Ontwerpverordening

Betrouwbaarheid en informatiebeveiliging van kansspelsystemen op grond van de kansspelwet

Inhoud

1 Wettelijk kader, toepassingsgebied en definities

1.1 De bevoegdheid van de toezichthoudende autoriteit om verordeningen uit te vaardigen

Het recht van de toezichthoudende instantie om bindende verordeningen uit te vaardigen is gebaseerd op artikel 44, lid 6 van de kansspelwet (xx/2025). Volgens genoemd lid kan de toezichthoudende autoriteit gedetailleerdere voorschriften bepalen over de betrouwbaarheid van de kansspelsystemen, loterijapparatuur en loterijmethoden die worden gebruikt bij de exploitatie van kansspelen, over de technische vereisten voor het waarborgen van de willekeur van de trekking, over de meer gedetailleerde vorm en inhoud van het onderzoek en de goedkeuring van het inspectieorgaan en over de voorwaarden waaraan het inspectieorgaan moet voldoen om door de autoriteit te worden goedgekeurd.

Volgens artikel 57 van de kansspelwet is de toezichthoudende autoriteit de Finse toezichthoudende autoriteit. Overeenkomstig artikel 106 van de wet treedt de Nationale Politieraad tot en met 31 december 2026 op als de in artikel 57 bedoelde bevoegde autoriteit.

1.2 Wetgeving

De volgende regels zijn relevant voor het voorwerp van deze verordening:

- Wet op de kansspelen (xx/2025)
- Wet inzake administratieve procedures (434/2003)
- Wet bescherming persoonsgegevens (1050/2018)
- Algemene verordening gegevensbescherming EU (2016/679)

1.3 Toepassingsgebied

Deze bepaling is van toepassing op een rechtspersoon of natuurlijke persoon als bedoeld in hoofdstuk 1, artikel 2, lid 1, van de kansspelwet aan wie op grond van de kansspelwet een exclusieve vergunning of een vergunning voor kansspelactiviteiten is verleend.

De exclusieve vergunning wordt beheerd door artikel 5 van de kansspelwet en de kansspelvergunning wordt beheerd door artikel 6.

1.4 Begripsbepalingen

Voor de toepassing van dit decreet zijn de volgende definities van toepassing. Voor de toepassing van deze regelgeving wordt verstaan onder:

- *exclusieve vergunning*: een vergunning die is verleend voor de soorten kansspelen zoals bedoeld in artikel 5 van de kansspelwet;

- kansspel*vergunning:* een vergunning die is verleend voor de soorten kansspelen zoals bedoeld in artikel 6 van de kansspelwet;
- *kansspeltransactie:* de door de speler op het spel ingezette inzet, de door de speler gekozen uitkomstoptie, de door de speler gemaakte keuzes die relevant zijn voor de uitkomst van het spel en de resultaten van de markten en trekkingen, alsmede eventuele winsten en verliezen die in het kansspelsysteem van de houder van een exclusieve vergunning of kansspelvergunning zijn geregistreerd;
- *transactie op de spelersrekening* betekent boekingen op de rekening.
- *kansspelsysteem:* een online informatiesysteem dat door of namens de kansspelexploitant wordt gebruikt voor de exploitatie van kansspelen;

2 Accreditatie van een inspectieorgaan

De vergunninghouder is verantwoordelijk voor de betrouwbaarheid van zijn loterijapparaten en kansspelsystemen, alsook voor het uitvoeren van de audits om die betrouwbaarheid te waarborgen. De beoordeling van de betrouwbaarheid en beveiliging wordt uitgevoerd door een extern geaccrediteerd inspectieorgaan. Het inspectieorgaan moet geaccrediteerd zijn in de zin van Verordening (EG) nr. 765/2008 van het Europees Parlement en de Raad tot vaststelling van de eisen inzake accreditatie en markttoezicht voor het verhandelen van producten en tot intrekking van Verordening (EEG) nr. 339/93.

Accreditatie kan aan inspectieorganen worden verleend door het nationale accreditatieorgaan FINAS (Finse accreditatiedienst). Een buitenlands accreditatieorgaan kan ook optreden als accreditatieorgaan, indien zij lid is van de Multilaterale Erkenningsovereenkomst (MLA) van de Europese Accreditatieorganisatie op het betreffende bevoegdheidsgebied. De vergunninghouder is verplicht ervoor te zorgen dat de externe exploitant die de audit uitvoert, over een geldige accreditatie beschikt.

