Proiect de regulament

Fiabilitatea și securitatea informațiilor sistemelor de jocuri de noroc în temeiul Legii privind jocurile de noroc

Cuprins

1 Cadrul juridic, domeniul de aplicare și definiții

1.1 Competența autorității de supraveghere de a emite ordine

Dreptul autorității de supraveghere de a emite reglementări obligatorii se bazează pe articolul 44 alineatul (6) din Legea privind jocurile de noroc (xx/2025). În conformitate cu alineatul menționat, autoritatea de supraveghere poate emite reglementări mai detaliate privind fiabilitatea sistemelor de jocuri de noroc, a echipamentelor și metodelor de loterie utilizate în exploatarea jocurilor de noroc, privind cerințele tehnice pentru asigurarea caracterului aleatoriu al extragerii, privind forma și conținutul mai detaliat al anchetei și aprobării organismului de inspecție, precum și privind condițiile pe care organismul de inspecție trebuie să le îndeplinească pentru a fi aprobat de autoritate.

În conformitate cu articolul 57 din Legea privind jocurile de noroc, autoritatea de supraveghere este Agenția pentru Licențe și Supraveghere. În conformitate cu articolul 106 din aceeași lege, până la data de 31 decembrie 2026, Consiliul Poliției Naționale exercită atribuțiile autorității competente menționate la articolul 57.

1.2 Legislație

Următoarele reglementări sunt relevante pentru obiectul prezentului regulament:

- Legea privind jocurile de noroc (xx/2025);
- Legea privind procedura administrativă (434/2003);
- Legea privind protecția datelor (1050/2018);
- Regulamentul general al UE privind protecția datelor (2016/679).

1.3 Domeniul de aplicare

Această dispoziție se aplică unei persoane juridice sau fizice menționate în capitolul 1 articolul 2 alineatul (1) din Legea privind jocurile de noroc, căreia i s-a acordat o licență exclusivă sau o licență pentru activități de jocuri de noroc în temeiul Legii privind jocurile de noroc.

Licența exclusivă este reglementată de articolul 5 din Legea privind jocurile de noroc, iar licența pentru jocuri de noroc este reglementată de articolul 6.

1.4 Definiții

În sensul prezentei dispoziții, se aplică definițiile următoare. În sensul prezentului regulament:

- „licență exclusivă” înseamnă o licență acordată pentru formele de jocuri de noroc menționate la articolul 5 din Legea privind jocurile de noroc;

- „licență de organizare a jocurilor de noroc” înseamnă o licență acordată pentru tipurile de jocuri de noroc menționate la articolul 6 din Legea privind jocurile de noroc;
- „tranzacție de jocuri de noroc” înseamnă miza pariată de jucător în joc, opțiunea de rezultat aleasă de jucător, alegerile făcute de jucător care sunt relevante pentru rezultatul jocului și rezultatele pieței și extragerilor, precum și orice câștig și pierdere înregistrată în sistemul de jocuri de noroc al deținătorului unei licențe exclusive sau al unei licențe de jocuri de noroc;
- „tranzacție de cont de jucător” înseamnă intrări din cont;
- „sistem de jocuri de noroc” înseamnă un sistem de informare online utilizat de operatorul de jocuri de noroc sau în numele acestuia pentru operarea jocurilor de noroc.

2 Acreditarea unui organism de inspecție

Deținătorul de licență este responsabil cu fiabilitatea dispozitivelor sale de loterie și a sistemelor sale de jocuri de noroc, precum și pentru efectuarea auditurilor efectuate pentru a asigura această fiabilitate. Evaluarea fiabilității și securității este efectuată de un organism de inspecție extern acreditat. Organismul de inspecție este acreditat în sensul Regulamentului (CE) nr. 765/2008 al Parlamentului European și al Consiliului de stabilire a cerințelor de acreditare și de supraveghere a pieței în ceea ce privește comercializarea produselor și de abrogare a Regulamentului (CEE) nr. 339/93.

