►**B**

PADOMES LĒMUMS (KĀDP) 2021/1026

(2021. gada 21. jūnijs),

ar ko atbalsta Ķīmisko ieroču aizlieguma organizācijas (*OPCW*) Kiberdrošības un noturības un informācijas aizsardzības programmu, īstenojot ES Stratēģiju masu iznīcināšanas ieroču izplatīšanas novēršanai

(OV L 224, 24.6.2021., 24. lpp.)

Grozīts ar:

		Oficiālais Vēstnesis		
		Nr.	Lappuse	Datums
►**M1**	Padomes Lēmums (KĀDP) 2023/1515 (2023. gada 20. jūlijs)	L 184	37	21.7.2023.

▼B

PADOMES LĒMUMS (KĀDP) 2021/1026

(2021. gada 21. jūnijs),

ar ko atbalsta Ķīmisko ieroču aizlieguma organizācijas (*OPCW*) Kiberdrošības un noturības un informācijas aizsardzības programmu, īstenojot ES Stratēģiju masu iznīcināšanas ieroču izplatīšanas novēršanai

1. pants

1. Lai varētu tūlīt un praktiski piemērot dažus ES Stratēģijā paredzētos elementus, Savienība atbalsta *OPCW* projektu, kura mērķis ir:

— atjaunināt IKT infrastruktūru atbilstīgi *OPCW* institucionālajam darbības nepārtrauktības satvaram, spēcīgu uzsvaru liekot uz noturību, un

— nodrošināt privileģētas piekļuves pārvaldību, kā arī fizisku, loģisku un kriptogrāfisku informācijas pārvaldību un nodalīšanu attiecībā uz visiem *OPCW* stratēģiskajiem un misiju tīkliem.

2. Šā panta 1. punkta kontekstā Savienības atbalstītās *OPCW* projekta darbības, kas atbilst ES Stratēģijas III nodaļā izklāstītajiem pasākumiem, ir šādas:

— tādas vides nodrošināšana, kas veicina notiekošos centienus kiberdrošības un noturības jomā ar vairākām vietām saistītās *OPCW* operācijās,

— pielāgotu risinājumu izstrāde lokālas un mākonī izvietotas sistēmas integrēšanai un konfigurēšanai ar *OPCW* IKT sistēmām un privileģētās piekļuves pārvaldības (*PAM*) risinājumiem, un

— *PAM* risinājumu izstrāde un testēšana.

3. Sīks 2. punktā minēto Savienības atbalstīto *OPCW* darbību apraksts ir izklāstīts pielikumā.

2. pants

1. Par šā lēmuma īstenošanu atbild Eiropas Savienības Augstais pārstāvis ārlietās un drošības politikas jautājumos (“AP”).

2. Šā lēmuma 1. pantā minētā projekta tehnisko īstenošanu veic *OPCW* Tehniskais sekretariāts (“Tehniskais sekretariāts”). Par to, kā tas veic šo uzdevumu, ir atbildīgs un to kontrolē AP. Šim nolūkam AP slēdz atbilstīgas vienošanās ar Tehnisko sekretariātu.

▼B

3. pants

1. Finanšu atsauces summa 1. pantā minētā projekta īstenošanai ir 2 151 823 EUR.

2. Izdevumus, ko finansē no 1. punktā minētās summas, pārvalda saskaņā ar procedūrām un noteikumiem, ko piemēro Savienības vispārējam budžetam.

3. Komisija uzrauga 2. punktā minēto izdevumu pareizu pārvaldību. Minētajam nolūkam tā slēdz nepieciešamo nolīgumu ar Tehnisko sekretariātu. Minētajā nolīgumā paredz, ka Tehniskais sekretariāts nodrošina Savienības ieguldījuma apjomam atbilstīgu redzamību un precizē pasākumus, lai veicinātu sinerģiju veidošanos un izvairītos no darbību dublēšanās.

4. Komisija cenšas noslēgt 3. punktā minēto nolīgumu, cik drīz vien iespējams pēc šī lēmuma stāšanās spēkā. Tā informē Padomi par jebkādām grūtībām šajā procesā, kā arī par nolīguma noslēgšanas dienu.

