Det Europæiske Økonomiske og Sociale Udvalgs udtalelse om »Forslag til Europa-Parlamentets og Rådets direktiv om foranstaltninger, der skal sikre et højt fælles niveau for net- og informationssikkerhed i hele EU«

COM(2013) 48 final – 2013/0027 (COD)

(2013/C 271/25)

Ordfører: **Thomas McDONOGH**

Rådet og Europa-Parlamentet besluttefde henholdsvis den 21. februar og den 15. april 2013 under henvisning til artikel 114 i traktaten om Den Europæiske Unions funktionsmåde at anmode om Det Europæiske Økonomiske og Sociale Udvalgs udtalelse om:

»*Forslag til Europa-Parlamentets og Rådets direktiv om foranstaltninger, der skal sikre et højt fælles niveau for net- og informationssikkerhed i hele EU*«

COM(2013) 48 final – 2013/0027 (COD).

Det forberedende arbejde henvistes til Den Faglige Sektion for Transport, Energi, Infrastruktur og Informationssamfundet, som vedtog sin udtalelse den 30. april 2013.

Det Europæiske Økonomiske og Sociale Udvalg vedtog på sin 490. plenarforsamling den 22.-23. maj 2013, mødet den 22. maj, følgende udtalelse med 163 stemmer for, 1 imod og 5 hverken for eller imod:

1. **Konklusioner og anbefalinger**

1.1 Det Europæiske Økonomiske og Sociale Udvalg (EØSU) ser direktivforslaget som en del af en større sammenhæng også omfattende den nyligt offentliggjorte strategi for cybersikkerhed ([1]), hvorunder der opridses en vidtfavnende vision for net- og informationssikkerhed (NIS), der skal tilvejebringe en sikker vækst i den digitale økonomi og samtidig fremme europæiske værdier som frihed og demokrati.

1.2 EØSU glæder sig over det foreslåede direktiv, som sigter mod at sikre et højt fælles niveau for NIS i hele EU. Harmonisering og styring af NIS på europæisk niveau er af afgørende betydning for gennemførelsen af det digitale indre marked og for et velfungerende indre marked som helhed. Udvalget er ligesom Kommissionen bekymret for den store skade, som en fejlslagen NIS kan forårsage på økonomien og borgernes velfærd, men det foreslåede direktiv lever ikke op til EØSU's forventninger om en solid lovgivning på dette vigtige område.

1.3 Udvalget er uhyre skuffet over det manglende fremskridt i mange medlemsstater for at gennemføre en effektiv NIS på nationalt niveau og beklager den øgede risiko, som dette skaber for borgerne, samt den negative indvirkning, det har på gennemførelsen af det indre digitale marked. Medlemsstater bør med det samme få gennemført deres udestående NIS-forpligtelser.

1.4 Det manglende fremskridt skaber endnu en digital kløft mellem elitegruppen af medlemsstater, som er meget langt fremme med NIS, og de mindre udviklede medlemsstater. Kløften slider på tilliden og samarbejdet om NIS på EU-niveau, og hvis ikke der tages hånd om problemet hurtigst muligt, er det sandsynligt, at forskellene i medlemsstaternes kapacitet vil medføre mangler på det indre marked.

1.5 Som EØSU har påpeget i tidligere udtalelser ([2]), er vage og frivillige foranstaltninger ikke effektive, og der er behov for at pålægge medlemsstaterne skrappe lovmæssige forpligtelser for at sikre harmonisering, styring og håndhævelse af den europæiske NIS. Desværre er det udvalgets opfattelse, at forslaget til direktiv ikke tilvejebringer den klare og helt afgørende lovgivning, som er påkrævet. Med henblik på at sikre det nødvendige høje fælles niveau for NIS mener EØSU, at en forordning med veldefinerede bindende forpligtelser for medlemsstaterne ville være mere effektiv end et direktiv.

1.6 På trods af Kommissionens hensigt om at vedtage gennemførelsesretsakter for at sikre nogle fælles betingelser for gennemførelsen af dele af direktivet, mener udvalget, at direktivforslaget mangler standarder, klare definitioner og ufravigelige forpligtelser og dermed giver medlemsstaterne for meget fleksibilitet med hensyn til, hvordan de skal fortolke og omsætte vigtige elementer. EØSU ser gerne, at der i forslaget indarbejdes meget mere eksplicitte definitioner på de standarder, krav og procedurer, som medlemsstaterne, offentlige myndigheder, markedsaktører og vigtige internetstøttefunktioner skal overholde.