Acreditarea poate fi acordată organismelor de control de către organismul național de acreditare FINAS (Serviciul finlandez de acreditare). Un organism de acreditare străin poate acționa, de asemenea, ca organism de acreditare dacă este membru al Acordului de recunoaștere multilaterală al Organizației Europene de Acreditare (EA MLA) în domeniul de competență relevant. Deținătorul de licență are obligația să se asigure că operatorul extern care efectuează auditul are o acreditare valabilă.

3 Practici generale de securitate a informațiilor

Deținătorul de licență este responsabil cu securitatea informațiilor, protecția datelor și alte caracteristici tehnice de fiabilitate ale propriilor sisteme de jocuri de noroc. Deținătorul de licență trebuie să respecte bunele practici în materie de securitate a informațiilor în operațiunile sale și să depună eforturi pentru a reduce la minimum amenințările la adresa securității informațiilor, încălcările securității datelor și alte probleme care ar putea pune în pericol fiabilitatea sistemelor de jocuri de noroc. Deținătorul de licență are, de asemenea, obligația de a monitoriza factorii menționați mai sus în afara inspecțiilor periodice prevăzute în prezentul regulament, pentru a asigura fiabilitatea sistemelor sale.

4 Organismul de inspecție care efectuează testarea securității informațiilor

Deținătorul de licență are obligația să efectueze teste de securitate pe sistemele sale de jocuri de noroc o dată la doi ani. Rezultatul testării securității informațiilor se transmite autorității de supraveghere. Testele de securitate a informațiilor și rezultatele acestora nu pot fi mai vechi de doi ani.

Testarea securității informațiilor se efectuează de către un organism de inspecție extern acreditat în conformitate cu ISO/IEC 17025, ISO/IEC 17065 sau ISO/IEC 17020, astfel cum se specifică la articolul 2 din prezentul regulament. Testarea securității informațiilor trebuie să acorde o atenție deosebită protecției și integrității componentelor sistemului de jocuri de noroc aleatorii, protecției componentelor care conțin date cu caracter personal și protecției componentelor legate de plăți.

Organismul de inspecție responsabil cu efectuarea testelor de securitate a informațiilor și personalul acestuia trebuie să fie competent și adecvat pentru efectuarea testelor. Competența necesară pentru efectuarea testelor de securitate a informațiilor poate fi demonstrată, printre altele, prin experiența profesională anterioară în testarea securității informațiilor, formarea profesională sau certificatele recunoscute în mod general în sector. Deținătorul de licență are obligația să se asigure că persoanele care efectuează testarea sunt calificate să efectueze teste de securitate a informațiilor și, la cerere, să își demonstreze calificările.

Se numește o persoană desemnată pentru implementarea testelor de securitate, care va fi responsabilă cu implementarea corespunzătoare. Raportul final al testului de securitate a informațiilor se semnează și se validează de către persoana desemnată și se transmite autorității de supraveghere.

În contextul testării securității informațiilor, se testează cel puțin următoarele componente, precum și vulnerabilitățile sau incidentele conexe:

- Posibilitatea de manipulare a componentelor de randomizare
- Accesul la baza de date a clienților
- Abilitatea de a influența rezultatul jocurilor
- Capacitatea de a influența sistemele de plată sau tranzacțiile de plată
- Accesul neautorizat la serverele utilizate pentru stocarea tranzacțiilor de jocuri de noroc și a tranzacțiilor aferente conturilor de jucători
- Capacitatea de a edita datele arhivate privind evenimentele legate de jocurile de noroc sau evenimentele legate de conturile de jocuri de noroc
- Modificarea sau distrugerea înregistrărilor referitoare la sistemele de jocuri de noroc

4.1 Domeniul de competență

Organismul de inspecție acreditat care efectuează auditul are domeniul de competență pentru jocurile de noroc în acreditarea sa ISO/IEC. Domeniul de competență trebuie să acopere cerințele stabilite de legislația finlandeză privind jocurile de noroc și de reglementările tehnice ale autorității de supraveghere.

