**Návrh nařízení**

# Spolehlivost a bezpečnost informací herních systémů podle zákona o hazardních hrách

## Obsah

Spolehlivost a bezpečnost informací herních systémů podle zákona o hazardních hrách....1
1 Právní rámec, oblast působnosti a definice....2
1.1 Pravomoc orgánu dohledu vydávat příkazy....2
1.2 Právní předpisy....2
1.3 Oblast působnosti....2
1.4 Základní pojmy....2
2 Akreditace kontrolního orgánu....3
3 Obecné postupy v oblasti bezpečnosti informací....3
4 Kontrolní orgán jako subjekt provádějící zkoušení informační bezpečnosti....3
4.1 Rozsah akreditace....4
5 Obnova zkoušení informační bezpečnosti....4
6 Zamítnuté zkoušení informační bezpečnosti....5
7 Skenování zranitelnosti....5
8 Skenování zranitelnosti prováděné v souvislosti se zkoušením informační bezpečnosti....6
9 Náprava zranitelností....6
10 Použití vydaných certifikátů....6
11 Odchylky....6
12 Vstup v platnost....7

# 1 Právní rámec, oblast působnosti a definice

## 1.1 Pravomoc orgánu dohledu vydávat příkazy

Pravomoc orgánu dohledu vydávat závazné předpisy vychází z ustanovení § 44 odst. 6 zákona o hazardních hrách (xx/2025). Podle výše uvedeného odstavce může orgán dohledu vydat podrobnější předpisy o spolehlivosti herních systémů, loterijního zařízení a loterijních metod používaných při provádění hazardních her a o technických požadavcích na zajištění náhodnosti losování, o podrobnější formě a obsahu šetření a schválení kontrolního orgánu a o podmínky, které musí kontrolní orgán splnit, aby mohl být schválen úřadem.

Podle § 57 zákona o hazardních hrách je orgánem dohledem Úřad pro udělování licencí a dohled. Podle § 106 zákona je příslušným orgánem ve smyslu § 57 do 31. prosince 2026 ředitelství státní policie.

## 1.2 Právní předpisy

Pro předmět tohoto nařízení jsou relevantní níže uvedené předpisy:

- Zákon o hazardních hrách (xx/2025)
- Zákon o správním řízení (434/2003)
- Zákon o ochraně osobních údajů (1050/2018)
- Obecné nařízení EU o ochraně osobních údajů (2016/679)

## 1.3 Oblast působnosti

Toto nařízení se vztahuje na právnickou osobu nebo fyzickou osobu uvedenou v kapitole 1 § 2 odst. 1 zákona o hazardních hrách, kterým byla udělena výlučná licence nebo licence k provozování hazardních her podle zákona o hazardních hrách.

Výhradní licence je upravena v § 5 zákona o hazardních hrách a licenci k provozování hazardních her upravuje § 6.

## 1.4 Základní pojmy

Pro účely tohoto nařízení se uplatňují tyto definice. Pro účely tohoto nařízení:

- *výhradní licencí* se rozumí licence udělená k provozování hazardních her ve formách uvedených v § 5 zákona o hazardních hrách
- *licencí k provozování hazardních her* se rozumí licence udělená pro druhy hazardních her uvedené v § 6 zákona o hazardních hrách
- *herní transakcí* se rozumí sázka podaná hráčem, výsledek zvolený hráčem, volby hráče, které mají vliv na výsledek hry, a předmět – a výsledky losování a veškeré

výhry a prohry zaznamenané v herním systému držitele výhradní licence nebo licence k provozování hazardních her

- *transakcí na herním účtu* se rozumí operace na herním účtu.
- *herním systémem* se rozumí elektronický informační systém používaný provozovatelem hazardních her nebo jeho jménem při provozování hazardních her

## 2 Akreditace kontrolního orgánu

Držitel licence je odpovědný za spolehlivost svého loterijního zařízení a herních systémů a za provádění auditů k zajištění spolehlivosti. Posouzení spolehlivosti a bezpečnosti provádí externí akreditovaný kontrolní orgán. Kontrolní orgán musí být akreditován v souladu s nařízením Evropského parlamentu a Rady (ES) č. 765/2008, kterým se stanoví požadavky na akreditaci a dozor nad trhem týkající se uvádění výrobků na trh a kterým se zrušuje nařízení (EHS) č. 339/93.

Akreditaci kontrolního orgánu může udělit národní akreditační orgán FINAS (Finská akreditační služba). Zahraniční akreditační orgán může rovněž působit jako akreditační orgán, pokud je členem Multilaterální dohody Evropské organizace pro spolupráci v oblasti akreditace (EA MLA) v příslušné oblasti působnosti. Držitel licence je povinen zajistit, aby externí strana provádějící audit měla platnou akreditaci.

## 3 Obecné postupy v oblasti bezpečnosti informací

Držitel licence je odpovědný za bezpečnost informací, ochranu údajů a další technické aspekty spolehlivosti svých herních systémů. Držitel licence musí ve své činnosti dodržovat osvědčené postupy v oblasti bezpečnosti informací a snažit se minimalizovat ohrožení bezpečnosti informací, porušení ochrany údajů a další problémy, které mohou ohrozit spolehlivost herních systémů. Držitel licence je rovněž povinen sledovat výše uvedené faktory mimo rámec pravidelných kontrol uvedených v tomto nařízení, aby zajistil spolehlivost svých systémů.

