Rendelettervezet

A szerencsejáték-rendszerek megbízhatósága és információbiztonsága a szerencsejátékokról szóló törvény szerint

Tartalom

1 Jogi keret, hatály és fogalommeghatározások

1.1 A felügyeleti hatóság rendeletek kiadására vonatkozó hatásköre

A felügyeleti hatóságnak a kötelező érvényű rendeletek kiadására vonatkozó joga a szerencsejátékokról szóló törvény (xx/2025) 44. §-ának (6) bekezdésén alapul. Az említett bekezdés szerint a felügyeleti hatóság részletesebb szabályozásokat adhat ki a szerencsejátékok működtetéséhez alkalmazott szerencsejáték-rendszerek, sorsoló berendezések és sorsolási módszerek megbízhatóságáról, a sorsolás véletlenszerűségének biztosítására vonatkozó technikai követelményekről, az ellenőrző szervezet általi vizsgálat és jóváhagyás részletesebb formájáról és tartalmáról, valamint azokról a feltételekről, amelyeket az ellenőrző szervnek teljesítenie kell ahhoz, hogy a Hatóság jóváhagyja.

A szerencsejátékokról szóló törvény 57. §-a szerint a felügyeleti hatóság a Finn Felügyeleti Hatóság. A törvény 106. §-a szerint 2026. december 31-ig az 57. § szerinti illetékes hatóságként a Nemzeti Rendőrségi Hivatal jár el.

1.2 Jogalkotás

E rendelet tárgya szempontjából a következő rendeletek bírnak jelentőséggel:

- A szerencsejátékokról szóló törvény (xx/2025)
- A közigazgatási eljárásról szóló törvény (434/2003)
- Adatvédelmi törvény (1050/2018)
- Az EU általános adatvédelmi rendelete (2016/679)

1.3 Alkalmazási kör

Ez a rendelkezés a szerencsejátékokról szóló törvény 1. fejezetének 2. §-a (1) bekezdésében említett olyan jogi vagy természetes személyekre vonatkozik, akik a szerencsejáték-törvény alapján kizárólagos engedélyt vagy szerencsejáték-tevékenységekre vonatkozó engedélyt kaptak.

A kizárólagos engedélyre a szerencsejátékokról szóló törvény 5. §-a, a szerencsejáték-engedélyre pedig a 6. § az irányadó.

1.4 Fogalommeghatározások

E rendelkezés alkalmazásában: E rendelet alkalmazásában:

- *kizárólagos engedély:* a szerencsejátékokról szóló törvény 5. §-ában említett szerencsejáték-típusokra kiadott engedély.
- *szerencsejáték-engedély:* a szerencsejáték-törvény 6. §-ában meghatározott szerencsejáték-típusokra kiadott engedély.

- *szerencsejáték-tranzakció:* a játékos által a játék során megtett tét, a játékos által választott kimeneteli lehetőség, a játékos által hozott, a játék kimenetele szempontjából lényeges döntések, a piacok és a sorsolások eredményei, valamint a kizárólagos engedély vagy szerencsejáték-engedély jogosultjának szerencsejáték-rendszerében rögzített nyeremények és veszteségek
- *játékosszámla-tranzakció:* számlabejegyzés
- *szerencsejáték-rendszer:* a szerencsejáték-működtető által vagy nevében a szerencsejáték működtetéséhez használt online információs rendszer

2 Ellenőrző szervezet akkreditálása

Az engedélyes felelős saját szerencsejáték-eszközeinek és szerencsejáték-rendszereinek megbízhatóságáért, valamint a megbízhatóságot biztosító ellenőrzések elvégzéséért. A megbízhatóság és a biztonság értékelését egy külső akkreditált ellenőrző szervezet végzi. Az ellenőrző szervezetet a termékek forgalmazása tekintetében az akkreditálás és piacfelügyelet előírásainak megállapításáról és a 339/93/EGK rendelet hatályon kívül helyezéséről szóló 765/2008/EK európai parlamenti és tanácsi rendeletnek megfelelően kell akkreditálni.

