Utkast till förordning

Tillförlitlighet och informationssäkerhet hos penningspelsystem enligt lagen om penningspel

Innehåll

1 Rättslig ram, tillämpningsområde och definitioner

1.1 Tillsynsmyndighetens befogenhet att utfärda förelägganden

Tillsynsmyndighetens rätt att utfärda bindande föreskrifter grundar sig på 44 § 6 mom. i lagen om penningspel (xx/2025). Enligt nämnda underavsnitt kan tillsynsmyndigheten utfärda mer detaljerade föreskrifter om tillförlitligheten hos de penningspelssystem, lotterimaskiner och lotterimetoder som används vid penningspelverksamhet, om de tekniska kraven för att säkerställa slumpmässigheten i dragningen, om den mer detaljerade formen och innehållet i inspektionsorganets utredning och godkännande, samt om de villkor som inspektionsorganet måste uppfylla för att godkännas av myndigheten.

Enligt 57 § i lagen om penningspel är tillsynsmyndigheten tillstånds- och tillsynsmyndigheten. Enligt 106 § i lagen ska Polisstyrelsen vara den behöriga myndighet som avses i 57 § till och med den 31 december 2026.

1.2 Lagstiftning

Följande föreskrifter är relevanta för tillämpningsområdet för denna förordning:

- Lagen om penningspel (xx/2025)
- Förvaltningslag (434/2003)
- Dataskyddslagen (1050/2018)
- EU:s allmänna dataskyddsförordning (2016/679)

1.3 Tillämpningsområde

Denna bestämmelse gäller juridiska eller fysiska personer som avses i kapitel 1, 2.1 § i lagen om penningspel och som har beviljats en exklusiv licens eller en licens för penningspelverksamhet enligt lagen om penningspel.

Den exklusiva licensen regleras av 5 § i lagen om penningspel och licensen för penningspel regleras av 6 §.

1.4 Definitioner

I denna bestämmelse gäller följande definitioner. I denna förordning avses med

- *exklusiv licens*: ett tillstånd som beviljats för de typer av penningspel som avses i 5 § i lagen om penningspel,
- *penningspelslicens* : ett tillstånd som beviljats för de typer av penningspel som avses i 6 § i lagen om penningspel,

- *speltransaktion i penningspel* avser den insats som spelaren satsar på spelet, det utfallsalternativ som spelaren väljer, de val som spelaren gör och som är relevanta för spelets utfall samt resultaten av marknaderna och dragningarna, liksom eventuella vinster och förluster som registreras i penningspelsystemet hos innehavaren av en exklusiv licens eller en penningspelslicens,
- *transaktion på spelarkonto*: kontohändelser,
- *penningspelssystem*: ett onlinebaserat informationssystem som används av eller på uppdrag av penningspelsaktören för att bedriva penningspelverksamhet.

2 Ackreditering av ett inspektionsorgan

Licenshavaren ansvarar för tillförlitligheten hos sina lotterianordningar och penningspelsystem samt för att utföra de revisioner som genomförs för att säkerställa tillförlitligheten. Bedömningen av tillförlitlighet och säkerhet utförs av ett externt ackrediterat inspektionsorgan. Organet ska vara ackrediterat enligt Europaparlamentets och rådets förordning (EG) nr 765/2008 om krav för ackreditering och marknadskontroll i samband med saluföring av produkter och upphävande av förordning (EEG) nr 339/93.

Ackreditering kan beviljas till kontrollorgan av det nationella ackrediteringsorganet FINAS (Finlands ackrediteringstjänst). Ett utländskt ackrediteringsorgan kan också fungera som ackrediteringsorgan om det är medlem i de europeiska ackrediteringsorganisationens multilaterala avtal om erkännande inom det relevanta kompetensområdet. Licenshavaren är skyldig att se till att den externa aktör som utför revisionen har en giltig ackreditering.

3 Allmänna rutiner för informationssäkerhet

Licenshavaren ansvarar för informationssäkerheten, dataskyddet och andra tekniska tillförlitlighetsegenskaper hos sina egna penningspelsystem. Licenshavaren ska följa god informationssäkerhetspraxis i sin verksamhet och sträva efter att minimera hot mot informationssäkerheten, dataintrång och andra problem som kan äventyra penningspelsystemens tillförlitlighet. Licenshavaren är också skyldig att övervaka ovannämnda faktorer utanför de regelbundna inspektioner som avses i denna förordning, för att säkerställa tillförlitligheten hos sina system.

4 Kontrollorgan som testar informationssäkerheten

Licenshavaren är skyldig att genomföra säkerhetstestning av sina penningspelsystem vartannat år. Resultatet av informationssäkerhetstestningen ska skickas till tillsynsmyndigheten. Informationssäkerhetstestningen och resultaten av denna får inte vara äldre än två år.