4. pants

Pamatojoties uz Tehniskā sekretariāta sagatavotiem regulāriem ziņojumiem, AP ziņo Padomei par šā lēmuma īstenošanu. AP ziņojumi ir Padomes veikto izvērtējumu pamatā. Komisija sniedz informāciju par 1. pantā minētā projekta finansiālajiem aspektiem.

5. pants

1. Šis lēmums stājas spēkā tā pieņemšanas dienā.

▼M1

2. Šis lēmums zaudē spēku 2024. gada 30. augustā.

▼B

PIELIKUMS

PROJEKTA DOKUMENTS

1. Konteksts

OPCW ir jāuztur infrastruktūra, kura ļauj pastāvēt tādai informācijas suverenitātei, kas atbilst privileģētas piekļuves klasifikācijām, atbilstīgām apstrādes procedūrām un pastāvošajiem apdraudējumiem un kas vienlaikus saglabā spēju aizsargāties pret jauniem riskiem. *OPCW* joprojām pastāvīgi saskaras ar nopietniem un jauniem riskiem saistībā ar kiberdrošību un kibernoturību. Pret *OPCW* uzbrukumus vērš ļoti prasmīgi un motivēti aktori, kam pieejami lieli resursi. Šie aktori turpina regulāri uzbrukt *OPCW* informācijas un infrastruktūras aktīvu konfidencialitātei un integritātei. Lai reaģētu uz bažām, kuras izraisa nesenie kiberuzbrukumi, pašreizējie politikas apsvērumi un Covid-19 krīze, un ņemot vērā unikālās prasības, ko izvirza *OPCW* darba raksturs – īstenot *CWC* pilnvaras –, ir skaidrs, ka ir nepieciešamas būtiskas investīcijas tehniskajās spējās.

Saskaņā ar *OPCW* Īpašo kiberdrošības, darbības nepārtrauktības un fiziskās infrastruktūras drošības fondu *OPCW* ir izstrādājusi savu Kiberdrošības un noturības un informācijas aizsardzības programmu (*OPCW* programma), kurā ir paredzētas 47 darbības, ar kurām vēršas pret pēdējā laikā pieredzētajiem drošības izaicinājumiem. *OPCW* programma ir pielāgota paraugpraksei, kuru popularizē tādas struktūras kā Eiropas Savienības Kiberdrošības aģentūra (*ENISA*), vai izmantojot koncepcijas, kas saistītas ar Eiropas Tīklu un informācijas sistēmu drošības (TID) direktīvu, kas attiecas uz telesakariem un aizsardzību. Kopumā *OPCW* programma aptver šādas tematiskas jomas: klasificēti un neklasificēti tīkli; politika un pārvaldība; atklāšana un reaģēšana; operācijas un apkope; un telesakari. *OPCW* programma ir paredzēta galvenokārt tam, lai palīdzētu *OPCW* samazināt iespējas, ka ar lieliem resursiem nodrošināti un/vai valsts algoti uzbrucēji sasniedz savus mērķus, un mazināt riskus, kurus rada gan ārējie, gan iekšējie apdraudējumi gan cilvēciskā, gan tehniskā aspektā. Savienības atbalsts ir strukturēts kā trīs darbību projekts, kuras atbilst divām no 47 *OPCW* programmas darbībām.

2. Projekta mērķis

Projekta vispārējais mērķis ir nodrošināt, ka *OPCW* sekretariāts spēj saglabāt piemērotu kiberdrošības un noturības līmeni, vēršoties pret esošiem un jauniem kiberdrošības aizsardzības izaicinājumiem *OPCW* galvenajā mītnē un papildu objektos, dot iespēju realizēt *OPCW* pilnvaras un efektīvi īstenot *CWC*.

3. Mērķi

— Atjaunināt IKT infrastruktūru atbilstīgi *OPCW* institucionālajam darbības nepārtrauktības satvaram, liekot spēcīgu uzsvaru uz noturību,

— nodrošināt privileģētas piekļuves pārvaldību, kā arī fizisku, loģisku un kriptogrāfisku informācijas pārvaldību un nodalīšanu attiecībā uz visiem stratēģiskajiem un misiju tīkliem.