## 4 Kontrolní orgán jako subjekt provádějící zkoušení informační bezpečnosti

Držitel licence je povinen každé dva roky provádět zkoušení informační bezpečnosti svých herních systémů. Výsledky zkoušení informační bezpečnosti musí být předloženy orgánu dohledu. Zkoušení informační bezpečnosti a jeho výsledky nesmí být starší než 2 roky.

Zkoušení informační bezpečnosti provádí externí kontrolní orgán akreditovaný v souladu s normami ISO/IEC 17025, ISO/IEC 17065 nebo ISO/IEC 17020, jak je uvedeno v oddílu 2 tohoto nařízení. Při zkoušení bezpečnosti informací je třeba věnovat zvláštní pozornost ochraně a integritě komponent, které generují náhodnost v herním systému, ochraně komponent obsahujících osobní údaje a ochraně komponent souvisejících s platbami.

Kontrolní orgán odpovědný za provádění bezpečnostních zkoušek a jeho personál musí být kompetentní a vhodný pro provádění těchto zkoušek. Nezbytnou kvalifikaci pro provádění bezpečnostních zkoušek lze prokázat například předchozími pracovními zkušenostmi v oblasti bezpečnostních zkoušek, školením nebo obecně uznávanými odvětvovými certifikáty. Držitel licence je povinen zajistit, aby osoby provádějící testování byly kompetentní k provádění zkoušení informační bezpečnosti a na požádání prokázaly svou kompetenci.

Musí být jmenována osoba odpovědná za provádění zkoušek informační bezpečnosti, aby bylo zajištěno jejich řádné provedení. Pověřená osoba musí podepsat a potvrdit závěrečnou zprávu o zkoušení bezpečnosti, která musí být předložena orgánu dohledu.

Zkoušení bezpečnosti musí zahrnovat alespoň následující komponenty a související zranitelnosti nebo anomálie:

- Možnost manipulace s náhodnými komponenty
- Přístup k databázi zákazníků
- Schopnost ovlivnit výsledek her
- Schopnost ovlivnit platební systémy nebo platební transakce
- Neoprávněný přístup k serverům používaným k ukládání herních transakcí a transakcí na herním účtu
- Možnost úpravy archivovaných údajů o herních transakcích nebo transakcích na herním účtu
- Úprava nebo zničení protokolů souvisejících s herními systémy

### 4.1 Rozsah akreditace

Akreditovaný kontrolní orgán provádějící audit musí mít v rámci své akreditace ISO/IEC rozsah akreditace pro hazardní hry. Oblast působnosti musí zahrnovat požadavky stanovené finskými právními předpisy v oblasti hazardních her a technickými předpisy orgánu dohledu.

Do 1. ledna 2027 může orgán dohledu akceptovat akreditaci, která zahrnuje rozsah posouzený a udělený na základě technických předpisů vydaných pro dánské nebo švédské systémy hazardních her.

## 5 Obnova zkoušení informační bezpečnosti

Držitel licence musí předložit výsledky schváleného testování informační bezpečnosti orgánu dohledu. Držitel licence nesmí zahájit provoz hazardních her před úspěšným dokončením zkoušení informační bezpečnosti. Výsledky zkoušení informační bezpečnosti nesmí být starší než 2 roky.

Orgán dohledu může podle svého uvážení poskytnout dodatečný čas na provedení zkoušení zabezpečení, během něhož může provoz hazardních her nadále pokračovat.

## 6 Zamítnuté zkoušení informační bezpečnosti

Kontrolní orgán provádějící bezpečnostní testování musí posoudit zranitelnosti zjištěné během zkoušení informační bezpečnosti a jejich význam pro spolehlivost herního systému. Zranitelnosti zjištěné během posouzení musí být vyhodnoceny pomocí kalkulátoru CVSS v3 („Common Vulnerability Scoring System Calculator version 3“) poskytovaného NIST („National Institute of Technology“). S ohledem na kalkulátor CVSS v3 musí být závažnost zranitelnosti posouzena pomocí metrik základního skóre. Pokud jsou během zkoušení zabezpečení zjištěny zranitelnosti s vypočtenou hodnotou CVSS vyšší než 5,0, nelze audit považovat za úspěšný.

Pokud zkoušení informační bezpečnosti držitele licence není schváleno, musí držitel licence okamžitě přijmout opatření k nápravě zjištěných bezpečnostních zranitelností. Držitel licence musí neúspěšné zkoušení informační bezpečnosti nahlásit orgánu dohledu.

Držitel licence musí do 90 dnů od neúspěšného zkoušení informační bezpečnosti provést nové zkoušení informační bezpečnosti. Obnovené zkoušení informační bezpečnosti nemusí být provedeno na celém herním systému; místo toho může být zaměřen na nedostatky, které vedly k neúspěchu. V souvislosti s opakovaným zkoušením informační bezpečnosti musí kontrolní orgán zajistit, aby byly odstraněny slabiny, které byly dříve identifikovány jako důvod zamítnutí.

