DIGITALEUROPE

Transpozícia Smernice EÚ o sieťovej a informačnej bezpečnosti (NIS)

Brusel, 4. júla 2016

ZHRNUTIE

Rada Európskej únie zverejnila 21.4.2016 konečnú verziu Smernice o sieťovej a informačnej bezpečnosti (NIS). V lete ju musí oficiálne schváliť Európsky parlament, samotný text bol odsúhlasený troma inštitúciami EÚ a jeho zmena sa neočakáva. Členské štáty by ju mali zakotviť do svojich vnútroštátnych zákonov v rámci 21 mesiacov od jej prijatia. V prílohe nájdete príručku s osvedčenými postupmi pri zavádzaní aspektov týkajúcich sa technologického odvetvia, ktorá by mala slúžiť ako pomôcka pri celom procese, pričom ukáže ako zachovať pôvodné zámery autorov.

Smernica EÚ NIS predstavuje prvú celoeurópsku legislatívnu úpravu v oblasti kybernetickej ochrany, ktorá sa zameriava na posilnenie právomocí príslušných vnútroštátnych orgánov, zvyšuje ich vzájomnú koordináciu a predstavuje bezpečnostné podmienky pre kľúčové sektory odvetvia.

Každá legislatíva, ktorá implementuje danú smernicu na lokálnej úrovni by mala mať na pamäti jej dva hlavné ciele: (1) zabezpečenie vysokej úrovne kybernetickej bezpečnosti v rámci kritickej infraštruktúry jednotlivých krajín; (2) vytvorenie mechanizmu efektívnej spolupráce medzi členskými štátmi EÚ s cieľom napĺňania uvedeného cieľu. Zdroje by sa mali v prvom rade využiť na dosahovanie spomínaných dvoch dôležitých zámerov.

Pre technologické odvetvie sú ustanovenia týkajúce sa takzvaných poskytovateľov digitálnych služieb (PDS) mimoriadne dôležité. Smernica jasne stanovuje, že existujú zásadné rozdiely medzi prevádzkovateľmi základných služieb (PZS) a PDS. Druhí menovaní sa nepovažujú za kritickú infraštruktúru ako takú. Podľa legislatívy by udalosti ovplyvňujúce digitálne služby mali predstavovať výrazne nižšie riziko pre hospodársku a verejnú bezpečnosť krajiny. Zachovanie daného rozdelenia je mimoriadne dôležité pre efektívne a účinné rozmiestnenie minimálnych zdrojov, ktoré majú úrady k dispozícii, pričom budú musieť presadzovať pravidlá a dozerať na ich dodržiavanie.

V konečnom dôsledku obhájime viac pozornosti pre zamýšľaný **zámer** daných služieb a vyzývame politikov, aby do bezpečnostných požiadaviek v rámci vnútroštátnej legislatívy nezahŕňali iné sektory ako PZS či PDS.

Čo sa týka **jurisdikcie**, PDS by mali mať možnosť spoľahnúť sa na platnú legislatívu v krajine, kde sa nachádza hlavné miesto ich podnikateľskej činnosti, aj keď sú v prípade angažované úrady z viacerých krajín. Pri **nedbalosti** by mali príslušné orgány uplatňovať skôr prístup *ex-post* než ukladať všeobecnú povinnosť dohľadu nad PDS. Okrem toho by sa mali zamerať na dôsledky a zachovávať rozdiely medzi PZS a PDS tým, že nebudú podrobovať druhých menovaných požiadavkám, ktoré sa nenachádzajú v Smernici, ako napríklad kontrolné a záväzné nariadenia.

DIGITALEUROPE
Rue de la Science, 14 - 1040 Brusel Belgicko
Tel. č. +32 (0) 2 609 53 10 Fax + 32 (0) 2 431 04 89
www.digitaleurope.org | info@digitaleurope.org | @DIGITALEUROPE
Člen Registra transparentnosti Komisie 64270747023

Bezpečnostné opatrenia pre PDS by mali byť odlišné od opatrení pre PZS, keďže podľa ustanovenia Smernice predstavujú omnoho nižšie bezpečnostné riziko. Politici by si mali uvedomiť čo je cieľom súladu medzi týmito službami, stanoviť medzinárodné štandardy pre celé odvetvie, predísť technologickým nariadeniam a dodržiavať práva PDS zakotvené v Smernici na definovanie bezpečnostných opatrení, ktoré by pre ich systémy boli najvhodnejšie. **Ohlasovanie incidentov** by malo byť na európskej úrovni zosúladené v najväčšej možnej miere, malo by sa sústrediť na udalosti, ktoré majú dopad na plynulosť služieb, zohľadniť flexibilitu v načasovaní hlásení a vytvoriť dôveryhodné prostredie, ktoré podporuje výmenu informácií bez toho, aby bola oznamovacia strana vystavená zvýšenej zodpovednosti.