Az akkreditációt a nemzeti akkreditáló testület, a FINAS (Finn Akkreditációs Szolgálat) adhatja meg az ellenőrző szervezeteknek. Akkreditáló testületként külföldi akkreditáló testület is eljárhat, ha az Európai Akkreditálási Szervezet többoldalú elismerési megállapodásának (EA MLA) részese a megfelelő hatásköri területen. Az engedélyes köteles meggyőződni arról, hogy az ellenőrzést végző külső szervezet érvényes akkreditációval rendelkezik.

3 Általános információbiztonsági gyakorlatok

Az engedélyes felel saját szerencsejáték-rendszereinek információbiztonságáért, adatvédeleméért és egyéb technikai megbízhatósági jellemzőiért. Az engedélyesnek bevált információbiztonsági gyakorlatokat kell követnie a működése során, és törekednie kell az információbiztonsági fenyegetések, az adatsértések és más, a szerencsejáték-rendszerek megbízhatóságát veszélyeztető problémák minimalizálására. Az engedélyes az e rendeletben említett rendszeres ellenőrzéseken kívül is köteles figyelemmel kísérni a fent említett tényezőket rendszerei megbízhatóságának biztosítása érdekében.

4 Információbiztonsági vizsgálatot végző ellenőrző szervezet

Az engedélyes köteles kétévente biztonsági vizsgálatot végrehajtani saját szerencsejáték-rendszerein. Az információbiztonsági vizsgálat eredményét be kell nyújtani a felügyeleti hatóságnak. Az információbiztonsági vizsgálat és annak eredménye nem lehet két évnél régebbi.

Az információbiztonsági vizsgálatot az ISO/IEC 17025, ISO/IEC 17065 vagy ISO/IEC 17020 szerint akkreditált külső ellenőrző szervezetnek kell elvégeznie az e rendelet 2. szakaszában leírtaknak megfelelően. Az információbiztonsági vizsgálat során különös figyelmet kell fordítani a szerencsejáték-rendszer véletlenszerű komponenseinek védelmére és sértetlenégére, a személyes adatokat tartalmazó komponensek védelmére, valamint a fizetéssel kapcsolatos komponensek védelmére.

Az információbiztonsági vizsgálatok végrehajtásáért felelős ellenőrző szervezetnek és személyzetének kompetensnek és alkalmasnak kell lennie a vizsgálat elvégzésére. Az információbiztonsági vizsgálat elvégzéséhez szükséges kompetenciát többek között az információbiztonsági vizsgálatok terén szerzett korábbi szakmai tapasztalat, képzés vagy általánosan elismert ágazati tanúsítványok igazolhatják. Az engedélyes köteles gondoskodni arról, hogy a vizsgálatot végző személyek rendelkezzenek az információbiztonsági vizsgálat elvégzéséhez szükséges képesítéssel, és ezt kérésre igazolni tudják.

A biztonsági vizsgálat végrehajtására ki kell jelölni egy megfelelő személyt, aki felelős a szabályszerű végrehajtásért. A végleges információbiztonsági vizsgálati jelentést a kijelölt személynek alá kell írnia és jóvá kell hagynia, majd be kell nyújtania a felügyeleti hatóságnak.

Az információbiztonsági vizsgálat keretében legalább a következő komponenseket, valamint a kapcsolódó sebezhetőségeket és biztonsági eseményeket kell tesztelni:

- Véletlenszerű komponensek manipulálásának lehetősége
- Hozzáférés az ügyféladatbázishoz
- A játék kimenetelének befolyásolására való képesség
- A fizetési rendszerek vagy fizetési tranzakciók befolyásolására való képesség
- Jogosulatlan hozzáférés a szerencsejáték-tranzakciók és játékosszámla-tranzakciók tárolására szolgáló szerverekhez
- Az archivált szerencsejáték-események vagy a szerencsejáték-számlák eseményadatainak szerkesztésére való képesség
- Szerencsejáték-rendszerekkel kapcsolatos naplófájlok módosítása vagy megsemmisítése

4.1 Illetékességi terület

Az auditot végző akkreditált ellenőrző szervezetnek az ISO/IEC akkreditációja alapján rendelkeznie kell a szerencsejátékokra vonatkozó illetékességgel. Az illetékességnek ki kell terjednie a szerencsejátékokra vonatkozó finn jogszabályokban és a felügyeleti hatóság technikai szabályzataiban meghatározott követelményekre.