Provozování hazardních her nesmí být zahájeno před schválením a platností zkoušení informační bezpečnosti.

## 7 Skenování zranitelnosti

Kromě zkoušení zabezpečení jsou držitelé licencí povinni monitorovat bezpečnost svých vlastních systémů prostřednictvím pravidelného skenování zranitelnosti. Účelem skenování zranitelnosti je zajistit, aby herní systémy používané držitelem licence neměly žádné vnější zranitelnosti informační bezpečnosti, které by mohly být zneužity k provedení útoků na herní systémy.

Držitelé licence jsou povinni provádět externí skenování zranitelnosti jednou ročně a výsledky hlásit orgánu dohledu. Skenování zranitelnosti může provádět externí kontrolní orgán akreditovaný v souladu s normami ISO/IEC 17025, ISO/IEC 17065 nebo ISO/IEC 17020, jak je uvedeno v oddílu 2 tohoto nařízení.

Držitel licence je povinen odstranit veškeré zranitelnosti zjištěné při skenování zranitelnosti pomocí aktualizací nebo jiných naléhavých opatření ke zmírnění rizika, pokud nejsou k dispozici opravné aktualizace. Na bezpečnostní zranitelnosti zjištěné během skenování zranitelností se použije metoda hodnocení popsaná v oddílu 6. Pokud

vypočtená hodnota CVSS identifikované externí zranitelnosti přesáhne 5,0, držitel licence přijme okamžitá opatření k nápravě těchto zranitelností.

Kontrolní orgán odpovědný za provádění skenování zranitelnosti a jeho personál musí být kompetentní a vhodný pro provádění zkoušení. Potřebnou způsobilost k provádění skenování zranitelností lze prokázat například předchozími pracovními zkušenostmi v oblasti zkoušení informační bezpečnosti, zkušenostmi s používáním skenerů zranitelností, školením nebo obecně uznávanými odvětvovými certifikáty. Držitel licence je povinen zajistit, aby osoby provádějící zkoušení byly způsobilé k provádění skenování zranitelností a aby na požádání prokázaly svou kvalifikaci.

Musí být jmenována osoba odpovědná za řádné provedení skenování zranitelnosti. Odpovědná osoba musí podepsat a potvrdit závěrečnou zprávu o skenování zranitelnosti, která musí být předložena orgánu dohledu.

## 8 Skenování zranitelnosti prováděné v souvislosti se zkoušením informační bezpečnosti

Držitel licence může provádět skenování zranitelnosti v rámci zkoušení informační bezpečnosti. Skenování zranitelnosti prováděné v souvislosti se zkoušení informační bezpečnosti podléhá stejným požadavkům jako ostatní skenování zranitelnosti.

## 9 Náprava zranitelností

Držitel licence je povinen pravidelně sledovat informační bezpečnost svých herních systémů, a to i mimo zkoušení informační bezpečnosti, a opravovat zranitelnosti, které ohrožují spolehlivost, jakmile jsou k dispozici opravy nebo jiné metody zmírnění rizik.

Pokud není možné zranitelnosti rychle opravit, musí se držitel licence snažit využít dostupné prostředky k prevenci zranitelností a minimalizaci jejich dopadu.

Pokud je hodnota CVSS v3 Base Score zjištěné externí zranitelnosti nižší než 5,0, může držitel licence podle vlastního uvážení provést opravy a posoudit naléhavost jejich nutnosti.

## 10 Použití vydaných certifikátů

Akreditovaný kontrolní orgán schválený orgánem dohledu odpovědným za provádění zkoušení bezpečnosti informací nebo skenování zranitelnosti může v rámci své kontroly používat certifikáty nebo jiná osvědčení udělená držiteli licence k softwaru pro hazardní hry. Pokud kontrolní orgán v rámci kontroly využívá stávající certifikáty, musí posoudit, zda lze tyto certifikáty považovat za dostatečně spolehlivý důkaz spolehlivosti a informační bezpečnosti herního systému držitele licence na herní software.

## 11 Odchylky

Držitel licence je povinen neprodleně oznámit orgánu dohledu veškeré zjištěné odchylky v oblasti bezpečnosti informací nebo ochrany údajů, pokud existuje důvodné podezření, že byla narušena spolehlivost herních systémů nebo loterijního zařízení používaného držitelem licence.

Držitelé licence nejsou povinni hlásit orgánu dohledu drobné odchylky týkající se informační bezpečnosti nebo ochrany údajů, pokud je odhadovaný dopad odchylky malý nebo pokud se nemá za to, že odchylka má významný dopad na spolehlivost herních systémů.

## 12 Vstup v platnost

Toto nařízení vstupuje v platnost dnem X. [měsíc] 2026.

**Ředitelství státní police**
**Správa hazardních her**
Konepajankatu 2, PL 50, 11101 Riihimäki
Telefonní číslo +358 295 480 181, poliisi.fi