([1]) »Et åbent, sikkert og beskyttet cyberspace« JOIN(2013) 1.

([2]) EØSU's udtalelse om *Beskyttelse af kritisk informationsinfrastruktur*, EUT C 255 af 22.9.2010, s. 98, og om *Direktiv om angreb på informationssystemer*, EUT C 218 af 23.7.2011, s. 130.

1.7 EØSU opfordrer til, at der etableres et EU-agentur for NIS svarende til Det Europæiske Luftfartssikkerhedsagentur (EASA) til at sikre kvaliteten af udformningen og gennemførelsen af NIS-politikken i EU ([3]). Agenturet skal opstille standarder og overvåge håndhævelsen af alle elementer af NIS i hele EU: fra certificering af sikkert terminaludstyr og anvendelse til netværkssikkerhed og datasikkerhed.

1.8 EØSU er meget opmærksom på de øgede risici for cybersikkerheden og databeskyttelsen, der er opstået efter indførelsen af cloud computing ([4]) i Europa. EØSU ser gerne, at forslaget udtrykkeligt kommer til at indeholde flere specielle sikkerhedskrav og forpligtelser vedrørende tilvejebringelse og brug af cloud-tjenester.

1.9 For at sikre en passende ansvarsfordeling vedrørende NIS bør forslaget gøre det klart, at enheder med forpligtelser i medfør af det foreslåede direktiv har ret til at holde software- og hardwareleverandører ansvarlige for mangler ved produkter eller tjenesteydelser, som er direkte medvirkende til NIS-hændelser.

1.10 EØSU opfordrer medlemsstaterne til særligt at fokusere på at øge de små og mellemstore virksomheders (SMV'er) viden om NIS og kompetencer inden for cybersikkerhed. Udvalget gør desuden Kommissionen opmærksom på, at der i USA ([5]) og visse medlemsstater ([6]) afholdes »hackerkonkurrencer«, som har stor succes med at øge bevidstheden om cybersikkerhed og udklække en ny generation af NIS-specialister.

1.11 Medlemsstaternes overholdelse af direktivet er meget vigtig for net- og informationssikkerheden i hele EU, og EØSU anmoder derfor Kommissionen om at overveje, hvilke midler under den flerårige finansielle ramme (FFR) der kan afsættes til NIS-overholdelse for at hjælpe medlemsstater, der har brug for finansiel bistand.

1.12 Finansiering af forskning, udvikling og innovation (FUI) til brug for NIS-teknologier bør prioriteres højt i EU's rammeprogram for forskning og innovation »Horisont 2020«, så Europa kan holde trit med cybertruslernes hurtigt skiftende karakter.

1.13 For at afklare hvilke enheder der har juridisk ansvar i medfør af det foreslåede direktiv, opfordrer EØSU til at forpligte medlemsstater til at offentliggøre et onlineregister over alle enheder, som er underlagt direktivets krav om risikostyring og anmeldelse. Dette udtryk for gennemsigtighed og offentlig ansvarlighed vil opbygge tillid og bidrage til overholdelsen.

1.14 EØSU gør Kommissionen opmærksomhed på sine mange tidligere udtalelser, hvor udvalget har behandlet net- og informationssikkerhed og kommenteret behovet for et sikkert informationssamfund og beskyttelse af vigtige infrastrukturer ([7]).

2. **Resumé af Kommissionens forslag**

2.1 Det foreslåede NIS-direktiv blev offentliggjort samtidig med EU's strategi for cybersikkerhed, som sigter mod at forbedre informationssystemers robusthed, mindske cyberkriminalitet og styrke EU's internationale cybersikkerhedspolitik og cyberforsvar samt udvikle de industrielle og teknologiske ressourcer til fremme af cybersikkerhed og samtidig fremme grundlæggende rettigheder og andre centrale EU-værdier.

2.2 NIS vedrører sikkerheden i internettet og andre netværk, informationssystemer samt de støttetjenester, som er nødvendige for, at vores samfund kan fungere. NIS er afgørende for et velfungerende indre marked.

2.3 Den helt frivillige tilgang til NIS, som EU har fulgt til nu, yder ikke tilstrækkelig beskyttelse mod NIS-risici. De nuværende NIS-kapaciteter er utilstrækkelige til at holde trit med truslernes hurtigt skiftende karakter og sikre et højt fælles beskyttelsesniveau i alle medlemsstater.