3 Algemene praktijken op het gebied van informatiebeveiliging

De vergunninghouder is verantwoordelijk voor de informatiebeveiliging, gegevensbescherming en andere technische betrouwbaarheidskenmerken van zijn eigen kansspelsystemen. De vergunninghouder moet bij zijn activiteiten goede praktijken op het gebied van informatiebeveiliging volgen en ernaar streven om bedreigingen voor de informatiebeveiliging, datalekken en andere problemen die de betrouwbaarheid van kansspelsystemen in gevaar kunnen brengen, tot een minimum te herleiden. De vergunninghouder is ook verplicht om de bovengenoemde factoren buiten de in deze verordening bedoelde regelmatige inspecties om te controleren, om de betrouwbaarheid van zijn systemen te waarborgen.

4 Inspectieorgaan dat de informatiebeveiligingstests uitvoert

De vergunninghouder is verplicht om zijn kansspelsystemen om de twee jaar aan beveiligingstests te onderwerpen. De resultaten van de informatiebeveiligingstests moeten worden voorgelegd aan de toezichthoudende autoriteit. Informatiebeveiligingstests en het resultaat daarvan mogen niet ouder zijn dan twee jaar.

De informatiebeveiligingstests worden uitgevoerd door een extern inspectieorgaan dat is geaccrediteerd overeenkomstig ISO/IEC 17025, ISO/IEC 17065 of ISO/IEC 17020, zoals gespecificeerd in artikel 2 van deze verordening. Bij de informatiebeveiligingstest wordt bijzondere aandacht besteed aan de bescherming en integriteit van de onderdelen van het willekeurig kansspelsysteem, aan de bescherming van onderdelen die persoonsgegevens bevatten en aan de bescherming van betalingsgerelateerde onderdelen.

Het inspectieorgaan dat verantwoordelijk is voor het uitvoeren van informatiebeveiligingstests en zijn personeel moeten bekwaam en geschikt zijn om de tests uit te voeren. De vereiste bekwaamheid om informatiebeveiligingstests uit te voeren, kan onder meer worden aangetoond door eerdere beroepservaring op het gebied van informatiebeveiligingstests, opleiding of algemeen erkende sectorcertificaten. De vergunninghouder is verplicht ervoor te zorgen dat de personen die de tests uitvoeren, gekwalificeerd zijn om informatiebeveiligingstests uit te voeren en op verzoek hun kwalificaties aan te tonen.

Er wordt een aangewezen persoon aangesteld voor de uitvoering van de beveiligingstests, die verantwoordelijk is voor de juiste uitvoering. Het definitieve testrapport over de informatiebeveiliging wordt door de aangewezen persoon ondertekend en gevalideerd en bij de toezichthoudende autoriteit ingediend.

In het kader van de informatiebeveiligingstests worden ten minste de volgende onderdelen en daarmee verband houdende kwetsbaarheden of incidenten getest:

- Mogelijkheid tot manipulatie van de willekeurige onderdelen
- Toegang tot de klantendatabase
- Mogelijkheid om de uitkomst van games te beïnvloeden
- Mogelijkheid om betalingssystemen of betalingstransacties te beïnvloeden
- Ongeoorloofde toegang tot servers die worden gebruikt voor de opslag van kansspeltransacties en transacties op spelersrekeningen
- Mogelijkheid om gearchiveerde gegevens over kansspelactiviteiten of kansspelrekeningen te bewerken
- Wijziging of vernietiging van logbestanden met betrekking tot kansspelsystemen

4.1 Bevoegdheidsgebied

Het geaccrediteerde inspectieorgaan dat de audit uitvoert, beschikt over het bevoegdheidsgebied voor kansspelen in haar ISO/IEC-accreditatie. Het bevoegdheidsgebied moet de vereisten omvatten die zijn bepaald in de Finse kansspelwetgeving en de technische voorschriften van de toezichthoudende autoriteit.

Tot 1 januari 2027 kan de toezichthoudende autoriteit accreditaties aanvaarden die een bevoegdheidsgebied omvatten dat is beoordeeld en toegekend op basis van technische voorschriften die werden uitgevaardigd voor de Deense of Zweedse kansspelsystemen.

