Detta dokument är endast avsett som dokumentationshjälpmedel och institutionerna ansvarar inte för innehållet

►**B** **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

(Text av betydelse för EES)

(EUT L 235, 9.9.2015, s. 1)

Rättad genom:

►**C1** Rättelse, EUT L 28, 4.2.2016, s. 18 (2015/1501)

▼B

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

(Text av betydelse för EES)

EUROPEISKA KOMMISSIONEN HAR ANTAGIT DENNA FÖRORDNING

med beaktande av fördraget om Europeiska unionens funktionssätt,

med beaktande av 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 ([1]), särskilt artikel 12.8, och

av följande skäl:

(1) Enligt artikel 12.2 i förordning (EU) nr 910/2014 bör ett interoperabilitetsramverk fastställas i syfte att skapa interoperabilitet mellan de nationella system för elektronisk identifiering som anmälts i enlighet med artikel 9.1 i den förordningen.

(2) Noder spelar en central roll i förbindelsen mellan de nationella systemen för elektronisk identifiering. En redogörelse för deras betydelse finns i den dokumentation som rör Fonden för ett sammanlänkat Europa som inrättats genom Europaparlamentets och rådets förordning (EU) nr 1316/2013 ([2]), vari även ”eIDAS-nodens” funktioner och komponenter ingår.

(3) Om en medlemsstat eller kommissionen tillhandahåller programvara, för att möjliggöra autentisering, till en nod som drivs av en annan medlemsstat får den part som levererar och uppdaterar den programvara som används för autentiseringsmekanismen överenskomma med den part som står värd för programvaran hur driften av autentiseringsmekanismen ska skötas. En sådan överenskommelse bör inte inbegripa oproportionella tekniska krav eller kostnader (t.ex. support, ansvar, värdkostnader eller andra kostnader) för den part som står för värdskapet.

(4) I den utsträckning som genomförandet av interoperabilitetsramverket motiverar det kan ytterligare tekniska specifikationer med ingående uppgifter om tekniska krav i enlighet med vad som anges i denna förordning utarbetas av kommissionen, i samarbete

([1]) EUT L 257, 28.8.2014, s. 73.

([2]) Europaparlamentets och rådets förordning (EU) nr 1316/2013 av den 11 december 2013 om inrättande av Fonden för ett sammanlänkat Europa, om ändring av förordning (EU) nr 913/2010 och om upphävande av förordningarna (EG) nr 680/2007 och (EG) nr 67/2010 (EUT L 348, 20.12.2013, s. 129).

▼B

med medlemsstaterna, i synnerhet under beaktande av yttranden från de samarbetsnätverk som avses i artikel 14 d i kommissionens genomförandebeslut (EU) 2015/296 ([1]). Sådana specifikationer bör utarbetas som en del av infrastrukturerna för digitala tjänster i förordning (EU) nr 1316/2013, som tillhandahåller medlen för det praktiska förverkligandet av en elektronisk identifieringsmodul.

(5) De tekniska kraven i denna förordning bör vara tillämpliga i de tekniska specifikationer som kan komma att utarbetas i kraft av artikel 12 i denna förordning.

(6) När bestämmelserna för interoperabilitetsramverket i denna förordning har fastställts har största möjliga hänsyn tagits till det storskaliga pilotprojektet Stork, inklusive de specifikationer som utarbetats av detta projekt, samt principer och begrepp från den europeiska interoperabilitetsramen för europeiska offentliga tjänster.

(7) Största möjliga hänsyn har tagits till resultaten av samarbetet mellan medlemsstaterna.

(8) De åtgärder som föreskrivs i denna förordning är förenliga med yttrandet från den kommitté som inrättats genom artikel 48 i förordning (EU) nr 910/2014.

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

Artikel 1

Syfte

I denna förordning fastställs de tekniska och operativa kraven för interoperabilitetsramverket i syfte att säkra interoperabiliteten mellan de system för elektronisk identifiering som medlemsstaterna anmäler till kommissionen.

Kraven innefattar i synnerhet

a) tekniska minimikrav rörande tillitsnivåer och kartläggning av nationella tillitsnivåer för anmälda medel för elektronisk identifiering som utfärdats inom ramen för anmälda system för elektronisk identifiering enligt artikel 8 i förordning (EU) nr 910/2014 såsom fastställs i artiklarna 3 och 4,

b) tekniska minimikrav på interoperabilitet enligt artiklarna 5 och 8,

c) minimuppsättningen av personidentifieringsuppgifter som är unika för en fysisk eller juridisk person enligt artikel 11 och i bilagan,

([1]) Kommissionens genomförandebeslut (EU) 2015/296 av den 24 februari 2015 om inrättande av förfaranden för samarbete mellan medlemsstaterna om elektronisk identifiering i enlighet med artikel 12.7 i Europaparlamentets och rådets förordning (EU) nr 910/2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden (EUT L 53, 25.2.2015, s. 14).