([3]) Det Europæiske Luftfartssikkerhedsagentur: http://easa.europa.eu/

([4]) EØSU's udtalelse om *Cloud-computing i Europa,* EUT C 24 af 28.1.2012, s. 40, og om *Udnyttelse af potentialet ved cloud computing i Europa,* EUT C 76 af 14.3.2013, s. 59.

([5]) http://www.nytimes.com/2013/03/25/technology/united-states-wants-to-attract-hackers-to-public-sector.html?pagewanted=all&_r=0

([6]) http://www.bbc.co.uk/news/technology-17333601

([7]) EØSU's udtalelse om *En strategi for et sikkert informationssamfund,* EUT C 97 af 28.4.2007, s. 21.
EØSU's udtalelse om *Beskyttelse af kritisk informationsinfrastruktur,* EUT C 255 af 22.9.2010, s. 98.
EØSU's udtalelse om *ENISA-forordning,* EUT C 107 af 6.4.2011, s. 58.
EØSU's udtalelse om *Generel forordning om databeskyttelse,* EUT C 229 af 31.7.2012, s. 90.
EØSU's udtalelse om *Angreb på informationssystemer,* EUT C 218 af 23.7.2011, s. 130.
EØSU's udtalelse om *Elektroniske transaktioner på det indre marked,* EUT C 351 af 15.11.2012, s. 73.
EØSU's udtalelse om *Udnyttelse af potentialet ved cloud computing i Europa,* EUT C 76 af 14.3.2013, s. 59.

2.4 Medlemsstaternes kapaciteter og beredskab er i dag meget forskellige, og det giver en usammenhængende tilgang til net- og informationssikkerhed i EU. Med tanke på, at netværk og systemer er indbyrdes forbundne, så svækkes EU's net- og informationssikkerhed af de medlemsstater, der har et utilstrækkeligt beskyttelsesniveau. Det hæmmer også opbygningen af tillid mellem ligestillede, som er en forudsætning for samarbejde og informationsudveksling. Som følge heraf er der kun samarbejde mellem et mindretal af medlemsstaterne med høj kapacitet.

2.5 Formålet med direktivet, som er foreslået i overensstemmelse med EUF-traktatens artikel 114, er at lette gennemførelsen af det digitale indre marked og et velfungerende indre marked ved at:

— indføre et fælles minimumsniveau for NIS i medlemsstaterne og dermed øge det generelle beredskabs- og indsatsniveau i forbindelse med hændelser;

— forbedre NIS-samarbejdet på EU-plan for at imødegå grænseoverskridende hændelser og trusler;

— skabe en risikostyringskultur og forbedre udvekslingen af oplysninger mellem den private og offentlige sektor.

2.6 Direktivforslaget indeholder en række lovkrav, herunder:

a) Hver medlemsstat skal gennemføre en NIS-strategi og udpege en national kompetent myndighed for sikkerheden af net og informationssystemer med tilstrækkelige tekniske, finansielle og menneskelige ressourcer til at forebygge, håndtere og reagere på NIS-risici og -hændelser.

b) Der skal indføres en samarbejdsmekanisme mellem medlemsstater og Kommissionen til udveksling af tidlig varsling om risici og hændelser, samarbejde og gennemførelse af regelmæssige peer reviews.

c) Visse særlige enheder i EU pålægges at gennemføre risikostyringsforanstaltninger og anmelde alvorlige hændelser, der vedrører deres centrale tjenester, til de nationale kompetente myndigheder. Enheder, der er omfattet af disse krav, er bl.a. operatører af kritisk infrastruktur inden for visse områder (finansielle tjenester, transport, energi, sundhed), formidlere af informationssamfundets tjenester (især cloud computing, e-handelsplatforme, internetbetaling, søgemaskiner, applikationsforhandlere og sociale netværk) og offentlige myndigheder.

2.7 Medlemsstater skal gennemføre direktivet senest 18 måneder efter, at det er vedtaget af Rådet og Europa-Parlamentet (forventet i løbet af 2014).

