiken.

I EU:s dataskyddsförordning finns flera bestämmelser som förutsätter eller ger utrymme för kompletterande nationella bestämmelser av olika slag. I Sverige finns kompletterande bestämmelser som behövs eller är lämpliga och som är av generell karaktär i dataskyddslagen. I dataskyddslagen förtydligas bl.a. under vilka förutsättningar personuppgifter får behandlas med stöd av dataskyddsförordningen. Vidare innehåller lagen bestämmelser om bl.a. rapportering av personuppgiftsincidenter, administrativa

sanktionsavgifter, begränsningar av de registrerades rättigheter, skadestånd och överklagande.

EU:s dataskyddsförordning och dataskyddslagen är tillämpliga på behandling av personuppgifter vid Myndigheten för digital förvaltning.

Personuppgiftsansvar vid tillhandahållandet av noder för gränsöverskridande elektronisk identifiering

Den som är personuppgiftsansvarig enligt EU:s dataskyddsförordning har en skyldighet att se till att personuppgifter behandlas i enlighet med tillämpliga bestämmelser. Enskilda ska alltid kunna vända sig till den personuppgiftsansvarige för att göra sina rättigheter gällande.

Med personuppgiftsansvarig avses en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som ensamt eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter (artikel 4.7). Den personuppgiftsansvarige har en rad skyldigheter enligt förordningen, bl.a. ska den se till och kunna visa att principerna om behandlingen av personuppgifter i artikel 5 följs (se närmare om principerna nedan). Ett annat exempel är den personuppgiftsansvariges skyldighet att genomföra lämpliga tekniska och organisatoriska åtgärder för att säkerställa och kunna visa att behandlingen av personuppgifter utförs i enlighet med förordningen (artikel 24).

För myndigheter är en reglering av vem som är personuppgiftsansvarig av störst vikt när det är fråga om en myndighet som är del av en större myndighetsstruktur, om det finns utrymme för tvekan kring vilken myndighet som har ansvaret för behandlingen av personuppgifter. En sådan särskild reglering av personuppgiftsansvaret kan också i andra fall förenkla för rättstillämparen och undvika otydligheter i fråga om identifiering av den ansvarige (jfr prop. 2019/20:106 s. 34).

De uppdrag som Myndigheten för digital förvaltning ska utföra och myndighetens befogenheter framgår bl.a. av myndighetens instruktion. Enligt 3 § 4 förordningen (2018:1486) med instruktion för Myndigheten för digital förvaltning ansvarar myndigheten för de svenska förbindelsepunkterna (noderna) för gränsöverskridande elektronisk identifiering i enlighet med EU:s förordning om elektronisk identifiering samt rättsakter som har meddelats med stöd av förordningen. Som anges i avsnitt 5 innefattar myndighetens ansvar enligt instruktionen även tillhandahållandet av noderna för elektronisk identifiering. Vidare bedömer regeringen att myndigheten ska ansvara för anmälan av system för elektronisk identifiering enligt EU:s förordning om elektronisk identifiering och de rättsakter som meddelas med stöd av förordningen och få meddela föreskrifter om anslutning till noderna för elektronisk identifiering (se avsnitt 6 och 8). Myndigheten för digital förvaltnings uppgifter och ansvar för frågor som rör noderna för gränsöverskridande elektronisk identifiering är därmed tydligt utpekade. Det har inte framkommit någon osäkerhet i fråga om vem som har personuppgiftsansvaret. Regeringen bedömer därför att det inte finns något behov av att införa särskilda bestämmelser om att Myndigheten för digital förvaltning är personuppgiftsansvarig för den behandling av personuppgifter som sker vid tillhandahållandet av noder för gränsöverskridande elektronisk identifiering.

Rättslig grund och principer för behandling av personuppgifter i myndighetens verksamhet i fråga om noderna för gränsöverskridande elektronisk identifiering

EU:s dataskyddsförordning utgår från att varje behandling av personuppgifter måste vila på en rättslig grund. En uttömmande uppräkning av de rättsliga grunderna finns i artikel 6.1. En av de rättsliga grunderna är att behandlingen är nödvändig för att utföra en uppgift av allmänt intresse eller som ett led i den personuppgiftsansvariges myndighetsutövning (artikel 6.1 e).

Enligt artikel 6.3 andra stycket ska vidare syftet med behandlingen fastställas i den rättsliga grunden eller, i fråga om behandling enligt artikel 6.1 e, vara nödvändig för att utföra en uppgift av allmänt intresse eller som ett led i den personuppgiftsansvariges myndighetsutövning. Av artikel 6.3 framgår vidare att vid behandling enligt artikel 6.1 c och e ska den rättsliga grunden fastställas i unionsrätten eller i nationell rätt. Där anges också att den rättsliga grunden kan innehålla särskilda bestämmelser för att anpassa tillämpningen av bestämmelserna i dataskyddsförordningen.

