Reglamento projektas

Lošimų sistemų patikimumas ir informacijos saugumas pagal Lošimų įstatymą

Turinys

1 Teisinis pagrindas, taikymo sritis ir apibrėžtys

1.1 Priežiūros institucijos įgaliojimas priimti įsakymus

Priežiūros institucijos teisė priimti privalomą įsakymą grindžiama Lošimų įstatymo (xx/2025) 44 straipsnio 6 dalimi. Pagal minėtą dalį priežiūros institucija gali priimti išsamesnes taisykles dėl vykdant lošimų veiklą naudojamų lošimų sistemų, loterijos įrenginių ir loterijos metodų patikimumo, dėl techninių reikalavimų, susijusių su loterijų atsitiktinumo užtikrinimu, dėl tikrinimo įstaigos tyrimo ir patvirtinimo išsamesnės formos ir turinio, taip pat dėl sąlygų, kurias turi atitikti tikrinimo įstaiga, kad gautų institucijos patvirtinimą.

Pagal Lošimų įstatymo 57 straipsnį priežiūros institucija yra Suomijos priežiūros institucija. Pagal įstatymo 106 straipsnį Nacionalinė policijos valdyba iki 2026 m. gruodžio 31 d. veikia kaip 57 straipsnyje nurodyta kompetentinga institucija.

1.2 Teisės aktai

Su šio reglamento dalyku susijusios šios taisyklės:

- Lošimų įstatymas (xx/2025);
- Administracinės procedūros įstatymas (434/2003);
- Duomenų apsaugos įstatymas (1050/2018);
- ES Bendrasis duomenų apsaugos reglamentas (2016/679).

1.3 Taikymo sritis

Ši nuostata taikoma Lošimų įstatymo 1 skyriaus 2 straipsnio 1 dalyje nurodytam juridiniam arba fiziniam asmeniui, kuriam pagal Lošimų įstatymą suteikta išimtinė licencija arba licencija vykdyti lošimų veiklą.

Išimtinė licencija reglamentuojama Lošimų įstatymo 5 straipsniu, o lošimų licenciją – 6 straipsniu.

1.4 Apibrėžtys

Šiame reglamente vartojamos toliau nurodytų sąvokų apibrėžtys. Šiame reglamente:

- *išimtinė licencija* – licencija, suteikta Lošimų įstatymo 5 straipsnyje nurodytoms lošimų formoms;
- *lošimų licencija* – Lošimų įstatymo 6 straipsnyje nurodytų rūšių lošimams išduota licencija;
- *lošimo operacija* – tai lošėjo statymas lošime, lošėjo pasirinktas rezultato variantas, lošėjo pasirinkimai, kurie yra svarbūs lošimo rezultatui bei lažybų ir

loterijų rezultatams, taip pat bet kokie laimėjimai ir pralaimėjimai, užregistruoti išimtinės licencijos arba lošimų licencijos savininko lošimo sistemoje;

- *lošėjo paskyros operacija* – paskyros įrašai;
- *lošimų sistema* – internetinė informacinė sistema, kurią lošimų organizatorius naudoja lošimams vykdyti arba kuri naudojama jo vardu.

2 Tikrinimo įstaigos akreditavimas

Licencijos savininkas yra atsakingas už savo loterijos prietaisų ir lošimų sistemų patikimumą, taip pat už auditų, atliekamų siekiant užtikrinti šį patikimumą, atlikimą. Patikimumo ir saugumo vertinimą atlieka išorės akredituota tikrinimo įstaiga. Tikrinimo įstaiga akredituojama pagal Europos Parlamento ir Tarybos reglamentą (EB) Nr. 765/2008, nustatantį su gaminių prekyba susijusius akreditavimo ir rinkos priežiūros reikalavimus ir panaikinantį Reglamentą (EEB) Nr. 339/93.

Akreditaciją tikrinimo įstaigoms gali suteikti nacionalinė akreditacijos įstaiga FINAS (Suomijos akreditacijos tarnyba). Užsienio akreditavimo įstaiga taip pat gali veikti kaip akreditacijos įstaiga, jei ji yra Europos akreditavimo organizacijos daugiašalio pripažinimo susitarimo (EA MLA) narė atitinkamoje kompetencijos srityje. Licencijos savininkas privalo užtikrinti, kad auditą atliekantis išorės subjektas turėtų galiojančią akreditaciją.