Informationssäkerhetstestningen ska utföras av ett externt kontrollorgan som är ackrediterat i enlighet med ISO/IEC 17025, ISO/IEC 17065 eller ISO/IEC 17020, enligt vad som anges i 2 § i denna förordning. I samband med informationssäkerhetstestning ska särskild uppmärksamhet ägnas åt skyddet och integriteten hos komponenterna i penningspelsystemets slumpkomponenter, skyddet av komponenter som innehåller personuppgifter och skyddet av betalningsrelaterade komponenter.

Det inspektionsorgan som ansvarar för att utföra informationssäkerhetstestning och dess personal ska vara kompetent och lämpa sig för att kunna utföra testerna. Den kompetens som krävs för att utföra informationssäkerhetstester kan bland annat styrkas genom tidigare yrkeserfarenhet av informationssäkerhetstestning, utbildning eller allmänt erkända branschintyg. Licenshavaren är skyldig att säkerställa att de personer som utför testningen är kvalificerade att utföra informationssäkerhetstestning och, på begäran, kunna styrka deras kvalifikationer.

En specifik person ska utses för genomförandet av säkerhetstestningen, som ska ansvara för den genomförs som den ska. Den slutliga rapporten om informationssäkerhetstestet ska undertecknas och godkännas av den utsedda personen och lämnas in till tillsynsmyndigheten.

I samband med informationssäkerhetstestningen ska åtminstone följande komponenter, samt relaterade sårbarheter eller incidenter, testas:

- Möjlighet till manipulering av de slumpmässiga komponenterna
- Åtkomst till kunddatabasen
- Förmåga att påverka spelens resultat
- Förmåga att påverka betalningssystem eller betalningstransaktioner
- Obehörig åtkomst till servrar som används för att lagra speltransaktioner i penningspel och transaktioner på spelarkonton
- Förmåga att redigera arkiverade uppgifter om penningspelsevenemang eller om penningspelskonton.
- Ändring eller förstöring av loggar med koppling till penningspelsystem

4.1 Behörighetsområde

Det ackrediterade kontrollorgan som utför revisionen ska ha behörighetsområdet penningspel i sin ISO/IEC-ackreditering. Behörighetsområdet måste omfatta de krav som ställs i den finska lagstiftningen om penningspel och tillsynsmyndighetens tekniska föreskrifter.

Fram till den 1 januari 2027 får tillsynsmyndigheten godta ackreditering som omfattar ett kompetensområde som bedömts och beviljats på grundval av tekniska föreskrifter som utfärdats för det danska eller svenska penningspelsystemet.

5 Förnyad informationssäkerhetstestning

Licenshavaren ska överlämna resultaten av den godkända informationssäkerhetstestningen till tillsynsmyndigheten. Licenshavaren får inte börja bedriva penningspelverksamhet förrän denne med framgång har genomgått säkerhetstestningen. Resultatet av informationssäkerhetstestningen får inte vara äldre än två år.

Tillsynsmyndigheten kan efter eget gottfinnande bevilja ytterligare tid för genomförandet av säkerhetstestningen, och under denna tid får penningspelverksamheten fortsätta.

6 Icke-godkänd informationssäkerhetstestning

Det kontrollorgan som utför informationssäkerhetstestningen bör bedöma de sårbarheter som har identifierats under informationssäkerhetstestningen och deras betydelse för penningspelsystemets tillförlitlighet. De sårbarheter som identifierats under bedömningen bör bedömas med hjälp av CVSS v3-kalkylatorn (Common Vulnerability Scoring System Calculator, version 3), som tillhandahålls av det nationella teknikinstitutet (NIST). För CVSS v3-kalkylatorn ska sårbarhetens allvarlighetsgrad bedömas med hjälp av baspoängsmått. Om sårbarheter med ett beräknat CVSS-värde på mer än 5,0 upptäcks under säkerhetstestningen kan testet inte betraktas som framgångsrikt.

Om licenshavarens informationssäkerhetstest inte godkänns måste licenshavaren omedelbart vidta åtgärder för att åtgärda de fastställda informationssäkerhetsbristerna. Licenshavaren ska rapportera det icke-godkända informationssäkerhetstestet till tillsynsmyndigheten.

Licenshavaren måste genomföra ett nytt säkerhetstest inom 90 dagar efter det icke-godkända informationssäkerhetstestet. Förnyad informationssäkerhetstestning behöver inte utföras för hela penningspelsystemet. Istället kan informationssäkerhetstestningen riktas mot de brister som ledde till att testet inte godkändes. I samband med den förnyade informationssäkerhetstestningen måste inspektionsorganet säkerställa att de sårbarheter som tidigare identifierades som skäl för avslag har korrigerats.

Bedrivandet av hasardspel får inte påbörjas innan godkänd och giltig säkerhetstestning har utförts.

