

Sprječavanje pranja novca i financiranja terorizma: zakonodavne aktualnosti, cyber rizici i AI



15. listopada 2026. u 10 sati | Online – MS Teams

Svrha i cilj edukacije

Hrvatska gospodarska komora nastavlja aktivnosti na provođenju edukacija o sprječavanju pranja novca i financiranja terorizma. Webinar je prvenstveno namijenjen obveznicima primjene mjera, radnji i postupaka iz Zakona o sprječavanju pranja novca i financiranja terorizma (NN 108/17, 39/19, 151/22). Edukacija može biti korisna i ostalim dionicima financijskog tržišta i poslovne zajednice koji žele bolje razumjeti kako digitalni rizici, uključujući one koje donosi umjetna inteligencija, izravno utječu na otpornost gospodarstva i financijskog sustava.

U prvom dijelu webinara sudionici će se upoznati s pravnim okvirom, obvezama obveznika i zakonodavnim aktualnostima u području sprječavanja pranja novca i financiranja terorizma u Republici Hrvatskoj, s posebnim naglaskom na konkretne primjere pranja novca i financiranja terorizma iz zemlje i svijeta. U nastavku će biti govora i o mjerama ograničavanja.

Cyber kriminal i umjetna inteligencija kao novo lice pranja novca i financiranja terorizma teme su drugog dijela webinara. Financijsko tržište je digitalizirano, klasične metode sprječavanja pranja novca više nisu dovoljne za razumijevanje pravih razmjera prijetnje. Cyber kriminal ne samo da omogućuje prikrivanje nezakonitih tokova, već se sve češće koristi kao poluga za samo pranje novca, od insceniranih ransomware napada do zloupotrebe fintech platformi i kriptovaluta. Umjetna inteligencija ovu sliku dodatno usložnjava: ista tehnologija koja kriminalcima omogućuje uvjerljivije prijevare i bržu automatizaciju, financijskim institucijama i tijelima nadzora daje snažnije alate za prepoznavanje sumnjivih obrazaca. Na webinaru ćemo, kroz primjere iz prakse, osvijetliti na koje se načine kibernetički rizici pretvaraju u financijske gubitke i u "opravdane" transakcije, te kako se isti obrasci koriste i za financiranje terorizma. Posebnu pažnju posvetit ćemo ulozi AI-ja s obje strane te jednadžbe, od deepfake identiteta i sintetičkih dokumenata koji zaobilaze provjere klijenata, do algoritamske analitike koja AML timovima omogućuje otkrivanje anomalija u stvarnom vremenu.

Svi sudionici dobit će Potvrdu o sudjelovanju i prezentacije s webinara.

Temeljem dobivene prethodne suglasnosti Ministarstva financija ovlašteni revizori ostvaruju 3 boda stalnog stručnog usavršavanja (Ostala područja, oznaka „A“).

Kome je edukacija namijenjena?

- djelatnost prometa plemenitih metala i dragog kamenja,
- djelatnosti povezane s virtualnom imovinom,
- priređivači igara na sreću,
- revizorska društva, samostalni revizori, društva za porezno savjetništvo, porezni savjetnici, računovođe,
- odvjetnička društva, odvjetnici, javni bilježnici,
- djelatnost posredovanja u prometu nekretnina,
- ovlašteni mjenjači,
- financijske institucije i ostali obveznici provedbe mjera iz članka 9. Zakona o sprječavanju pranja novca i financiranja terorizma te svi ostali zainteresirani za ovu temu.



Kotizacija za sudjelovanje:

- 100,00 € - uz plaćenu članarinu HGK, bilježi se kao konzumirana usluga iz članarine
- 100,00 €* - za ostale
- Prijave se primaju do utorka, 13. listopada 2026.
- Dostava poveznice za sudjelovanje dan uoči edukacije.



Kontakt osoba:

Vanja Dominović, HGK, Rooseveltov trg 2, Zagreb,
01 4561 564, vdominovic@hgk.hr

* Temeljem čl. 39. st. 1. toč. i) Zakona o PDV-u, kotizacija je oslobođena od PDV-a.