3 Bendrosios informacijos saugumo praktikos

Licencijos savininkas yra atsakingas už savo lošimų sistemų informacijos saugumą, duomenų apsaugą ir kitas techninio patikimumo savybes. Licencijos savininkas, vykdydamas savo veiklą, privalo laikytis gerosios informacijos saugumo praktikos ir stengtis kuo labiau sumažinti informacijos saugumo grėsmes, duomenų saugumo pažeidimus ir kitas problemas, kurios gali kelti pavojų lošimų sistemų patikimumui. Licencijos savininkas taip pat privalo stebėti pirmiau minėtus veiksnius ne tik atlikdamas šiame reglamente nurodytus reguliarius patikrinimus, kad užtikrintų savo sistemų patikimumą.

4 Informacijos saugumo bandymus atliekanti tikrinimo įstaiga

Licencijos savininkas privalo kas dvejus metus atlikti savo lošimų sistemų saugumo bandymus. Informacijos saugumo bandymų rezultatai pateikiami priežiūros institucijai. Informacijos saugumo bandymai ir jų rezultatai negali būti senesni nei dvejų metų.

Informacijos saugumo bandymus atlieka pagal ISO/IEC 17025, ISO/IEC 17065 arba ISO/IEC 17020 akredituota išorės tikrinimo įstaiga, kaip nurodyta šio reglamento 2 straipsnyje. Atliekant informacijos saugumo bandymus ypatingas dėmesys skiriamas atsitiktinių lošimų sistemos komponentų apsaugai ir vientisumui, komponentų, kuriuose yra asmens duomenų, apsaugai ir su mokėjimais susijusių komponentų apsaugai.

Už informacijos saugumo bandymų atlikimą atsakinga tikrinimo įstaiga ir jos personalas turi būti kompetentingi ir kvalifikuoti atlikti bandymus. Reikiamą kompetenciją atlikti informacijos saugumo bandymus galima įrodyti, be kita ko, ankstesne profesine patirtimi informacijos saugumo bandymų srityje, mokymais arba visuotinai pripažintais pramonės sertifikatais. Licencijos savininkas privalo užtikrinti, kad bandymus atliekantys asmenys būtų kvalifikuoti atlikti informacijos saugumo bandymus ir, paprašyti, įrodyti jų kvalifikaciją.

Saugumo bandymus turi atlikti paskirtas asmuo, kuris bus atsakingas už tinkamą įgyvendinimą. Galutinę informacijos saugumo bandymo ataskaitą pasirašo ir patvirtina paskirtas asmuo ir pateikia ją priežiūros institucijai.

Atliekant informacijos saugumo bandymus turi būti vykdomi bent šių komponentų bei susijusių pažeidžiamumų ar incidentų bandymai:

- atsitiktinių komponentų manipuliavimo galimybės;
- prieigos prie klientų duomenų bazės;
- gebėjimo daryti įtaką lošimų rezultatams;
- gebėjimo daryti įtaką mokėjimo sistemoms arba mokėjimo operacijoms;
- neteisėtos prieigos prie serverių, naudojamų lošimų operacijoms ir lošėjų paskyrų operacijoms saugoti;
- gebėjimo redaguoti archyvuotus lošimo įvykio ar lošimo paskyros įvykio duomenis;
- su lošimo sistemomis susijusių žurnalų pakeitimo ar sunaikinimo.

4.1 Kompetencijos sritis

Auditą atliekančios akredituotos tikrinimo įstaigos ISO/IEC akreditacijoje turi būti nurodyta lošimų kompetencijos sritis. Kompetencijos sritis turi apimti reikalavimus, nustatytus Suomijos lošimų teisės aktuose ir priežiūros institucijos techniniuose reglamentuose.

