

Nacrt Uredbe

Pouzdanost i informacijska sigurnost sustava igara na sreću na temelju Zakona o igrama na sreću

Sadržaj

Pouzdanost i informacijska sigurnost sustava igara na sreću na temelju Zakona o igrama na sreću....	1
1 Pravni okvir, područje primjene i definicije.....	2
1.1 Ovlašt nadzornog tijela za izdavanje naredbi.....	2
1.2 Zakonodavstvo.....	2
1.3 Područje primjene.....	2
1.4 Definicije.....	2
2 Akreditacija inspekcijskog tijela.....	3
3 Opće prakse u području informacijske sigurnosti.....	3
4 Inspekcijsko tijelo koje provodi ispitivanje informacijske sigurnosti.....	3
4.1 Područje nadležnosti.....	4
5 Obnova testiranja informacijske sigurnosti.....	4
6 Odbijeno ispitivanje informacijske sigurnosti.....	5
7 Skeniranje osjetljivosti.....	5
8 Provjere osjetljivosti provedene u vezi s testiranjem informacijske sigurnosti.....	6
9 Uklanjanje osjetljivosti.....	6
10 Uporaba izdanih potvrda.....	6
11 Neusklađenosti.....	6
12 Stupanje na snagu.....	7

1 Pravni okvir, područje primjene i definicije

1.1 Ovlast nadzornog tijela za izdavanje naredbi

Pravo nadzornog tijela na donošenje obvezujuće naredbe temelji se na članku 44. stavku 6. Zakona o igrama na sreću (xx/2025). U skladu s navedenim podstavkom, nadzorno tijelo može izdati detaljnije propise o pouzdanosti sustava igara na sreću, opreme za lutriju i metoda lutrije koje se upotrebljavaju u priređivanju igara na sreću, o tehničkim zahtjevima za osiguravanje nasumičnosti izvlačenja, o detaljnijem obliku i sadržaju istrage i odobrenja inspekcijskog tijela te o uvjetima koje inspekcijsko tijelo mora ispuniti kako bi ga odobrilo Nadzorno tijelo.

U skladu s člankom 57. Zakona o igrama na sreću, nadzorno tijelo je Finska nadzorna agencija. U skladu s člankom 106. Zakona, Nacionalni policijski odbor djeluje kao nadležno tijelo iz članka 57. do 31. prosinca 2026.

1.2 Zakonodavstvo

Za predmet ove naredbe relevantni su sljedeći propisi:

- Zakon o igrama na sreću (xx/2025)
- Zakon o upravnom postupku (434/2003)
- Zakon o zaštiti podataka (1050/2018)
- Opća uredba o zaštiti podataka (2016/679)

1.3 Područje primjene

Ova se odredba primjenjuje na pravnu ili fizičku osobu iz poglavlja 1. članka 2. stavka 1. Zakona o igrama na sreću kojoj je dodijeljena isključiva dozvola ili dozvola za aktivnosti igara na sreću u skladu sa Zakonom o igrama na sreću.

Isključiva dozvola uređena je člankom 5. Zakona o igrama na sreću, a dozvola za igre na sreću uređena je člankom 6.

1.4 Definicije

Za potrebe ove odredbe primjenjuju se sljedeće definicije: Za potrebe ove Uredbe:

- *isključiva dozvola* znači dozvola dodijeljena za oblike igara na sreću iz članka 5. Zakona o igrama na sreću
- *dozvola za igre* na sreću znači dozvola izdana za vrste igara na sreću iz članka 6. Zakona o igrama na sreću
- *transakcija igara na sreću* znači ulog koji igrač ulaže u igru, mogućnost ishoda koji je odabrao igrač, odabir igrača koji je relevantan za ishod igre i rezultate

tržišta i izvlačenja, kao i sve dobitke i gubitke zabilježene u sustavu igara na sreću nositelja isključive dozvole ili dozvole za igre na sreću

- *transakcija računa igrača* znači unose na račun
- *sustav igara na sreću* znači internetski informacijski sustav kojim se koristi priređivač igara na sreću ili koji se upotrebljava u njegovo ime za priređivanje igara na sreću.