Opatrenia uložené PZS ovplyvnia aj ďalšie odvetvia, keďže bezpečnostné opatrenia a ohlasovanie incidentov sa premietnu do zmluvných ustanovení. Uvedené platí najmä pre cloudové služby. Potom môžu byť PDS nepriamo predmetom vnútroštátnych zákonov v krajinách svojich zákazníkov a preto chceme, aby sa pri daných službách uplatňovali medzinárodne uznávané **bezpečnostné opatrenia**. Navrhujeme tiež maximálnu možnú koordináciu a synergiu medzi **ohlasovacími požiadavkami** pre PZS aj PDS, za predpokladu, že PDS budú pravdepodobne predmetom dvojitého oznamovania.

Smernica stanovuje zámer dosiahnuť vysokú spoločnú úroveň bezpečnosti sietí a informačných systémov na zlepšenie fungovania vnútorného trhu. Na dosiahnutie tohto vysokého cieľa **by sa transpozície na národnej úrovni mali sústrediť na zosúladený medzinárodný prístup založený na riziku**, ktorý prináša súkromným účastníkom trhu v danom odvetví flexibilitu, aby sa mohli prispôsobiť neustále sa meniacemu prostrediu, v ktorom čelia rôznym hrozbám, umožňuje kybernetickým orgánom sústrediť sa na riešenia najzávažnejších problémov a ukazuje, že riešenie bezhraničného problému musí byť globálne. Dúfame, že predmetná príručka bude po celý čas užitočnou pomôckou a radi odpovieme na vaše prípadné ďalšie otázky.

DIGITALEUROPE
Rue de la Science, 14 - 1040 Brusel Belgicko
Tel. č. +32 (0) 2 609 53 10 Fax + 32 (0) 2 431 04 89
www.digitaleurope.org | info@digitaleurope.org | @DIGITALEUROPE
Člen Registra transparentnosti Komisie 64270747023

Príloha: Príručka s osvedčenými postupmi na zavedenie Smernice NIS

1. Poskytovatelia digitálnych služieb

a) Rozsah

- Smernica stanovuje, že virtuálne trhoviská, webové vyhľadávacie nástroje a služby cloud computingu by sa mali považovať za poskytovateľov digitálnych služieb (PDS) a mali by teda byť zahrnuté v rozsahu Smernice. Keďže ide o Smernicu ohľadom minimálneho zosúladenia (článok 2), je dôležité zachovať konzistentnosť v rámci celej EÚ a preto by jej členské štáty nemali uplatňovať bezpečnostné požiadavky vnútroštátnej legislatívy na iné sektory než PDS či prevádzkovateľov základných služieb (PZS) - v súlade s článkom 3.

- Smernica podrobne stanovuje, že výrobcovia hardvéru a vývojári softvéru nie sú PDS ani PZS a nemali by tak byť zahrnutí vo vnútroštátnych zákonoch zavádzajúcich Smernicu (odôvodnenie 50).

- Smernica vyslovene vylučuje z rozsahu virtuálnych trhovísk webové služby, ktoré predstavujú sprostredkovateľov služieb tretích strán, pričom sa uzatvárajú predajné zmluvy alebo zmluvy o poskytnutí služieb (napr. nákupné stránky) (odôvodnenie 15).

- Vyhľadávacie funkcie obmedzujúce sa na obsah konkrétnej webovej stránky by nemali byť zahrnuté ako webové vyhľadávače, ani ak využívajú externých poskytovateľov (odôvodnenie 16).

- Definícia služieb cloud computingu spočíva podľa Smernice v zdrojoch, ktoré používajú viacerí používatelia (článok 4(19) a odôvodnenie 17). Vzhľadom na skutočnosť, že súkromné cloudové služby (na rozdiel od verejných) sú určené jednej organizácii, nemali by byť zahrnuté v Smernici.