3. **Generelle bemærkninger**

3.1 Internettets og det digitale samfunds udbredelse har stor betydning for dagligdagen, men i takt med, at vores afhængighed af internettet vokser, beror vores frihed, velstand og livskvalitet i stigende grad på en solid net- og informationssikkerhed (NIS). Hvis internettet er nede, og det i en nødsituation ikke er muligt at få adgang til elektroniske lægejournaler, vil det få dødelige konsekvenser. Imidlertid er der stadig flere og flere trusler mod sikkerheden af Europas kritiske informationsinfrastruktur, og vores NIS-niveau er ikke tilstrækkeligt højt.

3.2 Direktøren for Europol meddelte sidste år, at han var »… meget bekymret over denne malplacerede tillid til internettets usårlighed« ([8]). Vi hører ofte om nye cyberangreb på vigtige strukturer foretaget af kriminelle, terrorister eller udenlandske regeringer. De fleste angreb anmeldes ikke, da ofrene er bange for at få skadet omdømmet, men i de seneste uger er der sket angreb på Europas internetinfrastrukturer ([9]) og banksystemer ([10]), som var for forstyrrende til, at de kunne skjules. I følge en rapport ([11]) blev Nederlandene i 2011 ramt af 92 mio. cyberangreb og Tyskland af 82 mio. Den britiske regering vurderer, at Storbritannien blev ramt af 44 mio. cyberangreb i 2011, som kostede økonomien op til 30 mia. EUR ([12]).

3.3 I 2007 tog Rådet fat på NIS-problemet i Europa ([13]), men politikken har sidenhen ([14]) hovedsageligt været baseret på frivillige tiltag fra medlemsstaternes side, og kun et fåtal af dem har truffet effektive foranstaltninger. Udvalget bemærker, at mange medlemsstater hverken har offentliggjort en national cybersikkerhedsstrategi eller udarbejdet en national beredskabsplan for cyberhændelser, mens andre endnu ikke har oprettet en it-beredskabsenhed (CERT). I tillæg hertil har en række medlemsstater stadig ikke ratificeret Europarådets konvention om cyberkriminalitet ([15]).

([8]) http://forumblog.org/2012/05/what-if-the-internet-collapsed/
([9]) http://www.nytimes.com/2013/03/27/technology/internet/online-dispute-becomes-internet-snarling-attack.html?pagewanted=all&_r=0
([10]) http://www.dutchnews.nl/news/archives/2013/04/online_retailers_demand_banks.php
([11]) http://www.securelist.com/en/analysis/204792216/Kaspersky_Security_Bulletin_Statistics_2011
([12]) UK Cyber Security Strategy – Landscape Review: http://www.nao.org.uk/wp-content/uploads/2013/03/Cyber-security-Full-report.pdf
([13]) Rådets resolution 2007/C 68/01.
([14]) COM(2006) 251 og COM(2009) 149.
([15]) http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CL=ENG

3.4 Ti medlemsstater, som er meget langt fremme med NIS, har dannet den europæiske styringsgruppe for it-beredskabsenheder (EGC) med henblik på et tættere samarbejde om NIS og beredskab. EGC tager for nuværende ikke imod nye medlemmer: de resterede 17 medlemsstater, som ikke er nået så langt med NIS-udviklingen, og den nydannede enhed CERT-EU ([16]) er i øjeblikket udelukket fra denne elitegruppe. Der er ved at opstå en ny digital kløft mellem medlemsstater, der er meget langt fremme med NIS, og resten. Hvis ikke der slås bro over denne kløft, vil NIS-ubalancen ramme det indre digitale marked i hjertet og derved hæmme udviklingen af tillid, harmonisering og interoperabilitet. Uden solide foranstaltninger er det desuden sandsynligt, at kløften mellem de medlemsstater, der er nået langt på området, og de medlemsstater, der er nået knap så langt, vil øges, ligesom de mangler på det indre marked, der kan tilskrives medlemsstaternes forskellige kapacitet, vil blive forøget.

3.5 En forudsætning for, at cybersikkerhedsstrategien bliver en succes, og det foreslåede direktiv om NIS kommer til at fungere som tilsigtet, er, at der er en solid NIS-industri i Europa og tilstrækkeligt med specialister inden for NIS. EØSU glæder sig over, at det foreslåede direktiv omtaler behovet for, at medlemsstaterne investerer i teoretiske og praktiske uddannelsesprogrammer og oplysningsprogrammer vedrørende NIS. Udvalget opfordrer ligeledes medlemsstater til at gøre en særlig indsats for at oplyse, uddanne og støtte SMV'er i forhold til cybersikkerhed. De større virksomheder kan let skaffe sig den viden, de har brug for, men SMV'erne har brug for støtte.

