Svet
Evropske unije

Bruselj, 29. marec 2022
(OR. en)

Medinstitucionalna zadeva:
2022/0084 (COD)

7670/22
ADD 7

CSC 128
CSCI 45
CYBER 100
INST 99
INF 40
CODEC 385
IA 34

SPREMNI DOPIS

Pošiljatelj:	za generalno sekretarko Evropske komisije: direktorica Martine DEPREZ
Datum prejema:	22. marec 2022
Prejemnik:	generalni sekretar Sveta Evropske unije Jeppe TRANHOLM-MIKKELSEN
Št. dok. Kom.:	SWD(2022) 65 final
Zadeva:	DELOVNI DOKUMENT SLUŽB KOMISIJE POVZETEK OCENE UČINKA Spremni dokument predlog uredbe Evropskega parlamenta in Sveta o informacijski varnosti v institucijah, organih, uradih in agencijah unije

Delegacije prejmejo priloženi dokument SWD(2022) 65 final.

Priloga: SWD(2022) 65 final

EVROPSKA
KOMISIJA

Bruselj, 22.3.2022
SWD(2022) 65 final

DELOVNI DOKUMENT SLUŽB KOMISIJE

POVZETEK OCENE UČINKA

Spremni dokument

predlog uredbe Evropskega parlamenta in Sveta

o informacijski varnosti v institucijah, organih, uradih in agencijah unije

{COM(2022) 119 final} - {SWD(2022) 66 final}

Povzetek

Analiza učinka na informacijsko varnost v institucijah, organih, uradih in agencijah Unije

A. Politično ozadje

V strateški agendi Evropskega sveta za obdobje 2019–2024 so institucije pozvane, naj zaščitijo informacijska in komunikacijska omrežja EU ter svoje postopke odločanja pred vsemi vrstami zlonamernih dejavnosti, vključno s kibernetskimi in hibridnimi grožnjami. Posledično je Svet za splošne zadeve decembra 2019 sklenil, da bi morali institucije in organi EU razviti in izvajati celovit sklop ukrepov za zagotavljanje svoje informacijske varnosti.

Komisija je julija 2020 sprejela strategijo EU za varnostno unijo, s katero se je zavezala k dopolnjevanju nacionalnih prizadevanj na področju varnosti. Komisija je v okviru te strategije predlagala oblikovanje minimalnega sklopa pravil o informacijski in kibernetski varnosti v vseh institucijah in organih Unije.

B. V čem je težava?

Glavne težave so: i) znatna razlika med ravnjo varnosti institucijah in organih Unije glede na notranja pravila o varnosti informacij in ii) pomanjkanje usklajevanja med institucijami in organi Unije pri opravljanju njihovih nalog na področju varnosti.

Institucije in organi Unije imajo trenutno lastna pravila o varnosti informacij ali pa takih pravil sploh niso sprejeli. Razdrobljenost veljavnega pravnega okvira je privedla do različnih kategorij netajnih podatkov, različnih oznak in navodil za ravnanje na splošno. Kar zadeva tajne podatke EU, je interoperabilnost zadevnih sistemov še vedno omejena, kar preprečuje nemoten prenos informacij med institucijami in organi ter z državami članicami.

Te razmere povečujejo tveganje, da bi napadalci posegli v varnost v najšibkejšem členu in to uporabili kot izhodišče za nadaljnje napade na druge institucije ali organe.

C. Kaj bi bilo treba doseči?

Splošni cilj pobude je oblikovati pravila o informacijski varnosti za vse institucije in organe Unije za zagotovitev okrepljene in dosledne zaščite pred spreminjajočimi se grožnjami za njihove podatke.

Splošni cilj je povzet v štirih specifičnih ciljih:

- vzpostavitev usklajenih in celovitih kategorij informacij;
- opredelitev varnostnih vrzeli in izvajanje potrebnih ukrepov;
- vzpostavitev programa preudarnega sodelovanja na področju informacijske varnosti med institucijami in organi Unije;
- posodobitev politik za informacijsko varnost ob upoštevanju digitalne preobrazbe in dela na daljavo.

D. Kakšna so stališča različnih deležnikov?

Deležniki, s katerimi so potekala posvetovanja (institucije in organi Unije, nacionalni varnostni organi držav članic in strokovnjaki za raziskave iz Skupnega raziskovalnega središča), so se strinjali, da so

potrebni skupni standardi informacijske varnosti za vse institucije in organe Unije, s poudarkom na naslednjih točkah:

- upoštevati bi bilo treba raznolikost in različno poslovno okolje posamezne institucije ali organa Unije ter dopuščati lokalno rešitev;
- čeprav je večina institucij in organov pripravljena sodelovati s sorodnimi organi v skupnih organih za namene informacijske varnosti, niso pripravljeni prenesti svojih pooblastil za odločanje;
- osnutek uredbe bi bilo treba pripraviti ob upoštevanju medvladnega sporazuma[1] držav članic o varovanju tajnih podatkov.

E. Kakšen je učinek predloga?

Koristi

Osnutek uredbe bo z vzpostavitvijo osnove za pravila o informacijski varnosti v institucijah in organih Unije povečal splošno raven informacijske varnosti in hkrati zmanjšal sedanje razlike. Prav tako bi moral prispevati k odpravi morebitnih šibkih točk, hkrati pa zaščititi informacije, ki se izmenjujejo znotraj evropske uprave.

Z vidika učinkovitosti bi moral osnutek uredbe prinesti koristi od usklajenega izvajanja skupnih nalog na področju informacijske varnosti (npr. dovoljenja za dostop, akreditacija komunikacijskih in informacijskih sistemov) in vzpostavitve skupnih organov upravljanja (npr. medinstitucionalna koordinacijska skupina, tehnične podskupine).

Gospodarski učinek

Za institucije in organe Unije se pričakuje, da se bodo prizadevanja, potrebna za izvajanje nove zakonodaje, izravnala z večjo učinkovitostjo, medtem ko se lahko dodatni stroški krijejo iz obstoječih programov za izboljšanje informacijske varnosti vsake organizacije. Dolgoročno jim bo koristil skladen pristop k obravnavanju spreminjajočih se groženj za informacijsko varnost.

Evropska komisija bi morala zagotoviti stalni sekretariat medinstitucionalne usklajevalne skupine in dodeliti človeške vire za to nalogo (en uradnik AD in en uradnik AST).

Na ravni uprav držav članic in zasebnega sektorja naj ne bi bilo gospodarskih učinkov.

F. Spremljanje

Kdaj se bo politika pregledala?

Celovita ocena bo izvedena vsakih pet let po datumu začetka uporabe, da se ocenijo učinki in izvajanje osnutka uredbe. Komisija predstavi poročilo, v katerih navede svoje ugotovitve, ter ga predloži Evropskemu parlamentu in Svetu.

[1] Sporazum med državami članicami Evropske unije, ki so se sestale v okviru Sveta, o varovanju tajnih podatkov, ki se izmenjujejo v interesu Evropske unije, 2011/C202/05.