- Smernica zdôrazňuje, že existujú zásadné rozdiely medzi PDS a PZS, čo je dôvodom prečo platia pre PDS iné pravidlá (odôvodnenie 57). Uvedený rozdiel by pri uplatňovaní Smernice mal zostať zachovaný.

b) Súdna právomoc a dohľad

- Súdna právomoc vzťahujúca sa na PDS by sa mala týkať iba členského štátu, v ktorom má prevádzkovateľ hlavné miesto svojho podnikania, ktoré je v zásade rovnaké ako jeho centrála v EÚ (článok 18.1 a odôvodnenie 64). Tvrdíme, že PDS by sa sami mali identifikovať týmto spôsobom a uvedené rozhodnutie je potrebné prehodnocovať iba ak ho príslušné orgány spochybnia v rámci dohľadu *ex-post.*

- Ak majú PDS svoju sieť a informačné systémy v iných krajinách než majú hlavné miesto podnikania, článok 17.3 predpokladá spoluprácu príslušných orgánov. Z pohľadu PDS je však dôležité, aby sa uplatňovala legislatíva krajiny, v ktorej sa nachádza hlavné miesto ich podnikania a aby niesli plnú zodpovednosť výhradne vo vzťahu k príslušnému orgánu v danej jurisdikcii, ktorý bude vystupovať ako ich partner v dialógu.

DIGITALEUROPE
Rue de la Science, 14 - 1040 Brusel Belgicko
Tel. č. +32 (0) 2 609 53 10 Fax + 32 (0) 2 431 04 89
www.digitaleurope.org | info@digitaleurope.org | @DIGITALEUROPE
Člen Registra transparentnosti Komisie 64270747023

- Smernica pripomína, že PDS sú predmetom priameho reakčného dohľadu *ex-post* a kompetentné úrady nemajú všeobecnú povinnosť kontrolovať PDS a mali by konať iba v prípade, že existujú dôkazy. (Článok 17.1 a odôvodnenie 60). Pri implementácii Smernice je potrebné brať do úvahy uvedené ustanovenia.

- Na rozdiel od PZS, orgány smú v prípade PDS iba požadovať informácie a v prípade nedostatkov žiadať ich odstránenie. Smernica jednoznačne určuje, že orgány nemajú kontrolné právomoci a nemôžu vydávať záväzné nariadenia. Tieto ustanovenia by sa mali dodržiavať aj na vnútroštátnej úrovni.

c) Dodatočné požiadavky

- Bezpečnostné a ohlasovacie požiadavky PDS sú predmetom najvyššieho možného zosúladenia (článok 16.10). Uplatňovanie tohto článku by sa malo zvážiť pri produktoch, službách a riešeniach, ktoré vytvárajú ich sieť a informačné systémy. Potom by nemali byť potrebné ďalšie ustanovenia ako napríklad testovanie produktov do takej miery v akej sa produkty a služby využívajú v danom kontexte.

d) Bezpečnostné opatrenia a normy

- Bezpečnostné opatrenia pre PDS by mali byť miernejšie než pre PZS. PDS by mali mať možnosť samostatne si určiť akým spôsobom sa chcú starať o bezpečnosť a ochranu svojich sietí a informačných systémov pred možnými rizikami (odôvodnenie 49).

- Bezpečnostné opatrenia by mali byť orientované procesne a zamerané na riadenie rizík. Nemali by požadovať, aby sa produkty IKT navrhovali, vytvárali alebo vyrábali určitým spôsobom (odôvodnenie 51).

- Smernica prízvukuje, že členské štáty EÚ nesmú zaviesť ďalšie bezpečnostné požiadavky pre PDS (článok 16.10).

- Napriek tomu očakávame príručky od rôznych účastníkov. Členské štáty zabezpečia, aby boli prijaté opatrenia navrhnuté v Smernici (článok 16.1) a môžu podporiť uplatňovanie noriem na ich implementáciu (článok 19.1) ako aj prediskutovať dané normy s európskymi normalizačnými orgánmi v rámci pracovnej skupiny (článok 11.3(h)). ENISA poskytne poradenstvo ohľadom príslušných noriem (článok 19.2) a Európska komisia je poverená prijatím implementačných zákonov ohľadom bezpečnostných opatrení (článok 16.8).

- Vzhľadom na danú mieru zložitosti a výhody harmonizácie odporúčame, aby sa proces na vnútroštátnej úrovni podriadil vykonávacím aktom na účely odsúhlasenia primeraných opatrení, ktoré bude určite potrebné dokončiť v priebehu roka od prijatia Smernice. Vykonávacie akty by nemali obmedzovať schopnosť PDS stanoviť bezpečnostné opatrenia, ktoré sú najvhodnejšie pre ich systémy.