3.6 EØSU ser frem til at samarbejde med Det Europæiske Agentur for Net- og Informationssikkerhed (ENISA) for at fremme NIS i forbindelse med den europæiske internetsikkerhedsmåned senere på året. Med hensyn til cybersikkerhedsstrategiens og NIS-direktivets målsætning om at udvikle en sikkerhedsbevidst kultur i EU og øge niveauet for NIS-kompetencer gør udvalget Kommissionen opmærksom på »hackerkonkurrencer« for teenagere, som har haft stor succes med at øge bevidstheden i visse medlemsstater og i USA.

3.7 Udvalget glæder sig ligeledes over, at der i cybersikkerhedsstrategien er givet tilsagn om at afsætte FUI-midler til NIS-teknologi.

3.8 Udbredelsen af cloud computing skaber mange nye risici for cybersikkerhed, som skal håndteres. F.eks. har cyberkriminelle nu adgang til enorme mængder datakraft for forholdsvis få udgifter, og data fra tusindvis af virksomheder findes nu i centrale datalagre, som er sårbare over for målrettede angreb. EØSU har efterlyst større cyberrobusthed af cloud computing ([17]).

([16]) Den Europæiske Unions institutioner, agenturer og organer har oprettet deres egen permanente it-beredskabsenhed (CERT-EU).

([17]) EØSU's udtalelse om *Cloud-computing i Europa*, EUT C 24 af 28.1.2012, s. 40, og om *Udnyttelse af potentialet ved cloud computing i Europa*, EUT C 76 af 14.3.2013, s. 59.

3.9 Udvalget har tidligere tilskyndet til indførelsen af en frivillig europæisk eID-ordning for onlinetransaktioner som supplement til de nuværende nationale ordninger. En sådan ordning vil give bedre beskyttelse mod svig, et styrket tillidsforhold mellem de økonomiske operatører, lavere omkostninger forbundet med leveringen af tjenesteydelser og et højere kvalitetsniveau for tjenester samt en bedre beskyttelse for borgerne.

4. **Særlige bemærkninger**

4.1 Desværre er Kommissionens forslag til NIS-direktiv for vagt og uklart, og det sætter for stor lid til medlemsstaternes selvregulering. Manglen på standarder, klare definitioner og ufravigelige forpligtelser, særligt i direktivets Kapitel IV, giver medlemsstaterne for meget fleksibilitet med hensyn til, hvordan de skal fortolke og omsætte direktivets vigtige elementer. En forordning med veldefinerede bindende, juridiske forpligtelser for medlemsstater ville være mere effektiv end et direktiv.

4.2 EØSU bemærker, at direktivets artikel 6 pålægger medlemsstaterne at udpege en »kompetent myndighed«, der skal overvåge og sikre en konsekvent anvendelse af direktivet i hele EU. Udvalget anfører endvidere, at artikel 8 indeholder bestemmelser om oprettelsen af et »samarbejdsnetværk«, der ved hjælp af sine egne samt Kommissionens beføjelser vil tilvejebringe fælleseuropæisk lederskab, forvaltning og håndhævelse helt ned til medlemsstatsniveau. EØSU mener, at EU på baggrund af denne forvaltningsramme bør overveje at etablere et EU-agentur for NIS, svarende til Det Europæiske Luftfartssikkerhedsagentur (EASA), som opstiller standarder og forestår håndhævelsen og overholdelsen af sikkerhedsregler for fly, lufthavne og lufthavsydelser.

4.3 EU's NIS-agentur, som EØSU foreslår i punkt 4.2 ovenfor, kan oprettes på grundlag af det cybersikkerhedsarbejde, som allerede er i gang i ENISA, Den Europæiske Standardiseringsorganisation (CEN), CERT'erne, den europæiske styringsgruppe for it-beredskabsenheder (EGC) samt andre. Et sådan agentur vil kunne opstille standarder og overvåge håndhævelsen af alle elementer af NIS: fra certificering af sikkert terminaludstyr og anvendelse til netværkssikkerhed og datasikkerhed.