I dataskyddslagen tydliggörs att en uppgift av allmänt intresse utgör en rättslig grund för behandling av personuppgifter enligt artikel 6.1 e i dataskyddsförordningen om uppgiften följer av lag eller annan författning, av kollektivavtal eller av beslut som har meddelats med stöd av lag eller annan författning eller är ett led i den personuppgiftsansvariges myndighetsutövning om myndighetsutövningen sker enligt lag eller annan författning (2 kap. 2 §).

I förarbetena till dataskyddslagen uttalas att den verksamhet som en statlig eller kommunal myndighet bedriver inom ramen för sin befogenhet är av allmänt intresse och att det vanligen är den rättsliga grunden i artikel 6.1 e i dataskyddsförordningen som bör tillämpas av myndigheter. Detta utesluter dock inte att andra rättsliga grunder samtidigt kan vara tillämpliga i vissa fall (prop. 2017/18:105 s. 56 f.).

I artikel 5 i EU:s dataskyddsförordning ställs det vidare upp ett antal allmänna principer för behandlingen. Personuppgifterna ska bl.a. behandlas på ett lagligt, korrekt och öppet sätt i förhållande till den registrerade. De ska samlas in för särskilda, uttryckligt angivna och berättigade ändamål. De får inte senare behandlas på ett sätt som är oförenligt med dessa ursprungliga ändamål. Uppgifterna ska vidare vara adekvata, relevanta och inte för omfattande i förhållande till de ändamål för vilka de behandlas. De ska vara korrekta och, om nödvändigt, uppdaterade. Alla rimliga åtgärder måste vidtas för att säkerställa att personuppgifter som är felaktiga i förhållande till de ändamål för vilka de behandlas raderas eller rättas utan dröjsmål. Vidare får personuppgifter inte förvaras under en längre tid än vad som är nödvändigt och de måste behandlas på ett sätt som säkerställer lämplig säkerhet. Artiklarna 5 och 6 är kumulativa. Det innebär att en personuppgiftsbehandling måste ha stöd i någon av de rättsliga grunderna i artikel 6 och alla principer i artikel 5 ska följas.

Av EU:s förordning om elektronisk identifiering följer en skyldighet för Sverige att under vissa i förordningen beskrivna förhållanden erkänna utländska elektroniska identitetshandlingar i svenska nättjänster. För att kunna göra det krävs att det i Sverige finns noder som klarar av att dirigera trafiken av inkommande elektroniska identitetshandlingar för att kunna

bekräfta identiteten på de användare som vill ha tillträde till svenska nättjänster. Det kräver i sin tur behandling av de personuppgifter som anges i kommissionens genomförandeförordning (EU) 2015/1501. Inga personuppgifter utöver dem som anges där får behandlas av noden. I bilagan till genomförandeförordningen anges att en minimiuppsättning av uppgifter för en fysisk person ska innehålla följande: nuvarande efternamn, nuvarande förnamn, födelsedatum samt en unik identitetsbeteckning som satts samman av den utsändande medlemsstaten i enlighet med de tekniska specifikationerna för gränsöverskridande identifiering och som är mest beständig i tid. En minimiuppsättning för en fysisk person kan dessutom innehålla ett eller flera av följande: förnamn och efternamn vid födseln, födelseort, nuvarande adress och kön. Myndigheten måste vidare se till att de personuppgifter som behandlas hålls korrekta och att säkerheten upprätthålls för att skydda integritet och konfidentialitet. I artikel 6.2 i samma genomförandeförordning anges att noderna inte får lagra några personuppgifter, utom för det ändamål som anges i artikel 9.3. I artikel 9.3 anges att nodoperatören ska lagra uppgifter så att det, vid en incident, går att rekonstruera ordningsföljden i utbytet av meddelanden för att fastställa platsen för incidenten och dess art.

När Myndigheten för digital förvaltning behandlar personuppgifter inom ramen för sitt uppdrag att ansvara och tillhandahålla noderna för gränsöverskridande elektronisk identifiering sker detta för att utföra uppgifter av allmänt intresse (artikel 6.1 e) som följer av lag eller annan författning. Myndighetens behandling av personuppgifter vid tillhandahållandet av noderna är nödvändig för att utföra en uppgift av allmänt intresse och därigenom möjliggöra den gränsöverskridande elektroniska identifiering som följer av EU:s förordning om elektronisk identifiering. Därmed är även kravet i artikel 6.3 uppfyllt.

Bestämmelserna i EU:s förordning om elektronisk identifiering och kommissionens genomförandeförordning (EU) 2015/1501 föreskriver hur noderna ska tillhandahållas och hur personuppgifterna ska behandlas i noderna. Som nämnts ovan framgår ändamålet för behandlingen av personuppgifter, vilka personuppgifter som får behandlas, skyddet av personuppgifter och vad som gäller i fråga om lagring av personuppgifter av rättsakterna.