2 Akreditacija inspekcijskog tijela

Nositelj dozvole odgovoran je za pouzdanost svojih lutrijskih uređaja i sustava igara na sreću, kao i za provođenje revizija koje se obavljaju radi osiguranja te pouzdanosti. Procjenu pouzdanosti i sigurnosti provodi vanjsko akreditirano inspekcijsko tijelo. Tijelo je akreditirano u skladu s Uredbom (EZ) br. 765/2008 Europskog parlamenta i Vijeća o utvrđivanju zahtjeva za akreditaciju i za nadzor tržišta u odnosu na stavljanje proizvoda na tržište i o stavljanju izvan snage Uredbe (EEZ) br. 339/93.

Akreditaciju inspekcijskim tijelima može dodijeliti nacionalno akreditacijsko tijelo FINAS (Finska služba za akreditaciju). Strano akreditacijsko tijelo može djelovati i kao akreditacijsko tijelo ako je član Multilateralnog sporazuma o priznavanju jednakosti akreditacije s EA (EA MLA) u relevantnom području nadležnosti. Nositelj dozvole dužan je osigurati da vanjski subjekt koji provodi nadzor ima valjanu akreditaciju.

3 Opće prakse u području informacijske sigurnosti

Nositelj dozvole odgovoran je za informacijsku sigurnost, zaštitu podataka i druge tehničke značajke pouzdanosti vlastitih sustava igara na sreću. Nositelj dozvole mora u svom poslovanju primjenjivati dobre prakse informacijske sigurnosti te nastojati svesti na najmanju mjeru prijetnje informacijskoj sigurnosti, povrede podataka i druge probleme koji bi mogli ugroziti pouzdanost sustava igara na sreću. Nositelj dozvole dužan je i pratiti prethodno navedene čimbenike izvan redovitih inspekcijskih pregleda iz ove Uredbe kako bi osigurao pouzdanost svojih sustava.

4 Inspekcijsko tijelo koje provodi ispitivanje informacijske sigurnosti

Nositelj dozvole dužan je svake dvije godine provesti sigurnosno ispitivanje svojih sustava igara na sreću. Ishod testiranja informacijske sigurnosti podnosi se nadzornom tijelu. Ispitivanje informacijske sigurnosti i njegov ishod ne smiju biti stariji od dvije godine.

Ispitivanje informacijske sigurnosti provodi vanjsko inspekcijsko tijelo akreditirano u skladu s normama ISO/IEC 17025, ISO/IEC 17065 ili ISO/IEC 17020, kako je navedeno u članku 2. ove Uredbe. Pri testiranju informacijske sigurnosti posebna se pozornost posvećuje zaštiti i integritetu sastavnih dijelova sustava nasumičnih igara na sreću, zaštiti sastavnih dijelova koji sadržavaju osobne podatke i zaštiti sastavnih dijelova povezanih s plaćanjem.

Inspekcijsko tijelo odgovorno za provođenje ispitivanja informacijske sigurnosti i njegovi zaposlenici moraju biti kompetentni i prikladni za provođenje ispitivanja. Potrebna sposobnost za provođenje ispitivanja informacijske sigurnosti može se dokazati, među ostalim, prethodnim stručnim iskustvom u ispitivanju informacijske sigurnosti, osposobljavanju ili općenito priznatim industrijskim certifikatima. Nositelj dozvole dužan je osigurati da su osobe koje provode testiranje kvalificirane za provođenje testiranja informacijske sigurnosti i, na zahtjev, dokazati njihove kvalifikacije.

Za provedbu testiranja sigurnosti mora se imenovati određena osoba koja će biti odgovorna za njegovu odgovarajuću provedbu. Završno izvješće o ispitivanju informacijske sigurnosti potpisuje i potvrđuje imenovana osoba te se ono podnosi nadzornom tijelu.

U kontekstu ispitivanja informacijske sigurnosti ispituju se barem sljedeći sastavni dijelovi, kao i povezane osjetljivosti ili incidenti:

- Mogućnost manipulacije nasumičnim sastavnim dijelovima
- Pristup bazi podataka o klijentima
- Sposobnost utjecanja na ishod igara
- Sposobnost utjecanja na platne sustave ili platne transakcije
- Neovlašteni pristup poslužiteljima koji se upotrebljavaju za pohranu transakcija igara na sreću i transakcija računa igrača
- Mogućnost uređivanja arhiviranih podataka o događajima povezanim s igrama na sreću ili računima za igre na sreću
- Izmjena ili uništavanje zapisnika povezanih sa sustavima igara na sreću

4.1 Područje nadležnosti

Akreditirano inspekcijsko tijelo koje provodi reviziju mora imati područje nadležnosti za igre na sreću u svojoj akreditaciji prema normi ISO/IEC. Područje nadležnosti mora obuhvaćati zahtjeve utvrđene finskim zakonodavstvom o igrama na sreću i tehničkim propisima nadzornog tijela.

