Vijeće
Europske unije

Bruxelles, 29. ožujka 2022.
(OR. en)

7670/22
ADD 7

Međuinstitucijski predmet:
2022/0084 (COD)

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

POPRATNA BILJEŠKA

Od:	Glavna tajnica Europske komisije, potpisala direktorica Martine DEPREZ
Datum primitka:	22. ožujka 2022.
Za:	Jeppe TRANHOLM-MIKKELSEN, glavni tajnik Vijeća Europske unije
Br. dok. Kom.:	SWD(2022) 65 final
Predmet:	RADNI DOKUMENT SLUŽBI KOMISIJE SAŽETAK IZVJEŠĆA O ANALIZI UČINKA priložen dokumentu Prijedlog uredbe Europskog parlamenta i Vijeća o sigurnosti podataka u institucijama, tijelima, uredima i agencijama Unije

Za delegacije se u prilogu nalazi dokument SWD(2022) 65 final.

Priloženo: SWD(2022) 65 final

EUROPSKA
KOMISIJA

Bruxelles, 22.3.2022.
SWD(2022) 65 final

RADNI DOKUMENT SLUŽBI KOMISIJE

SAŽETAK IZVJEŠĆA O ANALIZI UČINKA

priložen dokumentu

Prijedlog uredbe Europskog parlamenta i Vijeća

o sigurnosti podataka u institucijama, tijelima, uredima i agencijama Unije

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

Sažetak

Analiza učinka na sigurnost podataka u institucijama, tijelima, uredima i agencijama Unije

A. Politički kontekst

Europsko vijeće pozvalo je u Strateškom programu za razdoblje 2019.–2024. institucije da zaštite informacijske i komunikacijske mreže EU-a i njegove postupke donošenja odluka od svih vrsta zlonamjernih aktivnosti, uključujući kiberprijetnje i hibridne prijetnje. Na temelju toga Vijeće za opće poslove zaključilo je u prosincu 2019. da bi institucije i tijela EU-a trebale osmisliti i provesti sveobuhvatan skup mjera kojima će se zajamčiti sigurnost podataka.

Komisija je u srpnju 2020. donijela Strategiju EU-a za sigurnosnu uniju kojom se obvezala pridonijeti nacionalnim aktivnostima u području sigurnosti. U okviru te strategije Komisija je predložila uvođenje minimalnog skupa pravila o sigurnosti podataka i kibersigurnosti u svim institucijama i tijelima Unije.

B. Koji se problem rješava?

Glavni su problemi sljedeći: i. znatne razlike u razini sigurnosti među institucijama i tijelima Unije ovisno o njihovim internim pravilima o sigurnosti podataka te ii. nedostatak koordinacije među institucijama i tijelima Unije u obavljanju njihovih sigurnosnih zadaća.

Institucije i tijela Unije trenutačno imaju svoja pravila o sigurnosti podataka ili ih uopće nisu donijela. Zbog rascjepkanog primjenjivog pravnog okvira postoje različite kategorije neklasificiranih podataka te različite oznake i upute za postupanje na svim razinama. Kad je riječ o klasificiranim podacima EU-a, interoperabilnost relevantnih sustava i dalje je ograničena, što sprečava neometan prijenos podataka između institucija i tijela te prijenos koji obuhvaća države članice.

Takvo stanje povećava rizik da napadači povrijede sigurnost u najslabijoj karici i iskoriste je kao polazište za daljnje napade na druge institucije ili tijela.

C. Što bi trebalo postići?

Opći cilj inicijative je utvrditi pravila o sigurnosti podataka za sve institucije i tijela Unije kako bi se osigurala snažnija i dosljedna zaštita od novih prijetnji njihovim podacima.

Opći je cilj pretočen u četiri specifična cilja:

- uspostaviti usklađene i sveobuhvatne kategorija podataka,
- utvrditi sigurnosne nedostatke i poduzeti potrebne mjere,
- uspostaviti racionalnu suradnju institucija i tijela Unije u području sigurnosti podataka,
- modernizirati politike sigurnosti podataka, uzimajući u obzir digitalnu transformaciju i rad na daljinu.

D. Koja su stajališta različitih dionika?

Dionici koji su sudjelovali u savjetovanju (institucije i tijela Unije, nacionalna sigurnosna tijela država članica i stručnjaci za istraživanja iz JRC-a) složili su se da postoji potreba za zajedničkim standardima

sigurnosti podataka za sve institucije i tijela Unije te pritom naglasili:

- trebalo bi voditi računa o raznolikosti i različitim poslovnim okruženjima u institucijama i tijelima Unije te omogućiti primjenu lokalnih rješenja;
- premda je većina institucija i tijela spremna surađivati s kolegama u zajedničkim tijelima za potrebe sigurnosti podataka, oni nisu voljni delegirati svoje ovlasti za donošenje odluka;
- pri izradi nacrta uredbe trebalo bi uzeti u obzir Međuvladin sporazum[1] država članica o zaštiti klasificiranih podataka.

E. Koji je učinak prijedloga?

Koristi

U nacrtu uredbe utvrdit će se osnovna pravila o sigurnosti podataka u svim institucijama i tijelima Unije te tako povećati ukupne razine sigurnosti podataka i ujedno smanjiti postojeće razlike. Njime će se pridonijeti i uklanjanju mogućih slabih karika te ujedno zaštititi podatke koji se razmjenjuju unutar europske uprave.

Trebala bi se i povećati učinkovitost zbog koordinirane provedbe zajedničkih zadaća u području sigurnosti podataka (npr. sigurnosne provjere, akreditacija komunikacijskih i informacijskih sustava) i osnivanja zajedničkih upravljačkih tijela (npr. međuinstitucijska koordinacijska skupina, tehničke podskupine).

Ekonomski učinak

Očekuje se da će se rad institucija i tijela Unije potreban za provedbu novog propisa nadoknaditi povećanjem učinkovitosti, a dodatni troškovi mogu se pokriti u okviru postojećih programa za povećanje sigurnosti podataka svake organizacije. Dugoročno će imati koristi od dosljednog pristupa rješavanju sve većih prijetnji sigurnosti podataka.

Europska komisija trebala bi uspostaviti stalno tajništvo međuinstitucijske koordinacijske skupine i dodijeliti službenike za tu zadaću (jedan dužnosnik razreda AD i jedan razreda AST).

Ne očekuju se ekonomski učinci na razini uprava država članica i privatnog sektora.

F. Daljnje mjere

Kad će se predložene mjere preispitati?

Svakih pet godina od datuma početka primjene provest će se potpuna evaluacija kako bi se ocijenili učinci i provedba nacrta uredbe. Komisija će o tome predstaviti izvješće sa zaključcima i podnijeti ga Europskom parlamentu i Vijeću.

[1]Sporazum između država članica Europske unije, koje su se sastale u okviru Vijeća, o zaštiti klasificiranih podataka koji se razmjenjuju u interesu Europske unije, 2011/C202/05