5 Vernieuwing van informatiebeveiligingstests

De vergunninghouder dient de resultaten van de goedgekeurde informatiebeveiligingstests in bij de toezichthoudende autoriteit. De vergunninghouder mag geen kansspelen beginnen aan te bieden voordat deze met succes een beveiligingstest heeft doorstaan. Het resultaat van de informatiebeveiligingstest mag niet meer dan twee jaar oud zijn.

De toezichthoudende autoriteit kan, naar eigen goeddunken, extra tijd toekennen voor de uitvoering van de beveiligingstests, tijdens welke de exploitatie van kansspelen kan worden voortgezet.

6 Afgewezen informatiebeveiligingstest

Het inspectieorgaan dat de informatiebeveiligingstest uitvoert, moet de kwetsbaarheden beoordelen die tijdens de informatiebeveiligingstest zijn bepaald en het belang ervan voor de betrouwbaarheid van het kansspelsysteem. De tijdens de beoordeling geïdentificeerde kwetsbaarheden moeten worden beoordeeld met behulp van de CVSS v3-calculator (Common Vulnerability Scoring System Calculator, versie 3) van het Nationaal Instituut voor Technologie (NIST). Voor de CVSS v3-calculator wordt de ernst van de kwetsbaarheid beoordeeld aan de hand van Base Score Metrics. Indien kwetsbaarheden met een berekende CVSS-waarde hoger dan 5,0 worden gedetecteerd tijdens een beveiligingstest, kan de test niet als succesvol worden beschouwd.

Indien de informatiebeveiligingstest van de vergunninghouder niet wordt goedgekeurd, moet de vergunninghouder onmiddellijk maatregelen nemen om de geïdentificeerde kwetsbaarheden in de informatiebeveiliging te verhelpen. De vergunninghouder rapporteert de afgewezen informatiebeveiligingstest aan de toezichthoudende autoriteit.

De vergunninghouder moet binnen 90 dagen na de afgewezen informatiebeveiligingstest een nieuwe beveiligingstest uitvoeren. Vernieuwde informatiebeveiligingstests hoeven niet op het gehele kansspelsysteem te worden uitgevoerd; in plaats daarvan kunnen informatiebeveiligingstests worden gericht op de tekortkomingen die de afwijzing hebben veroorzaakt. In het kader van de hernieuwde informatiebeveiligingstests moet het

inspectieorgaan zich ervan vergewissen dat de eerder als afwijzingsgrond aangemerkte zwakke punten zijn gecorrigeerd.

Met de uitvoering van kansspelen mag niet worden begonnen voordat goedgekeurde en geldige beveiligingstests zijn uitgevoerd.

7 Kwetsbaarheid scannen

Naast beveiligingstests zijn vergunninghouders verplicht om toezicht te houden op de beveiliging van hun eigen systemen door middel van regelmatige kwetsbaarheidsscans. Het doel van kwetsbaarheidsscans is ervoor te zorgen dat de kansspelsystemen die de vergunninghouder gebruikt, geen externe beveiligingskwetsbaarheden vertonen die kunnen worden misbruikt om aanvallen op de kansspelsystemen uit te voeren.

De vergunninghouder is verplicht eenmaal per jaar een externe kwetsbaarheidsscan uit te voeren en de resultaten daarvan te rapporteren aan de toezichthoudende autoriteit. Het scannen op kwetsbaarheden kan worden uitgevoerd door een extern inspectieorgaan dat is geaccrediteerd overeenkomstig ISO/IEC 17025, ISO/IEC 17065 of ISO/IEC 17020, zoals gespecificeerd in lid 2 van deze verordening.

De vergunninghouder is verplicht kwetsbaarheden die tijdens het scannen van kwetsbaarheden aan het licht zijn gekomen, te verhelpen door middel van updates of andere dringende risicobeperkende maatregelen indien er geen corrigerende updates beschikbaar zijn. De in artikel 6 beschreven beoordelingsmethode wordt toegepast op beveiligingskwetsbaarheden die tijdens kwetsbaarheidsscans worden gedetecteerd. Als de berekende CVSS-waarde van de geïdentificeerde externe kwetsbaarheid hoger is dan 5,0, moet de vergunninghouder onmiddellijk maatregelen nemen om de kwetsbaarheden te verhelpen.