Nadzorno tijelo može do 1. siječnja 2027. prihvatiti akreditaciju koja uključuje opseg nadležnosti koji je procijenjen i dodijeljen na temelju tehničkih propisa izdanih za danske ili švedske sustave igara na sreću.

5 Obnova testiranja informacijske sigurnosti

Nositelj dozvole dostavlja rezultate odobrenog ispitivanja informacijske sigurnosti nadzornom tijelu. Nositelj dozvole ne smije započeti s priređivanjem igara na sreću prije nego što uspješno prođe sigurnosno ispitivanje. Ishod ispitivanja informacijske sigurnosti ne smije biti stariji od dvije godine.

Nadzorno tijelo može, prema vlastitom nahođenju, odobriti dodatno vrijeme za provedbu sigurnosnog ispitivanja, tijekom kojeg se priređivanje igara na sreću može nastaviti.

6 Odbijeno ispitivanje informacijske sigurnosti

Inspeksijsko tijelo koje provodi ispitivanje informacijske sigurnosti treba procijeniti utvrđene osjetljivosti tijekom testiranja informacijske sigurnosti te njihov značaj za pouzdanost sustava igara na sreću. Osjetljivosti utvrđene tijekom procjene trebalo bi procijeniti s pomoću kalkulatora CVSS v3 (Zajednički sustav bodovanja osjetljivosti, verzija 3.) koji pruža Nacionalni institut za tehnologiju (NIST). Za kalkulator CVSS v3 ozbiljnost osjetljivosti procjenjuje se primjenom osnovnih pokazatelja rezultata. Ako se tijekom sigurnosnog ispitivanja otkriju osjetljivosti s izračunanom vrijednošću CVSS-a većom od 5,0, ispitivanje se ne može smatrati uspješnim.

Ako test informacijske sigurnosti nositelja dozvole nije odobren, nositelj dozvole mora odmah poduzeti mjere za otklanjanje utvrđenih osjetljivosti u području informacijske sigurnosti. Nositelj dozvole izvješćuje nadzorno tijelo o odbijenom testu informacijske sigurnosti.

Nositelj dozvole mora provesti novo ispitivanje sigurnosti u roku od 90 dana od odbijenog ispitivanja informacijske sigurnosti. Ponovljeno testiranje informacijske sigurnosti ne mora se provesti na cijelom sustavu igara na sreću; umjesto toga, testiranje informacijske sigurnosti može biti usmjereno na nedostatke koji su uzrokovali odbijanje. U vezi s ponovljenim testiranjem sigurnosti podataka, inspeksijsko tijelo mora osigurati da su osjetljivosti koje su prethodno utvrđene kao razlozi za odbijanje ispravljene.

Provedba igara na sreću ne smije započeti prije nego što se provedu odobreni i valjani testovi sigurnosti.

7 Skeniranje osjetljivosti

Osim testiranja sigurnosti, nositelji dozvola obvezni su pratiti sigurnost vlastitih sustava redovitim skeniranjem osjetljivosti. Svrha pregleda osjetljivosti jest osigurati da sustavi igara na sreću koje upotrebljava nositelj dozvole nemaju vanjske sigurnosne osjetljivosti koje bi se mogle iskoristiti za izvođenje napada na sustave igara na sreću.

Nositelj dozvole dužan je provesti vanjsko skeniranje osjetljivosti jednom godišnje i o rezultatima obavijestiti nadzorno tijelo. Skeniranje osjetljivosti može provesti vanjsko inspeksijsko tijelo akreditirano u skladu s normama ISO/IEC 17025, ISO/IEC 17065 ili ISO/IEC 17020, kako je navedeno u stavku 2. ove Uredbe.