DIGITALEUROPE
Rue de la Science, 14 - 1040 Brusel Belgicko
Tel. č. +32 (0) 2 609 53 10 Fax + 32 (0) 2 431 04 89
www.digitaleurope.org | info@digitaleurope.org | @DIGITALEUROPE
Člen Registra transparentnosti Komisie 64270747023

- Článok ohľadom noriem umožňuje, aby sa dalo odvolať na štandardy prijaté na európskej alebo medzinárodnej úrovni (článok 19.1). Vzhľadom na pripravenosť medzinárodných noriem v tejto oblasti si myslíme, že ak existujú primerané štandardy, certifikácia vo vzťahu k niektorému z nich (ako napríklad ISO 27001) by mala byť dostatočná na splnenie požiadaviek.

- V každom prípade by certifikácia mala byť dobrovoľná, nie povinná. Článok 19 prízvukuje, že dodržiavanie každej normy možno iba „podporovať" a malo by sa tak diať bez „zvýhodňovania alebo znevýhodňovania používania určitého druhu technológie."

e) Ohlasovanie bezpečnostných incidentov

- Čo sa bezpečnostných opatrení týka, podľa Smernice NIS sa na ohlasovaní incidentov podieľajú mnohí účastníci. Členské štáty sa musia ubezpečiť, že PDS budú nahlasovať udalosti ohrozujúce bezpečnosť, ktoré majú zásadný dopad na služby (čo je tiež cieľom Smernice), ktoré poskytujú (článok 16.3), pracovná skupina je poverená diskusiou o metódach ohlasovania (článok 11.3(m)) a úlohou Komisie je prijať vykonávacie akty (článok 16.8 a 9).

- Naším odporúčaním je opäť, aby vnútroštátne transpozície podrobili proces vykonávacím aktom, na základe ktorých musí byť v priebehu roka od dokončenia Smernice prijatý vykonávací akt ohľadom hranice pre ohlasovanie.

- Vzhľadom na to, aké druhy incidentov by sa mali nahlasovať, sú PDS poverení oznamovaním „všetkých udalostí, ktoré majú zásadný dopad na poskytovanie služieb" (článok 16.3). Čo sa týka zavedenia podobných ustanovení pre telekomunikačných operátorov v súlade s článkom 13a Rámcovej smernice, sme toho názoru, že by sme ho mali chápať ako zameranie sa na **plynulosť (alebo dostupnosť)** poskytovaných služieb. Inak povedané, mali by sa skôr ohlasovať výpadky, ktoré dosiahnu určitú hranicu (ktorú určia vykonávacie akty) než akékoľvek iné druhy bezpečnostných incidentov. Výhodou je, že pri zameraní sa na udalosti, ktoré najpravdepodobnejšie ovplyvnia hospodárstvo alebo spoločnosť možno minimalizovať (avšak nie úplne odstrániť) presah s požiadavkami na ohlasovanie narušenia ochrany osobných údajov pochádzajúcimi zo Všeobecného nariadenia o ochrane údajov.

- Ohlasovacia povinnosť „prevádzkovateľov základných služieb" stanovuje, že títo prevádzkovatelia sú povinní ohlásiť „udalosti so zásadným vplyvom na plynulosť základných poskytovaných služieb", čím sa teda jasne zameriava na kontinuitu (alebo dostupnosť) služby. Zákonodarcovia sa dohodli, že povinnosti PDS by mali byť miernejšie ako povinnosti PZS (pozri odôvodnenie 49). Povinnosť PDS nahlasovať incidenty vyplývajúca zo Smernice NIS by tak nemala byť rozsiahlejšia než pre PZS, čo sa hraničných hodnôt týka, práve naopak, mala by byť miernejšia. Tým si opäť pripomíname, že ohlasovanie incidentov zo strany PDS by malo byť obmedzené na udalosti, ktoré dosiahnú určitú hranicu a **majú dopad na plynulosť/dostupnosť služby** a nie incidenty súvisiace s úplnosťou a dôvernosťou údajov, ktoré sú už do veľkej miery zahrnuté v oznamovacích požiadavkách v rámci nariadení GDPR a eIDAS.