Het inspectieorgaan dat verantwoordelijk is voor het uitvoeren van de kwetsbaarheidsscan en zijn personeel moeten bekwaam en geschikt zijn om de tests uit te voeren. De nodige bekwaamheid om kwetsbaarheidsscans uit te voeren, kan onder meer worden aangetoond aan de hand van eerdere beroepservaring op het gebied van informatiebeveiligingstests, ervaring met het gebruik van kwetsbaarheidsscanners, opleiding of algemeen erkende sectorcertificaten. De vergunninghouder is verplicht ervoor te zorgen dat de personen die de tests uitvoeren, gekwalificeerd zijn om kwetsbaarheidsscans uit te voeren en, op verzoek, hun kwalificaties aan te tonen.

Er moet een persoon worden aangewezen die verantwoordelijk is voor het uitvoeren van de kwetsbaarheidsscan, om ervoor te zorgen dat deze juiste wordt uitgevoerd. Het definitieve rapport over de kwetsbaarheidsscan moet worden ondertekend en gevalideerd door de verantwoordelijke persoon en worden ingediend bij de toezichthoudende autoriteit.

8 Kwetsbaarheidsscans uitgevoerd in de context van informatiebeveiligingstesten

De vergunninghouder mag kwetsbaarheidsscans uitvoeren als onderdeel van informatiebeveiligingstests. Voor kwetsbaarheidsscans die worden uitgevoerd als onderdeel van informatiebeveiligingstests gelden dezelfde vereisten als voor andere kwetsbaarheidsscans.

9 Kwetsbaarheden verhelpen

De vergunninghouder is verplicht om regelmatig de informatiebeveiliging van zijn eigen kansspelsystemen te controleren, ook buiten informatiebeveiligingstests om, en om kwetsbaarheden die de betrouwbaarheid in gevaar brengen te verhelpen zodra er oplossingen of andere mitigerende methoden beschikbaar worden.

Als het niet mogelijk is om de kwetsbaarheden onmiddellijk te verhelpen, moet de vergunninghouder proberen om de beschikbare middelen te gebruiken om de kwetsbaarheden te bestrijden en de impact tot een minimum te herleiden.

Indien de CVSS v3-Base Score value van de gedetecteerde externe kwetsbaarheid minder dan 5.0 bedraagt, kan de vergunninghouder naar eigen goeddunken correcties doorvoeren en de urgentie van de noodzaak beoordelen.

10 Gebruik van afgegeven certificaten

Een geaccrediteerd inspectieorgaan dat is erkend door de toezichthoudende autoriteit die verantwoordelijk is voor het uitvoeren van informatiebeveiligingstests of kwetsbaarheidsscans, kan in het kader van haar inspectie certificaten of andere attesten gebruiken die aan de houder van de vergunning voor kansspelsoftware zijn verleend. Indien het inspectieorgaan in het kader van de inspectie bestaande certificaten gebruikt, moet het beoordelen of de certificaten kunnen worden beschouwd als voldoende betrouwbaar bewijs van de betrouwbaarheid en informatiebeveiliging van het kansspelsysteem van de houder van de vergunning voor kansspelsoftware.

11 Discrepanties

De vergunninghouder is verplicht om alle door hem geconstateerde inbreuken op de informatiebeveiliging of gegevensbescherming onverwijld aan de toezichthoudende autoriteit te melden indien er reden is om te vermoeden dat de betrouwbaarheid van de door de vergunninghouder gebruikte kansspelsystemen of loterijapparatuur in het gedrang is gekomen.

Vergunninghouders zijn niet verplicht om kleine incidenten op het gebied van beveiliging of gegevensbescherming te melden aan de toezichthoudende autoriteit voor kansspelen wanneer de geschatte effectiviteit van het incident beperkt is of wanneer het incident naar verwachting geen significante gevolgen heeft voor de betrouwbaarheid van kansspelsystemen.

12 Inwerkingtreding

Deze verordening treedt in werking met ingang van X [maand] 2026.

De Nationale Politieraad
Dienst kansspelen
Konepajankatu 2, PL 50, 11101 Riihimäki
Telefoon +358 295 480 181, poliisi.fi