Nositelj dozvole dužan je ispraviti osjetljivosti otkrivene tijekom skeniranja ranjivosti ažuriranjem ili drugim hitnim mjerama ublažavanja ako nisu dostupna korektivna ažuriranja. Metoda procjene opisana u članku 6. primjenjuje se na sigurnosne osjetljivosti otkrivene tijekom skeniranja osjetljivosti. Ako izračunana vrijednost CVSS-a

utvrđene vanjske osjetljivosti prekoračuje 5,0, nositelj dozvole odmah poduzima mjere za otklanjanje osjetljivosti.

Inspekcijsko tijelo odgovorno za provođenje skeniranja osjetljivosti i njegovi zaposlenici moraju biti kompetentni i prikladni za provođenje ispitivanja. Potrebna osposobljenost za provođenje skeniranja osjetljivosti može se dokazati, među ostalim, prethodnim stručnim iskustvom u testiranju informacijske sigurnosti, iskustvom u upotrebi skenera osjetljivosti, osposobljavanjem ili općepriznatim certifikatima industrije. Nositelj dozvole dužan je osigurati da su osobe koje provode testiranje kvalificirane za provođenje skeniranja osjetljivosti i, na zahtjev, dokazivanje svojih kvalifikacija.

Mora se imenovati osoba odgovorna za provođenje skeniranja osjetljivosti kako bi se osiguralo da se ono provodi na odgovarajući način. Konačno izvješće o skeniranju osjetljivosti potpisuje i potvrđuje odgovorna osoba te se podnosi nadzornom tijelu.

8 Provjere osjetljivosti provedene u vezi s testiranjem informacijske sigurnosti

Nositelj dozvole može provesti skeniranje osjetljivosti kao dio testiranja informacijske sigurnosti. Isti se zahtjevi primjenjuju na skeniranje osjetljivosti koje se provodi u okviru testiranja informacijske sigurnosti kao i na druga skeniranja osjetljivosti.

9 Uklanjanje osjetljivosti

Nositelj dozvole dužan je redovito pratiti informacijsku sigurnost vlastitih sustava igara na sreću, čak i izvan ispitivanja informacijske sigurnosti, te ispraviti osjetljivosti koje ugrožavaju pouzdanost kad popravci ili druge metode ublažavanja postanu dostupni.

Ako osjetljivosti nije moguće odmah otkloniti, nositelj dozvole nastoji upotrijebiti dostupna sredstva za suzbijanje osjetljivosti i smanjenje učinka na najmanju moguću mjeru.

Ako je vrijednost osnovne ocjene CVSS v3 otkrivene vanjske osjetljivosti manja od 5,0, nositelj dozvole može iskoristiti svoje diskrecijsko pravo pri provedbi ispravaka i procjeni hitnosti potrebe za njima.

10 Uporaba izdanih potvrda

Akreditirano inspekcijsko tijelo koje je odobrilo nadzorno tijelo odgovorno za provođenje ispitivanja informacijske sigurnosti ili skeniranja osjetljivosti može upotrebljavati potvrde ili druge potvrde dodijeljene nositelju dozvole za softver za igre na sreću u okviru svojeg inspekcijskog pregleda. Ako inspekcijsko tijelo upotrebljava postojeće potvrde u okviru inspekcije, mora procijeniti mogu li se potvrde smatrati dovoljno pouzdanim dokazom pouzdanosti i informacijske sigurnosti sustava igara na sreću nositelja dozvole za softver za igre na sreću.

11 Neusklađenosti

Nositelj dozvole dužan je bez odgode prijaviti nadzornom tijelu svaku povredu informacijske sigurnosti ili zaštite podataka koju otkrije ako postoji razlog za sumnju da je pouzdanost sustava igara na sreću ili opreme za igre na sreću kojom se koristi nositelj dozvole ugrožena.

Nositelji dozvole nisu dužni prijaviti manje sigurnosne incidente ili incidente povezane sa zaštitom podataka nadzornom tijelu za igre na sreću ako je procijenjena učinkovitost incidenta ograničena po prirodi ili ako se ne procijeni da incident ima znatan utjecaj na pouzdanost sustava igara na sreću.

12 Stupanje na snagu

Ova Uredba stupa na snagu X [mjesec] 2026.

Nacionalni policijski odbor

Uprava za igre na sreću

Konepajankatu 2, PL 50, 11101 Riihimäki

Telefon +358 295 480 181, poliisi.fi