▼B

4. Rezultāti

Sagaidāmie rezultāti, kurus projekts palīdz sasniegt, ir šādi:

— IKT aprīkojums un pakalpojumi nodrošina stipru sistēmas uzticamību (hibrīdā/ģeogrāfiskā redundance) un veicina plašāku IKT sistēmu un pakalpojumu pieejamību darbības nepārtrauktības atbalstam,

— līdz minimumam samazināta iespēja, ka jebkurš atsevišķs faktors vai cilvēks varētu nelabvēlīgi ietekmēt *OPCW* informācijas sistēmu konfidencialitāti un integritāti.

5. Darbības

5.1. Darbība Nr. 1 – tādas vides nodrošināšana, kas veicina notiekošos centienus kiberdrošības un noturības jomā ar vairākām vietām saistītās *OPCW* operācijās

Ar šo darbību cenšas nodrošināt labvēlīgu vidi netraucētai *OPCW* darbības nepārtrauktības plānošanai attiecībā uz kiberdrošību un noturību. To panāks, īstenojot infrastruktūras atjauninājumus – jaunu arhitektūru un/vai arhivēšanu *OPCW* darbības nepārtrauktībai attiecībā uz vairākās vietās notiekošām operācijām. Kā arī – turpinot atvieglināt un veicināt privileģētas piekļuves pārvaldību darbības nepārtrauktības plānošanas un reaģēšanas procesos.

5.2. Darbība Nr. 2 – pielāgota risinājuma izstrāde lokālu un mākonī izvietotu sistēmu integrēšanai un konfigurēšanai ar *OPCW* IKT sistēmām un privileģētās piekļuves pārvaldības (*PAM*) risinājumiem

Ar šo darbību ir paredzēts, balstoties uz labvēlīgu vidi, izstrādāt pielāgotu versiju lokālu un mākonī izvietotu sistēmu integrēšanai un konfigurēšanai ar *OPCW* IKT sistēmām un *PAM* risinājumiem. Sagaidāms, ka tas palielinās IKT sistēmu infrastruktūras efektivitāti un palīdzēs izstrādāt integrētu *PAM* sistēmu attiecībā uz kritiskiem aktīviem, kas var atturēt un konstatēt un atbilst proaktīvām draudu apzināšanas spējām.

5.3. Darbība Nr. 3 – *PAM* risinājumu izstrāde un testēšana

Šī darbība balstās uz ieviesto infrastruktūru un *PAM* risinājumiem, kas paredzēti, lai integrāciju un konfigurāciju virzītu no teorijas uz praksi. Sistēmas vajag kartēt, izstrādāt profilu un iegult esošajās sistēmās, vienlaikus ņemot vērā saistītos politikas un cilvēka faktorus. Pēc tam rūpīgā testēšanā pārbauda un nodrošina sistēmas izturību (visām jaunām sistēmām ir spēcīga autentificēšana attiecībā uz lietotājiem un ierīcēm, atbilstīga informācijas klasificēšana un aizsardzība un augsti attīstīta aizsardzība pret datu zudumu) īstenošanā un laika gaitā, kas *OPCW* sekretariātam dos iespēju, cik vien iespējams, identificēt un novērst trūkumus.

6. Ilgums

Sagaidāms, ka ar šo projektu finansētā īstenošana tiks sākta un pabeigta kopumā 24 mēnešos.

7. Saņēmēji

Šā projekta labuma guvēji būs *OPCW* Tehniskā sekretariāta personāls, politikas veidošanas struktūras, pakļautās izpildinstitūcijas un *CWC* ieinteresētās personas, tostarp projekta dalībvalstis.

8. ES redzamība

OPCW veiks visus vajadzīgos pasākumus, ievērojot saprātīgus drošības apsvērumus, lai darītu plaši zināmu to, ka šo projektu ir finansējusi Savienība.