Până la 1 ianuarie 2027, autoritatea de supraveghere poate accepta o acreditare care include un domeniu de competență evaluat și acordat pe baza reglementărilor tehnice emise pentru sistemele de jocuri de noroc daneze sau suedeze.

5 Reînnoirea testelor de securitate a informațiilor

Deținătorul de licență transmite autorității de supraveghere rezultatele testelor de securitate a informațiilor aprobate. Deținătorul de licență nu poate începe exploatarea jocurilor de noroc înainte de a fi trecut cu succes testele de securitate. Rezultatul testului de securitate a informațiilor nu trebuie să fie mai vechi de doi ani.

Autoritatea de supraveghere poate, la discreția sa, să acorde timp suplimentar pentru punerea în aplicare a testelor de securitate, în timpul cărora funcționarea jocurilor de noroc poate continua.

6 Testul de securitate a informațiilor respinse

Organismul de control care efectuează testul de securitate a informațiilor trebuie să evalueze vulnerabilitățile identificate în timpul testării securității informațiilor și importanța acestora pentru fiabilitatea sistemului de jocuri de noroc. Vulnerabilitățile identificate în timpul evaluării trebuie evaluate utilizând calculatorul CVSS v3 (Common Vulnerability Scoring System Calculator versiunea 3) furnizat de Institutul Național de Tehnologie (NIST). Pentru calculatorul CVSS v3, gravitatea vulnerabilității se evaluează cu ajutorul parametrilor scorului de bază. Dacă în timpul testelor de securitate sunt detectate vulnerabilități cu o valoare CVSS calculată mai mare de 5.0, testul nu poate fi considerat reușit.

Dacă testul de securitate a informațiilor al deținătorului de licență nu este aprobat, deținătorul de licență trebuie să ia imediat măsuri pentru a remedia vulnerabilitățile identificate în materie de securitate a informațiilor. Deținătorul de licență raportează autorității de supraveghere testul de securitate a informațiilor respins.

Deținătorul de licență trebuie să efectueze un nou test de securitate în termen de 90 de zile de la respingerea testului de securitate a informațiilor. Testarea reînnoită a securității informațiilor nu trebuie să fie efectuată pe întregul sistem de jocuri de noroc; în schimb, testarea securității informațiilor poate fi direcționată către deficiențele care au determinat respingerea. În legătură cu testarea reînnoită a securității informațiilor, organismul de control trebuie să se asigure că vulnerabilitățile identificate anterior ca motive de respingere au fost corectate.

Implementarea jocurilor de noroc nu poate începe înainte de efectuarea unor teste de securitate aprobate și valide.

7 Scanarea vulnerabilității

Pe lângă testele de securitate, deținătorii de licență au obligația să monitorizeze securitatea propriilor sisteme prin intermediul unor scanări periodice ale vulnerabilităților. Scopul scanărilor de vulnerabilitate este de a se asigura că sistemele de jocuri de noroc utilizate de deținătorul de licență nu prezintă vulnerabilități de securitate externe care ar putea fi exploatate pentru a efectua atacuri împotriva sistemelor de jocuri de noroc.

Deținătorul de licență are obligația să efectueze o scanare externă a vulnerabilității o dată pe an și să raporteze rezultatele autorității de supraveghere. Scanarea vulnerabilității poate fi efectuată de un organism de inspecție extern acreditat în conformitate cu ISO/IEC 17025, ISO/IEC 17065 sau ISO/IEC 17020, astfel cum se specifică la alineatul (2) din prezentul regulament.

Deținătorul de licență are obligația să remedieze vulnerabilitățile detectate în timpul scanării vulnerabilităților prin actualizări sau alte măsuri urgente de atenuare în cazul în care nu sunt disponibile actualizări corective. Metoda de evaluare descrisă la articolul 6 se aplică vulnerabilităților de securitate detectate în timpul scanărilor de vulnerabilitate. În cazul în care valoarea CVSS calculată a vulnerabilității externe identificate depășește 5,0, deținătorul de licență ia măsuri imediate pentru a remedia vulnerabilitățile.