▼B

d) gemensamma standarder för operativ säkerhet enligt artiklarna 6, 7, 9 och 10,

e) bestämmelser för tvistlösning enligt artikel 13.

Artikel 2

Definitioner

I denna förordning avses med

1. *nod*: en förbindelsepunkt som utgör en del av den interoperativa arkitekturen för elektronisk identifiering och 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,

2. *nodoperatör*: den enhet som ansvarar för att se till att noden på korrekt och tillförlitligt sätt utför sina funktioner som förbindelsepunkt.

Artikel 3

Tekniska minimikrav rörande tillitsnivåerna

Tekniska minimikrav rörande tillitsnivåerna ska fastställas i kommissionens genomförandeförordning (EU) 2015/1502 ([1]).

Artikel 4

Kartläggning av nationella tillitsnivåer

Kartläggningen av nationella tillitsnivåer för anmälda system för elektronisk identifiering ska följa de krav som fastställs i genomförandeförordning (EU) 2015/1502. ►C1 Resultaten av kartläggningen ska anmälas till kommissionen med hjälp av den mall som fastställs i kommissionens genomförandebeslut (EU) 2015/1984 ([2]). ◄

Artikel 5

Noder

1. En nod i en medlemsstat ska ha förmåga att koppla upp sig med noder i andra medlemsstater.

([1]) Kommissionens genomförandeförordning (EU) 2015/1502 av den 8 september 2015 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 (se sidan 7 i detta nummer av EUT).

([2]) 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 (EUT L 289, 5.11.2015, s. 18).

▼B

2. Noderna ska med tekniska medel ha förmågan att särskilja mellan offentliga organ och andra förlitande parter.

3. Vid en medlemsstats genomförande av de tekniska kraven i denna förordning får andra medlemsstater inte åläggas oproportionella tekniska krav och kostnader för att kunna samverka med det system som genomförs i den första medlemsstaten.

Artikel 6

Skydd av personuppgifter samt datasekretess

1. Skyddet av personuppgifter samt datasekretessen vad avser de uppgifter som utbyts och vidmakthållandet av dataintegriteten mellan noderna ska säkerställas genom användning av bästa tillgängliga tekniska lösningar och skyddspraxis.

2. Noderna får inte lagra några personuppgifter, utom för det ändamål som anges i artikel 9.3.

Artikel 7

Dataintegritet och uppgifternas äkthet vid kommunikation

Vid kommunikationen mellan noderna ska dataintegriteten och uppgifternas äkthet säkras så att varje begäran och varje svar är äkta och inte har manipulerats. För detta ändamål ska noderna använda lösningar som med goda resultat har utnyttjats för gränsöverskridande operativt bruk.

Artikel 8

Meddelandeformat för kommunikationen

Noderna ska som syntax använda gemensamma meddelandeformat baserade på standarder som redan har utnyttjats mer än en gång mellan medlemsstater och visat sig fungera i en operativ miljö. Syntaxen ska möjliggöra

a) korrekt behandling av minimuppsättningen av personidentifieringsuppgifter som är unika för en fysisk eller juridisk person,

b) korrekt behandling av tillitsnivån för medlet för elektronisk identifiering,

c) åtskillnad mellan offentliga organ och andra förlitande parter,

d) flexibilitet för att tillgodose behov av ytterligare identifieringsattribut.

Artikel 9

Hantering av säkerhetsinformation och metadata

1. Nodoperatören ska kommunicera nodhanteringens metadata på ett standardiserat maskinläsbart sätt som är säkert och pålitligt.

▼B

2. Åtminstone säkerhetsrelevanta parametrar ska hämtas automatiskt.

3. 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. Uppgifterna ska lagras under en period som överensstämmer med nationella krav och ska, allra minst, bestå av följande beståndsdelar:

a) Identifiering av noden.

b) Identifiering av meddelandet.

c) Datum och tidpunkt för meddelandet.

Artikel 10

Informationssäkerhet och säkerhetsstandarder

1. Nodoperatörer som tillhandahåller autentisering ska visa att noden, vad gäller dess deltagande i interoperabilitetsramverket, uppfyller kraven för standarden ISO/IEC 27001 genom certifiering, eller genom en likvärdig bedömningsmetod, eller genom att följa nationell lagstiftning.

2. Nodoperatörer ska utan onödiga dröjsmål genomföra säkerhetskritiska uppdateringar.

Artikel 11

Personidentifieringsuppgifter

1. En minimuppsättning av personidentifieringsuppgifter som är unika för en fysisk eller juridisk person ska uppfylla kraven i bilagan vid användning i ett gränsöverskridande sammanhang.

2. En minimuppsättning uppgifter om en fysisk person som företräder en juridisk person ska innehålla den kombination av attribut som förtecknas i bilagan med avseende på fysiska personer och juridiska personer vid användning i gränsöverskridande sammanhang.