Regeringen bedömer att 3 § 4 förordningen (2018:1486) med instruktion för Myndigheten för digital förvaltning i förening med bestämmelserna i EU:s förordning om elektronisk identifiering och kommissionens genomförandeförordning (EU) 2015/1501 reglerar nödvändig personuppgiftsbehandling i frågor som rör noderna för gränsöverskridande elektronisk identifiering på ett tydligt sätt. Det finns därför inte behov av att införa särskilda bestämmelser om sådan personuppgiftsbehandling.

10 Ikraftträdande- och övergångsbestämmelser

Regeringens förslag: Lagändringarna ska träda i kraft den 1 juni 2021.

Utredningens förslag överensstämmer inte med regeringens. Utredningen föreslår ett ikraftträdande den 29 september 2018.

Remissinstanserna har inga synpunkter**.**

Skälen för regeringens förslag: För att Sverige ska kunna uppfylla förordningens krav är det viktigt att de berörda aktörerna ansluter sina nättjänster till noden för inkommande gränsöverskridande elektronisk identifiering som Myndigheten för digital förvaltning tillhandahåller. Även om anslutningen i de flesta fall inte är resurskrävande, bör hänsyn tas till att situationen hos många offentliga aktörer är mycket ansträngd med anledning av utbrottet av covid-19. Ett lämpligt datum för ikraftträdande är därför den 1 juni 2021.

11 Konsekvenser

11.1 Konsekvenser för statliga myndigheter

Bestämmelserna om ömsesidigt erkännande av medel för elektronisk identifiering i EU:s förordning om elektronisk identifiering innebär i praktiken att offentliga organ som för åtkomst till sina nättjänster ställer krav på användning av en e-legitimation måste erkänna medel för elektronisk identifiering utfärdade i en annan medlemsstat för autentisering i tjänsten.

Kravet på de offentliga organen att ansluta nättjänster till den nod för inkommande gränsöverskridande identifiering som tillhandahålls av Myndigheten för digital förvaltning innebär att organen kommer att behöva utföra en viss verksamhetsutveckling, i huvudsak av it-relaterad karaktär. Anslutningsprocessen är dock relativt enkel. Tidsåtgången för anslutningen bedöms variera från några timmar till högst några dagar. Processen behöver i normalfallet bara genomföras en gång. För aktörer som har flera nättjänster finns det lösningar som möjliggör en gemensam anslutning för alla tjänster samtidigt. Regeringen bedömer att de berörda statliga myndigheterna kan genomföra åtgärderna inom befintliga utgiftsramar, med försumbar påverkan på myndighetens verksamhet.

Myndigheten för digital förvaltning har i uppgift att ansvara för den offentliga förvaltningens tillgång till infrastruktur och tjänster för elektronisk identifiering och underskrift och att främja användningen av sådana tjänster. Därutöver ska myndigheten lämna stöd och information till myndigheter i frågor som rör gränsöverskridande elektronisk identifiering enligt EU:s förordning om elektronisk identifiering. Anslutning av nya offentliga aktörer till noden för inkommande gränsöverskridande identifiering ingår alltså i myndighetens fortlöpande verksamhet. Med hänsyn till myndighetens erfarenhet och kunskap på området bedöms myndigheten kunna hantera anslutningarna inom ordinarie verksamhet och befintliga utgiftsramar. Privata aktörers anslutning till och användning av noden är frivillig. För att kunna hantera arbetet för sådan anslutning föreslås myndigheten få rätt att ta ut avgifter från sådana privata aktörer.

Övriga förslag – om underrättelseskyldighet i fråga om händelser av betydelse för funktionaliteten och säkerheten i noderna och om anmälan av

system för elektronisk identifiering – får främst konsekvenser för Myndigheten för digital förvaltning. Myndigheten behöver ta fram föreskrifter och anpassa sin verksamhet för att sköta anmälan av system för elektronisk identifiering. Även dessa uppgifter bedöms kunna hanteras inom befintliga utgiftsramar.

Förslagen bedöms inte öka statens kostnader. Staten bör inte bekosta de gränsöverskridande transaktioner som genomförs av svenska e-legitimationsutfärdare, vilket utesluter risken att en kraftigt ökad användning skulle leda till en ökning av statens kostnader.