2027. január 1-jéig a felügyeleti hatóság elfogadhat olyan akkreditációt, amely a dán vagy svéd szerencsejáték-rendszerekre kiadott technikai szabályok alapján értékelt és biztosított hatáskört tartalmaz.

5 Az információbiztonsági vizsgálat megújítása

Az engedélyes a jóváhagyott információbiztonsági vizsgálat eredményeit benyújtja a felügyeleti hatóságnak. Az engedélyes a biztonsági vizsgálat sikeres teljesítéséig nem kezdheti meg a szerencsejáték működtetését. Az információbiztonsági vizsgálat eredménye nem lehet két évnél régebbi.

A felügyeleti hatóság saját belátása szerint további időt biztosíthat a biztonsági vizsgálat végrehajtására, amelynek során a szerencsejáték működtetése folytatható.

6 Elutasított információbiztonsági vizsgálat

Az információbiztonsági vizsgálatot végző ellenőrző szervezetnek értékelnie kell az információbiztonsági vizsgálat során azonosított sebezhetőségeket, valamint azok jelentőségét a szerencsejáték-rendszer megbízhatósága szempontjából. Az értékelés során azonosított sebezhetőségeket a Nemzeti Technológiai Intézet (NIST) által rendelkezésre bocsátott CVSS v3 (Common Vulnerability Scoring System Calculator version 3) kalkulátor segítségével kell értékelni. A CVSS v3 kalkulátor esetében a sebezhetőség súlyosságát pontszámítási alapmutatók segítségével kell értékelni. Ha a biztonsági vizsgálat során 5,0-nál magasabb számított CVSS-értékkel rendelkező sebezhetőségeket észlelnek, a teszt nem tekinthető sikeresnek.

Ha az engedélyes információbiztonsági vizsgálata nem kerül jóváhagyásra, az engedélyesnek haladéktalanul intézkednie kell az azonosított információbiztonsági sebezhetőségek elhárítására. Az engedélyesnek be kell jelentenie az elutasított információbiztonsági vizsgálatot a felügyeleti hatóságnak.

Az engedélyesnek az elutasított információbiztonsági vizsgálattól számított 90 napon belül új biztonsági vizsgálatot kell végeznie. A megújított információbiztonsági vizsgálatot nem kell elvégezni a teljes szerencsejáték-rendszeren, hanem az információbiztonsági vizsgálat az elutasítást eredményező hiányosságokra irányulhat. A megújított információbiztonsági vizsgálattal összefüggésben az ellenőrző szervezetnek meg kell győződnie arról, hogy a korábban elutasítási okként azonosított sebezhetőségeket megszüntették.

A szerencsejátékok működtetése nem kezdődhet meg a végrehajtott biztonsági vizsgálat jóváhagyása és érvényessé válása előtt.

7 Sebezhetőségi vizsgálat

A biztonsági vizsgálat mellett az engedélyesek kötelesek rendszeres sebezhetőségi vizsgálatokkal is ellenőrizni saját rendszereik biztonságát. A sebezhetőségi vizsgálatok célja annak ellenőrzése, hogy az engedélyes által használt szerencsejáték-rendszerekben nem állnak-e fenn olyan külső biztonsági sebezhetőségek, amelyek révén támadások hajthatók végre a szerencsejáték-rendszerek ellen.

Az engedély jogosultja köteles évente egyszer külső sebezhetőségi vizsgálatot végezni és annak eredményeit a felügyeleti hatóságnak bejelenteni. A sebezhetőségi vizsgálatot az ISO/IEC 17025, ISO/IEC 17065 vagy ISO/IEC 17020 szerint akkreditált külső ellenőrző szervezetnek kell elvégeznie az e rendelet 2. pontjában leírtaknak megfelelően.

Az engedélyes köteles a sebezhetőségi vizsgálat során feltárt sebezhetőségeket frissítésekkel vagy más sürgős kockázatcsökkentő intézkedésekkel orvosolni, ha korrekciós frissítések nem állnak rendelkezésre. A sebezhetőségi vizsgálatok során észlelt biztonsági sebezhetőségekre a 6. szakaszban leírt értékelési módszert kell alkalmazni. Ha az azonosított külső sebezhetőség számított CVSS-értéke meghaladja az 5,0-t, az engedélyesnek haladéktalanul intézkednie kell a sebezhetőségek megszüntetése érdekében.