Iki 2027 m. sausio 1 d. priežiūros institucija gali priimti akreditaciją, kuri apima kompetencijos sritį, įvertintą ir suteiktą remiantis Danijos arba Švedijos lošimų sistemoms priimtais techniniais reglamentais.

5 Informacijos saugumo bandymų pratęsimas

Licencijos savininkas priežiūros institucijai pateikia patvirtintų informacijos saugumo bandymų rezultatus. Licencijos savininkas negali pradėti organizuoti lošimų, kol nėra sėkmingai baigęs saugumo bandymų. Informacijos saugumo bandymo rezultatas turi būti ne senesnis kaip dvejų metų.

Priežiūros institucija gali savo nuožiūra skirti papildomo laiko saugumo bandymams atlikti, per kurį galima tęsti lošimų veiklą.

6 Atmestas informacijos saugumo bandymas

Informacijos saugumo bandymą atliekanti tikrinimo įstaiga turėtų įvertinti informacijos saugumo bandymų metu nustatytus pažeidžiamumus ir jų svarbą lošimų sistemos patikimumui. Vertinimo metu nustatyti pažeidžiamumai turėtų būti vertinami naudojant NIST (National Institute of Technology) pateiktą CVSS v3 (Common Vulnerability Scoring System Calculator version 3) skaičiuoklę. CVSS v3 skaičiuoklėje pažeidžiamumo sunkumas vertinamas naudojant „Base Score Metrics“ (bazinius balų rodiklius). Jei saugumo bandymo metu nustatomi pažeidžiamumai, kurių apskaičiuota CVSS vertė didesnė nei 5,0, bandymas negali būti laikomas sėkmingu.

Jei licencijos savininko informacijos saugumo bandymas nepatvirtinamas, licencijos savininkas turi nedelsdamas imtis priemonių, kad pašalintų nustatytas informacijos saugumo pažeidžiamumus. Apie atmestą informacijos saugumo bandymą licencijos savininkas praneša priežiūros institucijai.

Licencijos savininkas per 90 dienų nuo atmesto informacijos saugumo bandymo turi atlikti naują saugumo bandymą. Pakartotinis informacijos saugumo bandymas nebūtinai turi būti atliekamas dėl visos lošimų sistemos; vietoj to, informacijos saugumo bandymai gali būti nukreipti į trūkumus, dėl kurių bandymas buvo atmestas. Pakartotinių informacijos saugumo bandymų atžvilgiu tikrinimo įstaiga turi užtikrinti, kad pažeidžiamumai, kurie anksčiau buvo nustatyti kaip atmetimo pagrindas, būtų ištaisyti.

Azartinių lošimų įgyvendinimas negali būti pradėtas, kol nebus atlikti patvirtinti ir galiojantys saugumo bandymai.

7 Pažeidžiamumų skenavimas

Licencijos savininkai privalo ne tik atlikti saugumo bandymus, bet ir stebėti savo sistemų saugumą reguliariai atlikdami pažeidžiamumų skenavimus. Pažeidžiamumų skenavimo tikslas – užtikrinti, kad licencijos savininko naudojamose lošimų sistemose nebūtų jokių išorinių saugumo pažeidžiamumų, kuriais būtų galima pasinaudoti vykdant atakas prieš lošimų sistemas.

Licencijos savininkas privalo kartą per metus atlikti išorės pažeidžiamumų skenavimą ir apie jo rezultatus pranešti priežiūros institucijai. Pažeidžiamumų skenavimą gali atlikti išorės tikrinimo įstaiga, akredituota pagal ISO/IEC 17025, ISO/IEC 17065 arba ISO/IEC 17020, kaip nurodyta šio reglamento 2 straipsnyje.

Licencijos savininkas privalo pašalinti pažeidžiamumą, nustatytą atliekant pažeidžiamumų skenavimą, įdiegdamas naujinius arba kitomis skubios rizikos mažinimo priemonėmis, jei korekciniai naujiniai nėra prieinami. 6 straipsnyje aprašytas vertinimo metodas taikomas saugumo pažeidžiamumams, nustatytiems atliekant pažeidžiamumų skenavimą. Jei apskaičiuota nustatyto išorės pažeidžiamumo CVSS vertė viršija 5,0, licencijos savininkas nedelsdamas imasi veiksmų pažeidžiamumui pašalinti.