3. Uppgifter ska överföras med originaltecken och, om så är tillämpligt, även transkriberade med latinska tecken.

Artikel 12

Tekniska specifikationer

1. Om det är motiverat av genomförandet av interoperabilitetsramverket får det samarbetsnätverk som inrättats genom genomförandebeslut (EU) 2015/296 i kraft av artikel 14 d i detta beslut yttra sig om behovet av att utarbeta tekniska specifikationer. Sådana tekniska specifikationer ska ge ytterligare information om tekniska krav som fastställs i denna förordning.

▼B

2. I kraft av yttranden som avses i punkt 1 ska kommissionen i samarbete med medlemsstaterna utarbeta de tekniska specifikationerna som en del av de infrastrukturerna för digitala tjänster i förordning (EU) nr 1316/2013.

3. Samarbetsnätverket ska i enlighet med artikel 14 d i genomförandebeslut (EU) 2015/296 yttra sig och lämna en utvärdering av huruvida och i vilken utsträckning de tekniska specifikationer som utarbetas enligt punkt 2 motsvarar de behov som angavs i yttranden som avses i punkt 1 eller de krav som fastställs i denna förordning. Det kan rekommendera medlemsstaterna att ta hänsyn till de tekniska specifikationerna vid genomförandet av interoperabilitetsramverket.

4. Kommissionen ska tillhandahålla ett referensgenomförande som en exempeltolkning av de tekniska specifikationerna. Medlemsstaterna kan tillämpa detta referensgenomförande eller använda det som ett exempel när de testar andra genomföranden av de tekniska specifikationerna.

Artikel 13

Tvistlösning

1. När så är möjligt ska eventuella tvister gällande interoperabilitetsramverket lösas genom förhandlingar mellan de berörda medlemsstaterna.

2. Om någon lösning inte nås i enlighet med punkt 1 ska det samarbetsnätverk som inrättats i enlighet med artikel 12 i kommissionens genomförandebeslut (EU) 2015/296 ha behörighet vad avser tvisten i enlighet med vad som anges i dess arbetsordning.

Artikel 14

Ikraftträdande

Denna förordning träder i kraft den tjugonde dagen efter det att den har offentliggjorts i *Europeiska unionens officiella tidning*.

Denna förordning är till alla delar bindande och direkt tillämplig i alla medlemsstater.

▼B

BILAGA

Krav enligt artikel 11 på minimiuppsättning av personidentifieringsuppgifter som är unika för en fysisk eller en juridisk person

1. Minimiuppsättning av uppgifter för fysisk person

En minimiuppsättning av uppgifter för en fysisk person ska innehålla följande obligatoriska attribut:

a) nuvarande efternamn,

b) nuvarande förnamn,

c) födelsedatum,

d) 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 innehålla ett eller flera av följande ytterligare attribut:

a) förnamn och efternamn vid födseln,

b) födelseort,

c) nuvarande adress,

d) kön.

2. Minimiuppsättning av uppgifter för juridisk person

En minimiuppsättning av uppgifter för en juridisk person ska innehålla följande obligatoriska attribut:

a) nuvarande juridiska namn,

b) 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 av uppgifter för en juridisk person kan innehålla ett eller flera av följande ytterligare attribut:

a) nuvarande adress,

b) momsregistreringsnummer,

c) skatteregistreringsnummer,

d) den identifikator som avses i artikel 3.1 i Europaparlamentets och rådets direktiv 2009/101/EG ([1]),

([1]) Europaparlamentets och rådets direktiv 2009/101/EG av den 16 september 2009 om samordning av de skyddsåtgärder som krävs i medlemsstaterna av de i artikel 48 andra stycket i fördraget avsedda bolagen i bolagsmännens och tredje mans intressen, i syfte att göra skyddsåtgärderna likvärdiga inom gemenskapen (EUT L 258, 1.10.2009, s. 11).

▼B

e) den identifieringskod för juridiska personer som avses i kommissionens genomförandeförordning (EU) nr 1247/2012 ([1]),

f) det registrerings- och identitetsnummer för ekonomiska aktörer som avses i kommissionens genomförandeförordning (EU) nr 1352/2013 ([2]),

g) punktskattenummer som avses i artikel 2.12 i rådets förordning (EU) nr 389/2012 ([3]).

([1]) Kommissionens genomförandeförordning (EU) nr 1247/2012 av den 19 december 2012 om fastställande av tekniska genomförandestandarder för form och frekvens för rapportering om handel till transaktionsregister enligt Europaparlamentets och rådets förordning (EU) nr 648/2012 om OTC-derivat, centrala motparter och transaktionsregister (EUT L 352, 21.12.2012, s. 20).

([2]) Kommissionens genomförandeförordning (EU) nr 1352/2013 av den 4 december 2013 om fastställande av de formulär som avses i Europaparlamentets och rådets förordning (EU) nr 608/2013 om tullens säkerställande av skyddet för immateriella rättigheter (EUT L 341, 18.12.2013, s. 10).

([3]) Rådets förordning (EU) nr 389/2012 av den 2 maj 2012 om administrativt samarbete i fråga om punktskatter och om upphävande av förordning (EG) nr 2073/2004 (EUT L 121, 8.5.2012, s. 1).