

Bruselj, 29. marec 2022
(OR. en)

Medinstitucionalna zadeva:
2022/0084 (COD)

7670/22
ADD 3

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

PREDLOG

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.:	COM(2022) 119 final - Annex 3
Zadeva:	PRILOGA k predlogu UREDBE EVROPSKEGA PARLAMENTA IN SVETA o informacijski varnosti v institucijah, organih, uradih in agencijah Unije

Delegacije prejmejo priloženi dokument COM(2022) 119 final - Annex 3.

Priloga: COM(2022) 119 final - Annex 3



EVROPSKA
KOMISIJA

Bruselj, 22.3.2022
COM(2022) 119 final

ANNEX 3

PRILOGA

k

**predlogu UREDBE EVROPSKEGA PARLAMENTA IN SVETA
o informacijski varnosti v institucijah, organih, uradih in agencijah Unije**

{SWD(2022) 65 final} - {SWD(2022) 66 final}

PRILOGA III

Ukrepi za fizično zaščito tajnih podatkov EU

Oprema in organizacijski ukrepi za fizično zaščito tajnih podatkov EU

1. Upravno območje mora izpolnjevati naslednje zahteve:
 - (a) ima vidno določen varnostni perimenter, ki omogoča preverjanje posameznikov in po možnosti vozil;
 - (b) zagotavlja, da so okna, ki bi lahko nepooblaščenim osebam omogočila vizualni dostop do tajnih podatkov EU na območju, motna ali opremljena s senčili, zavesami ali drugimi zastori;
 - (c) dostop brez spremstva se odobri le posameznikom, ki jih je za to ustrezno pooblastil varnostni organ zadevne institucije ali organa Unije;
 - (d) vsi drugi posamezniki imajo ves čas spremstvo ali so pod enakovrednim nadzorom.
2. Poleg zahtev iz točke 1 mora varovano območje izpolnjevati naslednje zahteve:
 - (a) ima vidno določen in zaščiten varnostni perimenter, prek katerega se stalno nadzorujejo vsi vhodi in izhodi;
 - (b) na njem ni nedovoljenih komunikacijskih vodov, nedovoljenih telefonov ali drugih nedovoljenih komunikacijskih naprav ter električne in elektronske opreme;
 - (c) opremljen je z nadzorom dostopa in sistemom za odkrivanje vdorov v realnem času (v nadaljnjem besedilu: IDS) v kombinaciji z varnostnim osebjem za odzivanje;
 - (d) pregleduje se ob koncu običajnega delovnega časa in v naključnih časovnih presledkih zunaj običajnega delovnega časa, če na njem ni dežurnega osebja 24 ur na dan in ni vzpostavljen sistem IDS za spremljanje v realnem času;
 - (e) upravlja ga usposobljeno, nadzorovano in ustrezno varnostno preverjeno varnostno osebje;
 - (f) vzpostavljene ima varnostno-operativne postopke, ki vključujejo naslednje elemente:
 - (i) stopnjo tajnosti tajnih podatkov EU, ki se lahko obravnavajo in hranijo ter o katerih se lahko razpravlja na območju;
 - (ii) nadzorne in zaščitne ukrepe, ki jih je treba izvajati;
 - (iii) posameznike, ki so na podlagi svojega pooblastila za dostop do tajnih podatkov EU in potrebe po seznanitvi pooblaščenici za dostop na območje brez spremstva;
 - (iv) kjer je to ustrezno, postopke v zvezi s spremljanjem ali postopke za zaščito tajnih podatkov EU, ko je drugim posameznikom dovoljen dostop na območje;
 - (v) vse druge ustrezne ukrepe in postopke.
3. Če vstop na varovano območje pomeni neposreden dostop do tajnih podatkov na njem, je treba območje določiti kot območje razreda I, v nasprotnem primeru pa kot območje razreda II.

Za oba razreda varovanih območij iz prvega pododstavka in poleg zahtev iz točke 2 mora varnostni oddelek/uradnik zadevne institucije ali organa Unije jasno navesti najvišjo stopnjo tajnosti podatkov, ki se običajno hranijo na območju, in jasno določiti varnostni perimenter, ki omogoča preverjanje posameznikov in, če je mogoče, vozil.

Institucije in organi Unije morajo zagotoviti, da posamezniki, ki dostopajo do varovanega območja, izpolnjujejo naslednja merila:

- (a) za vstop na območje potrebujejo posebno pooblastilo;
 - (b) ves čas morajo imeti spremstvo;
 - (c) so ustrezno varnostno preverjeni, razen če so sprejeti ukrepi za zagotovitev, da dostop do tajnih podatkov EU ni mogoč.
4. Varovano območje, zaščiteno pred pasivnim in aktivnim prisluškovanjem, mora biti označeno kot tehnično varovano območje. Poleg zahtev za varovana območja se uporabljajo naslednje zahteve:
- (a) območje mora biti opremljeno z IDS in, kadar v prostorih ni nikogar, zaklenjeno, sicer pa varovano. Z vsemi ključi je treba ravnati v skladu s členom 29(3);
 - (b) varnostni organ zadevne institucije ali organa Unije mora območje redno fizično in/ali tehnično pregledovati. Takšne preglede je treba izvesti tudi po vsakem nepooblaščenem vstopu ali sumu takšnega vstopa;
 - (c) imeti mora ustrezno akustično zaščito in zaščito TEMPEST.
5. Vse osebe, ki vstopajo na tehnično varovana območja, morajo izpolnjevati zahteve iz točke 3.
6. Na upravnem območju se lahko zaradi zaupnega sestanka ali za druge podobne namene začasno vzpostavijo varovana območja in tehnično varovana območja.
7. Na varovanih območjih je treba zgraditi sobe trezorje. Soba trezor je soba z okrepljeno fizično konstrukcijo, katere stene, tla, strope, okna in vrata, ki jih je mogoče zakleniti, odobri varnostni organ zadevne institucije ali organa Unije. Takšni prostori morajo zagotavljati zaščito, enakovredno blagajni, odobreni za hrambo tajnih podatkov EU enake stopnje tajnosti.

Fizični zaščitni ukrepi za obravnavanje in hrambo tajnih podatkov EU

8. Tajne podatke EU stopnje tajnosti RESTREINT UE/EU RESTRICTED je treba obravnavati in hraniti na katerem koli od naslednjih območij:
- (a) na varovanem območju;
 - (b) na upravnem območju, če so tajni podatki EU zaščiteni pred dostopom nepooblaščenih posameznikov;
 - (c) zunaj varovanega območja ali upravnega območja, če se je imetnik zavezal, da bo upošteval izravnalne ukrepe, ki jih je določil varnostni organ posamezne institucije in organa Unije.
9. Tajne podatke EU stopnje tajnosti RESTREINT UE/EU RESTRICTED je treba hraniti v zaklenjenem pisarniškem pohištvi na upravnem območju ali varovanem območju. Začasno se lahko hranijo zunaj upravnega ali varovanega območja, če se je

imetnik zavezal, da bo zadevne dokumente hranil v ustreznem zaklenjenem pisarniškem pohištvu, ko se ne berejo ali se o njih ne razpravlja.

10. Institucije in organi Unije lahko podatke stopnje tajnosti RESTREINT UE/EU RESTRICTED obravnavajo in hranijo zunaj svojih lokacij, če so zadevni podatki ustrezno zaščiteni. V ta namen morajo institucije in organi Unije upoštevati ukrepe iz točke 8(c).
11. Podatke stopenj tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL in SECRET UE/EU SECRET je treba obravnavati in hraniti na enem od naslednjih območij:
 - (a) na varovanem območju;
 - (b) na upravnem območju, če so tajni podatki EU zaščiteni pred dostopom nepooblaščenih posameznikov;
 - (c) zunaj varovanega območja ali upravnega območja, če so količinsko in časovno omejeni ter se je imetnik zavezal, da bo upošteval izravnalne ukrepe, ki jih je določil varnostni organ zadevne institucije ali organa Unije. Poleg tega mora imetnik tajnih podatkov EU sprejeti naslednje ukrepe:
 - (i) obvestiti pristojni register o tem, da se tajni dokumenti obravnavajo zunaj zaščitenih območij;
 - (ii) imeti dokument ves čas pod nadzorom.
12. Podatke stopenj tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL in SECRET UE/EU SECRET je treba hraniti na varovanem območju, ki ga je za zadevno stopnjo akreditiral pristojni organ za varnostno akreditacijo zadevne institucije ali organa Unije, in sicer v blagajni ali sobi trezorju.
13. Dokumente stopnje tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL ali višje lahko kopira samo pristojni register.
14. Podatke stopnje tajnosti TRÈS SECRET UE/EU TOP SECRET je treba obravnavati in hraniti na varovanem območju, akreditiranem za to stopnjo. V ta namen lahko institucije in organi Unije sklenejo potrebne dogovore za uporabo varovanega območja, ki ga gosti in na ustrezni stopnji akreditira organ za varnostno akreditacijo druge institucije in organa Unije.
15. Podatke stopnje tajnosti TRÈS SECRET UE/EU TOP SECRET je treba hraniti na varovanem območju, ki ga je za to stopnjo akreditiral pristojni organ za varnostno akreditacijo zadevne institucije ali organa Unije, in sicer pod enim od naslednjih pogojev:
 - (a) v blagajni, ki jo odobri varnostni organ vsake institucije in organa Unije, z eno od naslednjih vrst dodatnega nadzora:
 - (i) neprekinjena zaščita ali preverjanje, ki ga izvaja varnostno osebje ali dežurno osebje, ki je bilo ustrezno varnostno preverjeno;
 - (ii) odobren IDS v kombinaciji z varnostnim osebjem za odzivanje;
 - (b) v sobi trezorju, opremljeni z IDS, v kombinaciji z varnostnim osebjem za odzivanje.