11.2 Konsekvenser för kommuner, regioner och andra offentliga organ som berörs

Även för kommuner, regioner och andra offentliga organ som berörs – till exempel vissa statliga bolag – bedöms de åtgärder som kravet på anslutning till noden som Myndigheten för digital förvaltning tillhandahåller och underrättelseskyldigheten medför rymmas inom ramen för normalt verksamhetsarbete och inom befintliga ekonomiska ramar. *Sveriges Kommuner och Regioner*, *SKR* (tidigare Sveriges Kommuner och Landsting) efterfrågar i sitt remissvar en tydlig och utförlig vägledning till stöd för bl.a. kommuner och regioner i deras arbete för att erkänna utländska e-legitimationer i sina digitala tjänster. *SKR* har därefter tagit fram en vägledning som beskriver tillvägagångssättet för anslutning till noden och de olika alternativ som finns beroende på hur aktören har valt att bygga sin eller sina digitala tjänster. För en kommun med flera förvaltningar som har separata digitala tjänster finns exempelvis lösningar som möjliggör gemensam anslutning av alla digitala tjänster vid samma tillfälle. Anslutningen behöver bara ske en gång. Tidsåtgången för anslutningsarbetet beror på valt tillvägagångssätt och varierar mellan några timmar och ett par dagar. Kostnaden för anslutningen varierar beroende på vilken typ av lösning för digitala tjänster aktören har. Vidare har Myndigheten för digital förvaltning, och tidigare E-legitimationsnämnden, haft i uppdrag att sprida information om EU:s förordning om elektronisk identifiering och om anslutningsprocessen. De berörda aktörerna bör därför ha kännedom om EU-förordningen och om var information om anslutningsprocessen finns.

Enligt 14 kap. 3 § regeringsformen bör en inskränkning i den kommunala självstyrelsen inte gå utöver vad som är nödvändigt med hänsyn till de ändamål som har föranlett den. Förslaget om obligatorisk anslutning till noden för inkommande gränsöverskridande elektronisk identifiering påverkar den kommunala självstyrelsen. Anslutningskravet fråntar kommuner och regioner möjligheten att utveckla egna tekniska lösningar för att uppfylla de krav som förordningen ställer på dem. Som framgår av avsnitt 6 är det ett begränsat antal aktörer som hittills har vidtagit nödvändiga åtgärder för att uppfylla förordningens krav på erkännande av medel för elektronisk identifiering. Av de kommuner och regioner som kräver e-legitimation på tillitsnivå hög eller väsentlig för åtkomst till sina digitala tjänster bedöms enbart en tredjedel ha möjliggjort för gränsöverskridande elektronisk identifiering. Förslagets ändamål att Sverige ska leva upp till de krav EU:s förordning om elektronisk identifiering ställer bedöms

emellertid inte kunna uppnås på ett mindre ingripande sätt. Vidare anses en anslutning till den nod som det offentliga åtar sig att upprätthålla via Myndigheten för digital förvaltning vara det mest effektiva sättet att uppnå ändamålet. Regeringen bedömer mot denna bakgrund att inskränkningen i den kommunala självstyrelsen är proportionerlig.

11.3 Konsekvenser för näringsliv och privatpersoner

Privata aktörer kommer att få en möjlighet att ansluta sina digitala tjänster till noden för inkommande gränsöverskridande elektronisk identifiering som Myndigheten för digital förvaltning tillhandahåller. De kan på så sätt ta emot medel för elektronisk identifiering utfärdade i andra medlemsstater i sina digitala tjänster, vilket kan underlätta för digital kommunikation och leda till nya digitala tjänster då nya målgrupper i andra länder kan nås.

Privata utfärdare av medel för elektronisk identifiering får också möjlighet att tillhandahålla e-legitimationstjänster i andra länder via infrastrukturen för elektronisk identifiering. Detta kan i sin tur öka möjligheterna till e-handel och tillgång till digitala tjänster inom EU för både företag och privatpersoner.

Att svenska e-legitimationer kan användas för gränsöverskridande elektronisk identifiering ger enskilda möjlighet att använda digitala tjänster i andra EU-medlemsstater, vilket kan minska behovet av resor, underlätta snabbare service och minska kostnader för pappershantering.

11.4 Övriga konsekvenser

Förslagen förväntas inte att få några konsekvenser för jämställdheten mellan kvinnor och män men kan få en positiv miljöpåverkan om möjligheterna till digital kommunikation med offentliga organ i andra stater ökar. Förslagen bidrar till Sveriges möjligheter att uppfylla kraven i EU:s förordning om en gemensam digital ingång.

12 Författningskommentar

Förslaget till lag om ändring i lagen (2016:561) med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering

Elektronisk identifiering

1 a § *Ett offentligt organ som tillhandahåller en nättjänst ska ansluta tjänsten till den svenska förbindelsepunkten (noden) för inkommande gränsöverskridande elektronisk identifiering, om nättjänsten omfattas av kravet på erkännande av medel för elektronisk identifiering som utfärdats i en annan medlemsstat enligt artikel 6 i EU:s förordning om elektronisk identifiering. Detta gäller dock inte om anslutningen medför risk för skada för totalförsvaret eller Sveriges säkerhet i övrigt.*

Regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om anslutning till noden.