SAT	NAZIV
09:45 - 10:00	Prijava sudionika putem Microsoft Teams aplikacije
10:00 - 10:15	Hrvatska gospodarska komora Odjel za financijske institucije i osiguravajuća društva Vanja Dominović • Uvodno izlaganje i predstavljanje usluga Digitalne komore

▼ **Predavač: Tatjana Kovač Klemar**

10:15 - 11:45	Zakonodavni okvir, aktualnosti i primjeri iz prakse • Sprječavanje pranja novca i financiranja terorizma – zakonodavni okvir i obveze obveznika • AMLA – Anti-Money Laundering Authority • Specifičnosti sprječavanja financiranja terorizma • Slučajevi pranja novca iz zemlje i svijeta • Slučajevi financiranja terorizma iz svijeta • Zakon o mjerama ograničavanja
11:45 - 12:00	Pauza

▼ **Predavač: Marko Gulan**

12:00 - 13:30	Cyber kriminal i umjetna inteligencija kao novo lice pranja novca i financiranja terorizma: • Kako cyber napadi služe kao maska za legalizaciju prljavog novca? • Zašto je suradnja između AML i cyber sigurnosti ključna? • Koje nove prijetnje dolaze kroz kriptovalute, DeFi i darknet tržišta? • Kako umjetna inteligencija istovremeno postaje oružje pranja novca (deepfake verifikacija identiteta, sintetički dokumenti, automatizirane mule mreže) i ključan alat za njegovo otkrivanje (napredna analitika, prepoznavanje obrazaca ponašanja, prediktivni modeli rizika)?
---------------	--

Tatjana Kovač Klemar

inicijalno je završila Ekonomski fakultet, smjer: financije, da bi kasnije obranila znanstveni magisterij iz područja Međunarodnih odnosa i nacionalne sigurnosti s temom: Modaliteti financiranja terorizma.

Autorica je niza provedbenih propisa iz područja sprječavanja pranja novca i financiranja terorizma iz područja tržišta kapitala. Bila je na više tjednoj edukaciji, na poziv State Departmenta SAD-a, iz područja sprječavanja pranja novca, financiranja terorizma i antikorupcije u Sjedinjenim Američkim Državama. Koautorica je knjige o Sprječavanju pranja novca i financiranja terorizma i autorica nekoliko međunarodno objavljenih članaka s tematikom vezanom uz sprječavanje pranja novca i financiranja terorizma.



Marko Gulan

CEO Astera Advisory, ISO 27001:2022 Lead Auditor, više od 15 godina prisutan je na domaćem i regionalnom ICT tržištu, s posljednjih osam godina fokusa na sigurnost i kibernetičku sigurnost. Kroz karijeru je surađivao s najznačajnijim organizacijama kritične infrastructure u jugo-istočnij Europi na implementaciji sigurnosnih rješenja, edukaciji timova i izgradnji strategija upravljanja rizicima u digitalnom okruženju.

Prije poduzetničkog puta bio je direktor kibernetičke sigurnosti u globalnoj korporaciji za područje jugoistočne Europe te regionalni CISO, gdje je sigurnosne strategije oblikovao na razini koja povezuje tehničku izvedbu s poslovnim odlukama uprave. Aktivno je sudjelovao u transpoziciji NIS2 Direktive te u usklađivanju proizvoda i rješenja za kritičnu infrastrukturu s Cyber Resilience Actom i industrijskim standardom IEC 62443 u 22 zemlje EU-a. To je iskustvo koje danas ugrađuje u savjetovanje klijenata na Hrvatskom i regionalnom tržištu.

Autor je programa Akademije kibernetičke sigurnosti pri Hrvatskoj gospodarskoj komori, kroz koji sustavno doprinosi razumijevanju prijetnji i odgovora na kibernetičke incidente u poslovnom sektoru. Član je Hrvatske udruge menadžera sigurnosti, gdje aktivno promiče dobru praksu u zaštiti podataka i sustava. Poseban fokus stavlja na povezivanje kibernetičke sigurnosti sa strategijama poslovnog kontinuiteta, osiguranjem i edukacijom upravljačkih struktura, jer otpornost organizacije danas počinje od poslovne zrelosti i strateške odluke uprave da rizik shvati kao svoj, a ne samo tehnički problem.