- Vo vzťahu k načasovaniu oznámení oceňujeme flexibilitu, ktorú implikujú jazykové prostriedky pri ohlasovaní ako povedzme „bez zbytočného odkladu" (článok 16.3). Implementácia by nemala

viesť k náročným termínom, keďže incidenty môžu mať rôzne úrovne zložitosti. Jednotné ohlasovacie časy by viedli k nepresnému oznamovaniu, nakoľko pôvodný rozsah zasiahnutých systémov je nejasný a ovplyvnil by schopnosť odborníkov reagujúcich na incidenty, ktorí by na incident skôr reagovali než ho oznámili.

- Ako bolo spomínané, bezpečnostné incidenty, ktoré sa majú na základe Smernice nahlásiť môžu vyžadovať aj notifikáciu podľa zákona o ochrane údajov, v závislosti od toho, či boli narušené osobné údaje. Nielenže sa tak rovnaký incident nahlasuje rôznym orgánom, ale dané orgány môžu byť aj v rozdielnych členských štátoch v závislosti od súdnej právomoci, ktorá sa uplatňuje pri PDS spadajúcich pod dve legislatívy. Odporúčame členským štátom, aby sa snažili zabezpečiť každé hlásenie incidentu a vytvárali komunikačné kanály na vzájomné zdieľanie dôležitých informácií a to bez porušenia obchodného tajomstva.

- Pred zverejnením informácií o incidentoch by kompetentné úrady mali zohľadniť dôsledky pre povesť a reklamu PDS. Respektíve, vyzradenie incidentu by mohlo zvýšiť bezpečnostné riziko. A preto je pred akýmkoľvek zverejnením dôležitá koordinácia účastníkov.

- Smernica zdôrazňuje, že s informáciami, ktoré sa považujú za dôverné by sa malo aj patrične zaobchádzať (odôvodnenia 41, 59, článok 1.5).

- Článok 16.3 hovorí, že oznámenie bezpečnostného incidentu nesmie vystaviť oznamujúcu stranu zvýšenej zodpovednosti.

2. Prevádzkovatelia základných služieb

a) Bezpečnostné opatrenia

- Na PDS, ktorých zákazníci sú PZS sa budú vzťahovať platné bezpečnostné opatrenia, z ktorých vyplynú zmluvné rokovania na základe štatutárnych povinností prevádzkovateľov základných služieb (článok 14.1). Ako také môžu byť nepriamo predmetom vnútroštátnych zákonov svojich zákazníkov bez ohľadu na platnú legislatívu v krajine EÚ, v ktorej sa nachádza ich centrála.

- A tak by snahy o zosúladenie bezpečnostných opatrení pre prevádzkovateľov základných služieb boli vítané. Hoci členské štáty majú právo zaviesť pre prevádzkovateľov základných služieb prísnejšie povinnosti než v Smernici (článok 3), neodporúčame to a uprednostňujeme, aby členské štáty pracovali na zosúladenom prístupe. Uvedené možno dosiahnuť zamedzením dodatočných opatrení vo vnútroštátnych transpozíciách a snahou vyvinúť vhodné bezpečnostné opatrenia v pracovnej skupine na rozdiel od zamerania sa na vnútroštátny proces.

- Bezpečnostné požiadavky by mali vychádzať z medzinárodných noriem a overených postupov v najvyššej možnej miere (ako ISO27x).

- Bezpečnostné opatrenia uložené PZS by za žiadnych okolností nemali vyžadovať, aby sa určitým spôsobom navrhovali, vytvárali alebo vyrábali určité produkty IKT (odôvodnenie 51).

b) Časový aspekt ohlasovania bezpečnostných incidentov

- Prevádzkovatelia základných služieb sú povinní oznámiť bezpečnostné incidenty, ktoré nastanú ich zmluvným PDS a ktoré majú dopad na plynulosť ich základných služieb (článok 16.5). PDS tak budú musieť na základe zmluvy informovať patričných prevádzkovateľov základných služieb o bezpečnostných udalostiach, ktoré by na nich mohli mať dopad.

- Oceňujeme flexibilitu v načasovaní pri ohlasovaní PZS obsiahnutú vo výraze „bez zbytočného odkladu“ (článok 14.3). Vnútroštátne transpozície by nemali určovať konkrétne termíny a v každom prípade ak majú PZS zdôvodniť čas potrebný na notifikáciu, by obdobie, ktoré sa bude posudzovať, malo začať chvíľou, kedy sa o udalosti dozvedeli PZS, nie PDS.