4.4 Som følge af, at medlemsstaterne i høj grad er afhængige af hinanden for at kunne tilvejebringe NIS i hele EU og af, at omkostningerne ved NIS-fejlhændelser potentielt kan blive meget høje for alle berørte parter, ser EØSU gerne, at der i lovgivningen fastlægges eksplicitte og proportionelle sanktioner for manglende overholdelse. Disse sanktioner skal være harmoniserede for at afspejle ansvarets fælleseuropæiske dimension og omfanget af de skader, som kan forvoldes på ikke blot hjemmemarkedet, men i hele EU. Direktivforslagets artikel 17, som omhandler sanktioner, er af generel karakter og giver medlemsstaterne for meget frirum til at fastlægge sanktioner. Den indeholder desuden ikke tilstrækkelige retningslinjer, som tager højde for grænseoverskridende og fælleseuropæiske indvirkninger.

4.5 For nuværende offentliggør myndigheder og udbydere af livsvigtige tjenesteydelser ikke sikkerheds- og robusthedssvigt, medmindre de er nødt til det. Denne mangel på åbenhed skader EU's evne til at handle hurtigt og effektivt over for cybertrusler og forbedre den generelle NIS gennem udveksling af erfaringer. EØSU bifalder Kommissionens beslutning om at gøre anmeldelse af alvorlige NIS-hændelser obligatorisk i medfør af direktivet. Det er udvalgets opfattelse, at frivillig anmeldelse af hændelser ikke er effektivt, da frygt for et skadet omdømme og erstatningsansvar giver incitament til at dække over fejlhændelser.

4.6 Direktivets artikel 14 om anmeldelse indeholder imidlertid ikke en definition på en hændelse med »betydelig indvirkning« på sikkerheden og giver relevante enheder og medlemsstater for stor frihed til at vælge, om de vil anmelde NIS-hændelser eller ej. En effektiv lovgivning forudsætter entydige krav. Eftersom det foreslåede direktiv er for vagt med hensyn til den vigtige definition af krav, er det ikke muligt at holde parter til ansvar for manglende overholdelse, som påtænkt i direktivets artikel 17.

4.7 Da det hovedsageligt er den private sektor, der står for tilvejebringelsen af NIS, er det vigtigt at etablere et højt niveau af tillid og samarbejde med alle virksomheder, der har ansvar for livsvigtig informationsinfrastruktur og tjenester. Initiativet vedrørende det europæiske offentlig-private partnerskab for en robust infrastruktur (EP3R), som Kommissionen lancerede i 2009, bør bifaldes og fremmes. Dog mener udvalget, at initiativet bør styrkes og understøttes med en lovmæssig forpligtelse i NIS-direktivet om at tvinge vigtige interessenter til at samarbejde, når de ikke selv gør nok i den henseende.

4.8 Hver enkelt medlemsstat bør offentliggøre et onlineregister over alle enheder under dens jurisdiktion, som er underlagt sikkerhedskravene og forpligtelsen til at anmelde hændelser i medfør af det foreslåede direktivs artikel 14. I tillæg til at afklare hvorledes medlemsstaterne beslutter at anvende definitionerne i direktivets artikel 3, vil det skabe gennemsigtighed og dermed hjælpe med at opbygge tillid og fremme en risikostyringskultur blandt borgere.

4.9 EØSU noterer sig, at direktivets krav eksplicit ikke omfatter softwareudviklere og hardwarefabrikanter, eftersom de ikke udbyder informationssamfundstjenester. Udvalget mener imidlertid, at direktivforslaget bør fastlægge, at enheder med forpligtelser i medfør af direktivet kan gøre krav gældende mod software- og hardwareleverandører for mangler ved produkter eller tjenesteydelser, som er direkte medvirkende til NIS-hændelser.

4.10 Selvom Kommissionen skønner, at omkostningerne til gennemførelse af det foreslåede NIS-direktiv vil ligge på omkring 2 mia. euro om året, fordelt på den offentlige og private sektor i Europa, påpeger EØSU, at visse medlemsstater i finansielle vanskeligheder vil få svært ved at finde de fornødne midler til overholdelsen. Det er nødvendigt at overveje, hvordan der inden for FFR ved hjælp af forskellige instrumenter som Den Europæiske Fond for Regionaludvikling (EFRU) og eventuelt Fonden for Intern Sikkerhed kan ydes støtte til overholdelse af NIS.

Bruxelles, den 22. maj 2013

Henri MALOSSE

Formand

for Det Europæiske Økonomiske og Sociale Udvalg