Regeringen får meddela föreskrifter om undantag från anslutningsskyldigheten i fråga om verksamhet som avser totalförsvaret eller Sveriges säkerhet i övrigt.

Paragrafen, som är ny, reglerar offentliga organs skyldighet att ansluta sina nättjänster till den svenska noden för inkommande gränsöverskridande elektronisk identifiering. Övervägandena finns i avsnitt 6.

Enligt *första stycket första meningen* ska ett offentligt organ som omfattas av kravet på erkännande av medel för elektronisk identifiering i artikel 6 i EU:s förordning om elektronisk identifiering ansluta till den svenska förbindelsepunkten (noden) för inkommande gränsöverskridande elektronisk identifiering. Noden tillhandahålls av Myndigheten för digital förvaltning. Vilka aktörer som avses med offentligt organ definieras i artikel 3.7 i EU:s förordning om elektronisk identifiering, jfr 1 § andra stycket. Förordningens krav gäller för sådana nättjänster där det krävs elektronisk identifiering på tillitsnivå väsentlig eller hög för inloggning. Tillitsnivåerna för system för elektronisk identifiering beskrivs i artikel 8 i EU:s förordning om elektronisk identifiering. Ett offentligt organ som tillhandahåller nättjänster måste själv ta ställning till om en nättjänst omfattas av förordningens tillämpningsområde och av lagens bestämmelser om skyldighet att ansluta till noden.

I *andra meningen* finns ett undantag från anslutningsskyldigheten i fall då anslutningen medför risk för skada för totalförsvaret eller Sveriges säkerhet i övrigt. Det ankommer på varje berörd aktör att göra en bedömning av huruvida en anslutning till noden medför en sådan risk. Undantaget påverkar inte giltigheten av kravet på ömsesidigt erkännande av medel för elektronisk identifiering som följer av artikel 6 i EU:s förordning om elektronisk identifiering.

Andra stycket innehåller ett bemyndigande för regeringen eller den myndighet som regeringen bestämmer att meddela föreskrifter om anslutningen till noden. Genom sådana föreskrifter kan det exempelvis ställas krav på säkerhet som en aktör ska uppfylla för att ansluta sina nättjänster till

noden. Sådana krav för anslutning kan även riktas mot en aktör som inte omfattas av anslutningsskyldigheten i första stycket.

I *tredje stycket* finns ett bemyndigande för regeringen att meddela föreskrifter om undantag från anslutningsskyldigheten i fråga om verksamhet som avser totalförsvaret eller Sveriges säkerhet i övrigt. Genom en sådan föreskrift kan myndigheter som bedriver verksamhet som avser totalförsvaret eller Sveriges säkerhet i övrigt helt undantas från anslutningsskyldigheten.

1 b § *Den som är ansluten till en svensk nod för inkommande eller utgående gränsöverskridande elektronisk identifiering ska så snart som möjligt underrätta den myndighet som ansvarar för noden om händelser som kan ha betydelse för nodens funktionalitet eller säkerhet.*

Regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om underrättelseskyldigheten.

Paragrafen, som är ny, reglerar en underrättelseskyldighet för aktörer anslutna till någon av noderna för gränsöverskridande elektronisk identifiering som Myndigheten för digital förvaltning tillhandahåller. Övervägandena finns i avsnitt 7.

I *första stycket* finns en skyldighet för aktörer anslutna till en nod för gränsöverskridande elektronisk identifiering att underrätta Myndigheten för digital förvaltning om händelser som kan ha betydelse för funktionaliteten eller säkerheten i noden. Det avser händelser som kan påverka den fysiska noden och dess funktion eller de processer som sker i noden. Bestämmelsen påverkar inte underrättelseskyldighet som följer av andra författningar, t.ex. den i säkerhetsskyddslagen (2018:585).

Andra stycket innehåller ett bemyndigande till regeringen eller den myndighet som regeringen bestämmer att meddela föreskrifter om underrättelseskyldigheten. Genom sådana föreskrifter kan exempelvis preciseras vilka händelser som anses påverka funktionaliteten respektive säkerheten i noderna och hur underrättelsen ska ske.

1 c § *Regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om vilka krav som ska gälla för att ett system för elektronisk identifiering ska anmälas för gränsöverskridande elektronisk identifiering enligt EU:s förordning om elektronisk identifiering och de rättsakter som meddelas med stöd av förordningen.*

I paragrafen, som är ny, ges regeringen eller den myndighet som regeringen bestämmer ett bemyndigande att meddela föreskrifter om de krav som ska gälla för att ett system för elektronisk identifiering ska anmälas för gränsöverskridande elektronisk identifiering. Övervägandena finns i avsnitt 8.