7 Sårbarhetsskanning

Utöver säkerhetstestning är licenshavarna skyldiga att övervaka säkerheten i sina egna system genom regelbundna sårbarhetsskanningar. Syftet med sårbarhetsskanningarna är att säkerställa att de penningspelsystem som används av licenshavaren inte har några externa säkerhetsbrister som kan utnyttjas för att genomföra attacker mot penningspelsystemen.

Licenshavaren är skyldig att genomföra en extern sårbarhetsskanning en gång om året och rapportera resultaten till tillsynsmyndigheten. Sårbarhetsskanning får utföras av ett externt inspektionsorgan som är ackrediterat i enlighet med ISO/IEC 17025, ISO/IEC 17065 eller ISO/IEC 17020, enligt vad som anges i punkt 2 i denna förordning.

Licenshavaren är skyldig att åtgärda sårbarheter som upptäcks i samband med sårbarhetsskanning genom uppdateringar eller andra riskbegränsningsåtgärder som skyndsamt vidtas om korrigerande uppdateringar inte finns tillgängliga. Den bedömningsmetod som beskrivs i 6 § ska tillämpas på säkerhetssårbarheter som upptäcks i samband med sårbarhetsskanningar. Om det beräknade CVSS-värdet för den identifierade externa sårbarheten överstiger 5,0 ska licenshavaren vidta omedelbara åtgärder för att avhjälpa sårbarheterna.

Det inspektionsorgan som ansvarar för att genomföra sårbarhetsskanningen och dess personal ska vara kompetent och lämpa sig för att utföra testerna. Den kompetens som krävs för att utföra sårbarhetsskanningar kan bland annat styrkas genom tidigare yrkeserfarenhet av informationssäkerhetstestning, erfarenhet av användning av sårbarhetsskannrar, utbildning eller allmänt erkända branschintyg. Licenshavaren är skyldig att säkerställa att de personer som utför testningen är kvalificerade att utföra sårbarhetsskanningar och, på begäran, kunna styrka deras kvalifikationer.

En person som ansvarar för att utföra sårbarhetsskanningen måste utses för att säkerställa att den utförs på ett korrekt sätt. Den slutliga sårbarhetsskanningsrapporten ska undertecknas och godkännas av den ansvariga personen och lämnas in till tillsynsmyndigheten.

8 Sårbarhetsskanningar som utförs i samband med informationssäkerhetstestning

Licenshavaren får utföra sårbarhetsskanningar som en del av informationssäkerhetstestningen. Samma krav gäller för sårbarhetsskanningar som utförs som en del av informationssäkerhetstestning som för andra sårbarhetsskanningar.

9 Åtgärda sårbarheter

Licenshavaren är skyldig att regelbundet övervaka informationssäkerheten i sina egna penningspelsystem, även utanför informationssäkerhetstesterna, och att åtgärda sårbarheter som äventyrar tillförlitligheten när lösningar eller andra begränsningsmetoder blir tillgängliga.

Om det inte går att snabbt åtgärda sårbarheterna ska licenshavaren försöka använda tillgängliga medel för att bekämpa sårbarheterna och minimera effekterna.

Om värdet för CVSS v3-baspoängen för den upptäckta externa sårbarheten är mindre än 5,0 får licenshavaren efter eget gottfinnande genomföra korrigeringar och bedöma hur pass brådskande behovet av dem är.

10 Användning av utfärdade intyg

Ett ackrediterat inspektionsorgan som har godkänts av den tillsynsmyndighet som ansvarar för att genomföra informationssäkerhetstestning eller sårbarhetsskanningar får använda intyg eller andra bevis som har beviljats innehavaren av programvarulicensen för penningspel som en del av sin inspektion. Om inspektionsorganet använder befintliga intyg som en del av inspektionen måste det bedöma om intygen kan anses vara tillräckligt tillförlitliga bevis på tillförlitligheten och informationssäkerheten hos det penningspelsystem som används av innehavaren av programvarulicensen för penningspel.

11 Avvikelser

Licenshavaren är skyldig att utan dröjsmål rapportera alla överträdelser mot informationssäkerheten eller dataskyddet som denne upptäcker till tillsynsmyndigheten, om det finns anledning att misstänka att tillförlitligheten hos de penningspelsystem eller den lotteriutrustning som används av licenshavaren har äventyrats.

Licenshavare ska inte vara skyldiga att rapportera mindre säkerhets- eller dataskyddsincidenter till tillsynsmyndigheten för penningspel om incidentens uppskattade påverkan är begränsad eller om incidenten inte bedöms ha en betydande inverkan på penningspelsystemens tillförlitlighet.

12 Ikraftträdande

Denna förordning träder i kraft den X [månad] 2026.

Polisstyrelsen
Lotteriförvaltningen
Konepajankatu 2, PL 50, 11101 Riihimäki
Telefon +358 295 480 181, poliisi.fi