A sebezhetőségi vizsgálat végrehajtásáért felelős ellenőrző szervezetnek és személyzetének kompetensnek és alkalmasnak kell lennie a vizsgálatok elvégzésére. A sebezhetőségi vizsgálatok elvégzéséhez szükséges kompetenciát többek között az információbiztonsági vizsgálatok terén szerzett korábbi szakmai tapasztalat, a sebezhetőségi vizsgálóeszközök használata terén szerzett tapasztalat, képzés vagy általánosan elismert ágazati tanúsítványok igazolhatják. Az engedélyes köteles gondoskodni arról, hogy a vizsgálatot végző személyek rendelkezzenek a sebezhetőségi vizsgálat elvégzéséhez szükséges képesítéssel, és ezt kérésre igazolni tudják.

A sebezhetőségi vizsgálat megfelelő elvégzése érdekében ki kell jelölni egy annak végrehajtásáért felelős személyt. A végleges sebezhetőségi vizsgálati jelentést a felelős személynek alá kell írnia és jóvá kell hagynia, majd be kell nyújtania a felügyeleti hatóságnak.

8 Információbiztonsági vizsgálat keretében végzett sebezhetőségi vizsgálat

Az engedélyes a sebezhetőségi vizsgálatot az információbiztonsági vizsgálat részeként is elvégezheti. Az információbiztonsági tesztelés részeként végzett sebezhetőségi vizsgálatokra ugyanazok a követelmények vonatkoznak, mint más sebezhetőségi vizsgálatokra.

9 A sebezhetőségek orvoslása

Az engedélyes köteles az információbiztonsági vizsgálatokon kívül is rendszeresen ellenőrizni saját szerencsejáték-rendszereinek információbiztonságát és orvosolni a megbízhatóságot veszélyeztető sebezhetőségeket, ha javítások vagy más kockázatcsökkentő módszerek állnak rendelkezésre.

Ha a sebezhetőségek nem orvosolhatók azonnal, az engedélyesnek törekednie kell arra, hogy a rendelkezésre álló eszközökkel küzdjön a sebezhetőségek ellen és minimalizálja azok hatását.

Ha az észlelt külső sebezhetőség CVSS v3 alappontszáma 5,0-nál kisebb, az engedélyes saját belátása szerint korrekciókat hajthat végre és értékelheti azok végrehajtásának sürgősségét.

10 A kiadott tanúsítványok felhasználása

Az információbiztonsági vizsgálat vagy a sebezhetőségi vizsgálat végrehajtásáért felelős felügyeleti hatóság által jóváhagyott akkreditált ellenőrző szervezet az ellenőrzés során felhasználhatja a szerencsejáték-szoftver engedélyese részére kiadott tanúsítványokat vagy egyéb igazolásokat. Ha az ellenőrző szervezet az ellenőrzés során meglévő tanúsítványokat használ fel, meg kell vizsgálnia, hogy a tanúsítványok kellően megbízható bizonyítéknak tekinthetők-e a szerencsejáték-szoftver engedélyese által működtetett szerencsejáték-rendszer megbízhatóságára és információbiztonságára vonatkozóan.

11 Eltérések

Az engedélyes köteles haladéktalanul bejelenteni a felügyeleti hatóságnak minden általa észlelt információbiztonsági és adatvédelmi jogsértést, ha okkal feltételezhető, hogy az engedélyes által használt szerencsejáték-rendszerek vagy sorsoló berendezések megbízhatósága veszélybe került.

Az engedélyesek nem kötelesek bejelenteni a kisebb biztonsági vagy adatvédelmi eseményeket a szerencsejáték-felügyeleti hatóságnak, ha az esemény becsült hatása korlátozott, vagy ha értékelésük szerint az esemény nem gyakorol jelentős hatást a szerencsejáték-rendszerek megbízhatóságára.

12 Hatálybalépés

Ez a rendelet 2026. [hónap] X napján lép hatályba.

Nemzeti Rendőrségi Hivatal
Szerencsejáték Hatóság
Konepajankatu 2, PL 50, 11101 Riihimäki
Telefon +358 295 480 181, poliisi.fi