Föreskrifterna kan exempelvis avse krav gällande säkerheten inom systemet för elektronisk identifiering, krav på kvalitetsgranskning, att medlet för elektronisk identifiering ska ingå i ett valfrihetssystem för gränsöverskridande elektronisk identifiering enligt lagen (2013:311) om valfrihetssystem i fråga om tjänster för elektronisk identifiering eller krav som ska uppfyllas för anslutning till noden för utgående gränsöverskridande elektronisk identifiering. Bemyndigandet kan också avse tekniska

krav på medlet för elektronisk identifiering och andra nödvändiga preciseringar för att kraven för anmälan i EU:s förordning om elektronisk identifiering och de rättsakter som har meddelats med stöd av den ska uppfyllas. Det rör sig främst om Kommissionens genomförandebeslut (EU) 2015/1984 av den 3 november 2015 om förutsättningar, format och förfaranden för anmälan enligt artikel 9.5 i Europaparlamentets och rådets förordning (EU) nr 910/2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden.

Sammanfattning av slutbetänkandet reboot – omstart för den digitala förvaltningen (SOU 2017:117)

Utredningen bedömer att regeringen det senaste året genom en serie olika initiativ har markerat en tydlig förändring av inriktningen av politiken för den digitala förvaltningen. I flera avseenden innebär initiativen en tydlig omprövning av tidigare ställningstaganden. Det som pågår kan därför beskrivas som en omstart – reboot – av politiken för digitalisering inom den offentliga sektorn. De förslag som återges i detta slutbetänkande, liksom förslagen i utredningens delbetänkande, bygger vidare på dessa åtgärder och är avsedda att komplettera dem.

Effektiv styrning

Om styrningen ska vara effektiv måste den riktas direkt till den eller de offentliga myndigheter som ska styras. Styrningen behöver anpassas både till den eller de som ska styras och till den typ av verksamhet eller de förvaltningsgemensamma digitala funktioner som avses. För detta behöver riksdagen och regeringen använda och utforma en väl balanserad kombination av flera olika styrmedel, både bindande och icke-bindande, liksom finansiella och legala. En effektiv finansiell styrning och finansiering av förvaltningsgemensamma digitala funktioner innebär att riksdagen och regeringen måste styra resurserna utifrån ett förvaltningsövergripande perspektiv och att kraven på kvalitet och effektivitet i dessa funktioner måste tillgodoses och bedömas på en förvaltningsövergripande nivå. Det måste finnas formella beslut om vad som ska vara det offentliga åtagandet i den nationella digitala infrastrukturen. Av det skälet bör riksdagen lägga fast ett mål för den offentliga förvaltningens digitalisering. Detta ska ligga till grund för regeringens redovisning till riksdagen och styrningen av de offentliga myndigheterna. Det bör också finnas ett digitaliseringsmål för alla statliga myndigheter. Regeringen behöver fastställa en särskild intern process för att bereda initiativ till samt utvärdera förvaltningsgemensamma digitala funktioner. Regeringen bör vidare besluta om en tidsbestämd övergripande plan – en strategi – för digitalisering och it i den offentliga förvaltningen samt förnya avsiktsförklaringen om digitalisering med Sveriges Kommuner och Landsting.

Statlig elektronisk identitetshandling

Utredningen bedömer att det bör vara ett statligt åtagande att det finns en tillförlitlig process för grundidentifiering, det vill säga att säkerställa individers identitet. Staten ska också utfärda en elektronisk identitetshandling för att på det viset säkerställa att medborgare och folkbokförda kan få en sådan. Den statliga elektroniska identitetshandlingen ska utfärdas samtidigt med en statlig fysisk identitetshandling. Den statliga elektroniska identitetshandlingen ska kunna användas för identifiering hos myndigheter men också kunna växlas till en mobil elektronisk identitetshandling. Därmed kan den statliga elektroniska identitetshandlingen fungera som en backup om t.ex. mobiltelefonen blir obrukbar.

Utredningen bedömer att det finns ett behov av att staten säkerställer att Sverige kan anmäla en elektronisk identitetshandling för användning i Europa enligt eIDAS-förordningen. Sverige bör delta aktivt i det europeiska arbetet med att möjliggöra gränsöverskridande användning av elektroniska identitetshandlingar. När det gäller att öppna upp elektroniska tjänster anser utredningen att Sverige bör samverka med länder som har identitetsbeteckningar som liknar det svenska personnumret och som har anmält eller avser att anmäla en nationell elektronisk identitetshandling. Samarbetet bör präglas av ömsesidighet och tjänster som används frekvent bör prioriteras.

Det redan påbörjade nordiska samarbetet är en lämplig början. Regeringen bör ge uppdrag till myndigheter som har särskilt ofta förekommande ärenden rörande nordiska medborgare att delta i och stödja samarbetsprojekt med motsvarande myndigheter i de nordiska och baltiska länderna. Som ett stöd för arbetet bör Skatteverket få i uppdrag att inrätta ett svenskt register över säkerställda kopplingar mellan europeiska elektroniska identitetshandlingar och svenska personnummer.