Už pažeidžiamumų skenavimą atsakinga tikrinimo įstaiga ir jos personalas turi būti kompetentingi ir kvalifikuoti atlikti bandymus. Būtiną kompetenciją atlikti pažeidžiamumų skenavimą galima įrodyti, be kita ko, ankstesne profesine patirtimi informacijos saugumo bandymų srityje, patirtimi naudojant pažeidžiamumų skenerius, mokymais arba visuotinai pripažintais pramonės sertifikatais. Licencijos savininkas privalo užtikrinti, kad bandymus atliekantys asmenys būtų kvalifikuoti atlikti pažeidžiamumų skenavimą ir, paprašyti, įrodyti jų kvalifikaciją.

Siekiant užtikrinti, kad pažeidžiamumų skenavimas būtų atliekamas tinkamai, turi būti paskirtas už jo atlikimą atsakingas asmuo. Galutinę pažeidžiamumų skenavimo ataskaitą pasirašo ir patvirtina atsakingas asmuo ir pateikia ją priežiūros institucijai.

8 Pažeidžiamumų skenavimas, atliekamas kartu vykdant informacijos saugumo bandymą

Licencijos savininkas, atlikdamas informacijos saugumo bandymus, gali atlikti pažeidžiamumų skenavimą. Pažeidžiamumų skenavimams, atliekamiems kaip informacijos saugumo badymų dalis, taikomi tokie patys reikalavimai, kaip ir kitiems pažeidžiamumų skenavimams.

9 Pažeidžiamumų pašalinimas

Licencijos savininkas privalo reguliariai stebėti savo lošimų sistemų informacijos saugumą (ne tik vykdydamas informacijos saugumo bandymus) ir pašalinti pažeidžiamumus, dėl kurių sumažėja patikimumas, kai atsiranda pašalinimo galimybių ar kitų rizikos mažinimo metodų.

Jei pažeidžiamumų neįmanoma greitai pašalinti, licencijos savininkas stengiasi pasinaudoti turimomis priemonėmis, kad pašalintų pažeidžiamumus ir kuo labiau sumažintų poveikį.

Jei nustatyto išorės pažeidžiamumo CVSS v3 Base Score vertė yra mažesnė nei 5,0, licencijos savininkas gali savo nuožiūra atlikti pataisymus ir įvertinti, ar reikia skubiai juos atlikti.

10 Išduotų sertifikatų naudojimas

Akredituota tikrinimo įstaiga, kurią patvirtino priežiūros institucija, atsakinga už informacijos saugumo bandymus arba pažeidžiamumų skenavimą, atlikdama patikrinimą gali naudoti sertifikatus ar kitus patvirtinimus, suteiktus lošimo programinės įrangos licencijos savininkui. Jei tikrinimo įstaiga, atlikdama patikrinimą, naudoja esamus sertifikatus, ji turi įvertinti, ar sertifikatus galima laikyti pakankamai patikimais lošimų programinės įrangos licencijos savininko lošimų sistemos patikimumo ir informacijos saugumo įrodymais.

11 Neatitikimai

Licencijos savininkas privalo nedelsdamas pranešti priežiūros institucijai apie bet kokius jo nustatytus informacijos saugumo ar duomenų apsaugos pažeidimus, jei yra pagrindo įtarti, kad licencijos savininko naudojamų lošimų sistemų ar loterijos įrenginių patikimumas buvo pažeistas.

Licencijų savininkai neprivalo pranešti apie nedidelius saugumo arba duomenų apsaugos incidentus lošimų priežiūros institucijai, jei apskaičiuotas incidento veiksmingumas yra ribotas arba jei incidentas nėra įvertintas kaip darantis didelį poveikį lošimų sistemų patikimumui.

12 Įsigaliojimas

Šis reglamentas įsigalioja 2026 m. [mėnuo] X d.

Nacionalinė policijos valdyba
Lošimų administravimas
Konepajankatu 2, PL 50, 11101 Riihimäki
Telefono Nr. +358 295 480 181, poliisi.fi