- Podľa článku 14.7 sa uvažuje o pracovnej skupine, ktorá by vytvorila príručku pre okolnosti ohlasovania na rozdiel od úlohy Komisie zosúladiť oznámenia PDS. Vzhľadom na dvojitú oznamovaciu požiadavku na strane PDS je dôležité, aby si prípadné oznamovacie požiadavky neodporovali a boli vyrovnané v najvyššej možnej miere. Za týmto účelom by sa mal proces preveriť. Oznamovacie požiadavky pre PDS by navyše mali zohľadňovať povinnosť mlčanlivosti, ktorá im vyplýva voči svojim zákazníkom PZS a nežiadať od nich vyzradenie obchodných tajomstiev.

DIGITALEUROPE
Rue de la Science, 14 - 1040 Brusel Belgicko
Tel. č. +32 (0) 2 609 53 10 Fax + 32 (0) 2 431 04 89
www.digitaleurope.org | info@digitaleurope.org | @DIGITALEUROPE
Člen Registra transparentnosti Komisie 64270747023

O DIGITALEUROPE

DIGITALEUROPE predstavuje európske odvetvie digitálnej technológie. Medzi našich členov patria niektoré najväčšie počítačové a telekomunikačné firmy, ako aj predajcovia spotrebnej elektrotechniky a celoštátne asociácie zo všetkých kútov Európy. Zámerom DIGITALEUROPE je, aby firmy a obyvatelia mohli plne využívať výhody digitálnych technológií a aby Európa rástla, udržiavala si a priťahovala najlepšie svetové značky v digitálnej technológii.

DIGITALEUROPE zabezpečuje, že odvetvie sa podieľa na tvorbe a zavádzaní politiky EÚ. DIGITALEUROPE má 62 korporátnych členov a 37 vnútroštátnych obchodných asociácií z celej Európy. Ak chcete vedieť viac o našich najnovších aktivitách, navštívte stránku: http://www.digitaleurope.org

Členstvo DIGITALEUROPE

Korporátni členovia

Airbus, Amazon Web Services, AMD, Apple, BlackBerry, Bose, Brother, CA Technologies, Canon, Cisco, Dell, Epson, Ericsson, Fujitsu, Google, Hewlett Packard Enterprise, Hitachi, HP Inc., Huawei, IBM, Ingram Micro, Intel, iQor, JVC Kenwood Group, Konica Minolta, Kyocera, Lenovo, Lexmark, LG Electronics, Loewe, Microsoft, Mitsubishi Electric Europe, Motorola Solutions, NEC, Nokia, Nvidia Ltd., Océ, Oki, Oracle, Panasonic Europe, Philips, Pioneer, Qualcomm, Ricoh Europe PLC, Samsung, SAP, SAS, Schneider Electric IT Corporation, Sharp Electronics, Siemens, Sony, Swatch Group, Technicolor, Texas Instruments, Toshiba, TP Vision, VMware, Western Digital, Xerox, Zebra Technologies, ZTE Corporation.

Obchodné združenia na národnej úrovni

Belgicko: AGORIA
Bielorusko: INFOPARK
Bulharsko: BAIT
Cyprus: CITEA
Dánsko: DI Digital, IT-BRANCHEN
Estónsko: ITL
Fínsko: FFTI
Francúzsko: AFNUM, Force Numérique, Tech in France
Grécko: SEPE
Holandsko: Nederland, ICT, FIAR
Írsko: ICT IRELAND
Litva: INFOBALT
Maďarsko: IVSZ
Nemecko: BITKOM, ZVEI
Poľsko: KIGEIT, PIIT, ZIPSEE
Portugalsko: AGEFE
Rakúsko: IOÖ
Rumunsko: ANIS, APDETIC
Slovensko: ITAS
Slovinsko: GZS
Španielsko: AMETIC
Spojené kráľovstvo: techUK
Švajčiarsko: SWICO
Švédsko: Foreningen Teknikföretagen i Sverige, IT&Telekomföretagen
Taliansko: ANITEC
Turecko: Digital Turkey Platform, ECID
Ukrajina: IT UKRAINE

DIGITALEUROPE
Rue de la Science, 14 - 1040 Brusel Belgicko
Tel. č. +32 (0) 2 609 53 10 Fax + 32 (0) 2 431 04 89
www.digitaleurope.org | info@digitaleurope.org | @DIGITALEUROPE
Člen Registra transparentnosti Komisie 64270747023