Mina meddelanden

Utredningen föreslår att Mina meddelanden ska regleras i en lag om infrastruktur för digital post. Av flera skäl anser utredningen att infrastrukturen Mina meddelanden behöver ännu tydligare reglering än vad som föreslogs i delbetänkandet. Anpassningar till dataskyddsförordningen och fördelning av personuppgiftsansvaret behöver stöd i lag. Dessutom bör infrastrukturen öppnas upp för privata aktörer som avsändare, vilket också bör regleras i lag.

Utdrag ur betänkandets lagförslag

Förslag till lag om ändring i lagen (2016:561) med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering

Härigenom föreskrivs i fråga om lagen (2016:561) med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering att det i lagen ska införas nio nya paragrafer, tre nya rubriker samt en ny rubriknivå med följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	Tillsynsmyndigheten
	5 §
	Tillsynsmyndigheten har rätt att på begäran få de upplysningar och handlingar som behövs för tillsynen.
	Tillsynsmyndigheten har också rätt att få tillträde till områden, lokaler och andra utrymmen, dock inte bostäder, där verksamhet som står under tillsyn bedrivs.
	Tillsynsmyndigheten har rätt att få biträde av Kronofogdemyndigheten för tillsyn enligt första och andra styckena.
Avgifter	*Avgifter*
	7 §
	Regeringen eller, efter regeringens bemyndigande, tillsynsmyndigheten får meddela föreskrifter om skyldighet för tillhandahållare av betrodda tjänster att betala avgift för tillsynsmyndighetens verksamhet enligt denna lag.
Överklagande	*Överklagande*
	8 §
	Tillsynsmyndighetens beslut enligt EU:s förordning om elektronisk identifiering och rättsakter som har meddelats med stöd av den förordningen, samt enligt denna lag och föreskrifter som har meddelats med stöd av lagen, får överklagas till allmän förvaltningsdomstol.
	Prövningstillstånd krävs vid överklagande till kammarrätten.
	Noden
	9 §
	Den myndighet som regeringen utser (nodmyndigheten) ska ansvara för att tillhandahålla en offentlig förbindelsepunkt (nod) för gräns-

överskridande elektronisk identifiering och att den fungerar i enlighet med EU:s förordning om elektronisk identifiering och rättsakter som har meddelats med stöd av den förordningen.

Regeringen eller, efter regeringens bemyndigande, nodmyndigheten får meddela föreskrifter om noden.

10 §

För att användare ska kunna identifieras får nodmyndigheten behandla de personuppgifter som kommer till noden. Vilka personuppgifter som kommer till noden regleras i bilagan till Kommissionens genomförandeförordning (EU) 2015/1501.

Nodmyndigheten är personuppgiftsansvarig för de behandlingar av personuppgifter som utförs i noden.

11 §

Nodmyndigheten får behandla (tekniska) uppgifter för de aktörer vars uppgifter ska behandlas av noden. Myndigheten får även behandla de personuppgifter som är nödvändiga för att säkerställa behörigheter för aktörernas ombud.

12 §

Alla myndigheter som, för att ge åtkomst till sina nättjänster, omfattas av kraven på elektronisk identifiering enligt EU:s förordning om elektronisk identifiering, ska ansluta till den svenska offentliga noden.

Myndigheter som inte omfattas av förordningens krav får ansluta till den svenska offentliga noden.

13 §

Privata aktörer får ansluta till den svenska offentliga noden.

Regeringen eller, efter regeringens bemyndigande, nodmyndigheten får meddela föreskrifter om skyldighet för privata aktörer att betala avgift för att ansluta till noden enligt denna lag.

14 §

Alla som är anslutna till noden ska utan otillbörligt dröjsmål underrätta nodmyndigheten om alla händelser som påverkat funktionalitet eller säkerhet i noden.

Anmälan av svenska medel för elektronisk identifiering

15 §

Den myndighet som regeringen utser ansvarar för anmälan av svenska medel för elektronisk identifiering för gränsöverskridande elektronisk identifiering enligt EU:s förordning om elektronisk identifiering (anmälande myndighet).

Regeringen eller den myndighet som regeringen bemyndigar får meddela föreskrifter om hur anmälan ska gå till.

16 §

För att kunna anmälas för gränsöverskridande elektronisk identifiering ska ett svenskt medel för elektronisk identifiering

1. vara kvalitetsgranskat av digitaliseringsmyndigheten,

2. endast utfärdas till medborgare eller folkbokförda i Sverige,

3. ingå i valfrihetssystem enligt lagen (2013:311) om valfrihetssystem i fråga om tjänster för elektronisk identifiering, och

4. vara utfärdat av en aktör som har tecknat försäkring som täcker ersättning för skada som åsamkats fysiska eller juridiska personer avsiktligt eller på grund av oaktsamhet genom underlåtenhet att uppfylla de skyldigheter som avses i artikel 7 i EU:s förordning om elektronisk identifiering.