Organismul de inspecție responsabil cu efectuarea scanării vulnerabilității și personalul său trebuie să fie competent și adecvat pentru efectuarea testelor. Competența necesară pentru efectuarea scanărilor de vulnerabilitate poate fi demonstrată, printre altele, prin experiența profesională anterioară în testarea securității informațiilor, experiența în utilizarea scanerelor de vulnerabilități, formarea profesională sau certificatele recunoscute în mod general în sector. Deținătorul de licență are obligația să se asigure că persoanele care efectuează testarea sunt calificate să efectueze scanări de vulnerabilitate și, la cerere, să își demonstreze calificările.

Trebuie desemnată o persoană responsabilă cu efectuarea scanării vulnerabilității pentru a se asigura că aceasta se efectuează în mod corespunzător. Raportul final de scanare a vulnerabilității se semnează și se validează de către persoana responsabilă și se transmite autorității de supraveghere.

8 Scanări de vulnerabilitate efectuate în legătură cu testarea securității informațiilor

Deținătorul de licență poate efectua scanări de vulnerabilitate ca parte a testelor de securitate a informațiilor. Aceleași cerințe se aplică scanărilor de vulnerabilitate efectuate ca parte a testării de securitate a informațiilor ca și altor scanări de vulnerabilitate.

9 Remedierea vulnerabilităților

Deținătorul de licență are obligația să monitorizeze periodic securitatea informațiilor din propriile sisteme de jocuri de noroc, chiar și în afara testelor de securitate a informațiilor, și să remedieze vulnerabilitățile care compromit fiabilitatea atunci când devin disponibile remedieri sau alte metode de atenuare.

Dacă nu este posibilă remedierea promptă a vulnerabilităților, deținătorul de licență va încerca să utilizeze mijloacele disponibile pentru a combate vulnerabilitățile și a minimiza impactul.

În cazul în care valoarea scorului de bază CVSS v3 al vulnerabilității externe detectate este mai mică de 5,0, deținătorul de licență își poate utiliza propria discreție pentru punerea în aplicare a corecțiilor și evaluarea caracterului urgent al nevoii pentru acestea.

10 Utilizarea certificatelor eliberate

Un organism de inspecție acreditat, aprobat de autoritatea de supraveghere responsabilă cu efectuarea testelor de securitate a informațiilor sau a scanărilor de vulnerabilitate, poate utiliza certificate sau alte atestate acordate deținătorului de licență de software de jocuri de noroc în cadrul inspecției sale. În cazul în care organismul de inspecție utilizează certificatele existente în cadrul inspecției, acesta trebuie să evalueze dacă certificatele pot fi considerate dovezi suficient de fiabile ale fiabilității și securității informațiilor sistemului de jocuri de noroc al deținătorului de licență de software de jocuri de noroc.

11 Discrepanțe

Deținătorul de licență are obligația de a raporta fără întârziere autorității de supraveghere orice încălcare a securității informațiilor sau a protecției datelor pe care le detectează, dacă există motive să se suspecteze că fiabilitatea sistemelor de jocuri de noroc sau a echipamentelor de loterie utilizate de deținătorul de licență a fost compromisă.

Deținătorii de licență nu au obligația să raporteze incidentele minore de securitate sau de protecție a datelor autorității de supraveghere a jocurilor de noroc în cazul în care eficacitatea estimată a incidentului este limitată ca natură sau în cazul în care se estimează că incidentul nu are un impact semnificativ asupra fiabilității sistemelor de jocuri de noroc.

12 Intrare în vigoare

Prezentul regulament intră în vigoare la X [luna] 2026.

Consiliul Poliției Naționale
Autoritatea de supraveghere a jocurilor de noroc
Konepajankatu 2, PL 50, 11101 Riihimäki
Telefon +358 295 480 181, poliisi.fi