17 §

Anmälande myndighet ansvarar även för att tillfälligt upphäva, återkalla, återinföra och dra till-

	baka elektroniska identitetshandlingar vid säkerhetsincidenter enligt artikel 10 i EU:s förordning om elektronisk identifiering.	Bilaga 2

Denna lag träder i kraft den 29 september 2018.

Förteckning över remissinstanserna

Efter remiss har yttrande över betänkandet reboot – omstart för den digitala förvaltningen (SOU 2017:114) inkommit från Riksdagens ombudsmän, Riksrevisionen, Göta Hovrätt, Kammarrätten i Stockholm, Förvaltningsrätten i Göteborg, Lycksele tingsrätt, Justitiekanslern, Domstolsverket, Polismyndigheten, Säkerhetspolisen, Myndigheten för samhällsskydd och beredskap, Migrationsverket, Datainspektionen, Styrelsen för internationellt utvecklingssamarbete, Styrelsen för ackreditering och teknisk kontroll, Försvarsmakten, Försvarets materielverk, Totalförsvarets rekryteringsmyndighet, Försvarets radioanstalt, Försäkringskassan, Inspektionen för vård och omsorg, Myndigheten för delaktighet, Pensionsmyndigheten, E-hälsomyndigheten, Tullverket, Ekonomistyrningsverket, Finansinspektionen, Skatteverket, Kronofogdemyndigheten, Kammarkollegiet, Statistiska centralbyrån, Arbetsgivarverket, Länsstyrelsen i Norrbotten, Länsstyrelsen i Västernorrland, Länsstyrelsen i Västra Götalands län, Länsstyrelsen i Skåne, Statskontoret, Statens servicecenter, Statens tjänstepensionsverk, E-legitimationsnämnden, Konsumentverket, Allmänna reklamationsnämnden, Statens skolverk, Linköpings universitet, Mittuniversitetet, Centrala studiestödsnämnden, Naturvårdsverket, Sveriges meteorologiska och hydrologiska institut, Statens energimyndighet, Post- och telestyrelsen, Trafikverket, Sjöfartsverket, Transportstyrelsen, Konkurrensverket, Sveriges geologiska undersökning, Bolagsverket, Verket för innovationssystem, Tillväxtverket, Skogsstyrelsen, Statens jordbruksverk, Livsmedelsverket, Boverket, Lantmäteriet, Statens kulturråd, Konstnärsnämnden, Riksarkivet, Arbetsförmedlingen, Borås kommun, Botkyrka kommun, Falkenbergs kommun, Gotlands kommun, Haninge kommun, Huddinge kommun, Jönköpings kommun, Karlstads kommun, Kiruna kommun, Kramfors kommun, Linköpings kommun, Malmö kommun, Nacka kommun, Norrköpings kommun, Skellefteå kommun, Stockholms kommun, Svenljunga kommun, Södertälje kommun, Trollhättans kommun, Trosa kommun, Täby kommun, Uddevalla kommun, Uppsala kommun, Örebro kommun, Östhammars kommun, Jämtlands läns landsting, Stockholms läns landsting, Västra Götalands läns landsting, Östergötlands läns landsting, Sveriges Kommuner och Landsting, Regelrådet, Finansiell ID-teknik, Funktionsrätt Sverige, Företagarna, Handelshögskolan i Stockholm, Internetstiftelsen i Sverige, Inera AB, IT & Telekomföretagen, Kivra Sverige AB, Landsorganisationen i Sverige, Postnord Sverige AB, SPF Seniorerna, Svenska bankföreningen, Sveriges akademikers centralorganisation, Telia Sverige AB och Verisec AB.

Yttranden har även inkommit från Elöverkänsligas riksförbund, Lärarnas riksförbund, SES Swedish standards institute, Sveriges advokatsamfund, Sveriges A-kassor och Synskadades riksförbund.

Havs- och vattenmyndigheten, Arvidsjaurs kommun, Falu kommun, Gnosjö kommun, Höganäs kommun, Karlshamns kommun, Leksands kommun, Malå kommun, Motala kommun, Smedjebackens kommun, Västerås kommun, Åre kommun, Älmhults kommun, Överkalix kommun, Norrbottens läns landsting, Skåne läns landsting, AB Svenska Pass, Bring Citymail Sweden AB, Dataföreningen i Sverige, Lika unika, Nexus,

Pensionärernas riksorganisation, Svenskt näringsliv, Sveriges konsumenter, Säkerhets- och försvarsföretagen, Teknikföretagen och Tjänstemännens centralorganisation har beretts tillfälle att lämna synpunkter, men avstått från att yttra sig eller inte avhörts.