**Verordnungsentwurf**

# Zuverlässigkeit und Informationssicherheit von Glücksspielsystemen nach dem Glücksspielgesetz

## Inhalt

# 1 Rechtsrahmen, Anwendungsbereich und Begriffsbestimmungen

## 1.1 Ermächtigung zum Erlassen von Vorschriften der Aufsichtsbehörde

Das Recht der Aufsichtsbehörde, verbindliche Vorschriften zu erlassen, beruht auf Abschnitt 44 Absatz 6 des Glücksspielgesetzes (xx/2025). Dieser Unterabschnitt ermächtigt die Aufsichtsbehörde, detailliertere Vorschriften zu erlassen. Diese Vorschriften betreffen die Zuverlässigkeit der Glücksspielsysteme, Lotterieausrüstung und Lotteriemethoden, die beim Betrieb von Glücksspielen verwendet werden. Außerdem betreffen sie die technischen Anforderungen zur Gewährleistung der Zufälligkeit der Ziehung. Weitere Vorschriften betreffen die detailliertere Form und den Inhalt der Untersuchung und Genehmigung durch die Prüfstelle. Schließlich betreffen sie auch die Bedingungen, die die Prüfstelle erfüllen muss, um von der Behörde zugelassen zu werden.

Gemäß Abschnitt 57 des Glücksspielgesetzes ist die Aufsichtsbehörde die finnische Aufsichtsbehörde. Gemäß Abschnitt 106 des Gesetzes fungiert das nationale Polizeiamt bis zum 31. Dezember 2026 als die in § 57 genannte zuständige Behörde.

## 1.2 Rechtsvorschriften

Die folgenden Vorschriften sind für den Gegenstand dieser Verordnung von Bedeutung:

- Glücksspielgesetz (xx/2025)
- Verwaltungsverfahrensgesetz (434/2003)
- Datenschutzgesetz (1050/2018)
- EU-Datenschutz-Grundverordnung (2016/679)

## 1.3 Geltungsbereich

Diese Bestimmung gilt für eine in Kapitel 1 Abschnitt 2 Absatz 1 des Glücksspielgesetzes genannte juristische oder natürliche Person, der nach dem Glücksspielgesetz eine ausschließliche Lizenz oder eine Lizenz für Glücksspielaktivitäten erteilt wurde.

Die ausschließliche Lizenz unterliegt Abschnitt 5 des Glücksspielgesetzes und die Glücksspiellizenz unterliegt Abschnitt 6.

## 1.4 Begriffsbestimmungen

In diesen Vorschriften gelten folgende Begriffsbestimmungen: Im Sinne der vorliegenden Verordnung gelten folgende Begriffsbestimmungen:

- *Ausschließliche Lizenz* ist eine Lizenz, die für die in Abschnitt 5 des Glücksspielgesetzes genannten Formen von Glücksspielen gewährt wird

- *Glücksspiellizenz* ist eine Lizenz, die für die in Abschnitt 6 des Glücksspielgesetzes genannten Arten von Glücksspielen erteilt wird
- *Glücksspieltransaktion* bedeutet den Einsatz, den der Spieler auf das Spiel setzt, die vom Spieler gewählte Ergebnisoption, die vom Spieler getroffenen Entscheidungen, die für das Ergebnis des Spiels und die Ergebnisse der Märkte und Ziehungen relevant sind, sowie alle Gewinne und Verluste, die im Glücksspielsystem des Inhabers einer exklusiven Lizenz oder Glücksspiellizenz verzeichnet sind
- *Spielerkontotransaktion* bedeutet Kontoeinträge.
- *Glücksspielsystem* bezeichnet ein Online-Informationssystem, das vom Glücksspielanbieter oder in dessen Auftrag für den Betrieb von Glücksspielen genutzt wird

## 2 Akkreditierung einer Kontrollstelle

Der Lizenzinhaber ist für die Zuverlässigkeit seiner Lotteriegeräte und Glücksspielsysteme sowie für die Durchführung von Audits zur Gewährleistung dieser Zuverlässigkeit verantwortlich. Die Bewertung der Zuverlässigkeit und Sicherheit wird von einer externen akkreditierten Kontrollstelle durchgeführt. Die Kontrollstelle muss nach der Verordnung (EG) Nr. 765/2008 des Europäischen Parlaments und des Rates über die Vorschriften für die Akkreditierung und Marktüberwachung im Zusammenhang mit der Vermarktung von Produkten und zur Aufhebung der Verordnung (EWG) Nr. 339/93 akkreditiert sein.

Die Akkreditierung kann Kontrollstellen durch die nationale Akkreditierungsstelle FINAS (Finnischer Akkreditierungsdienst) erteilt werden. Eine ausländische Akkreditierungsstelle kann auch als Akkreditierungsstelle fungieren, wenn sie Mitglied des Multilateralen Anerkennungsabkommens (EA MLA) der Europäischen Akkreditierungsorganisation im einschlägigen Zuständigkeitsbereich ist. Der Lizenzinhaber hat dafür zu sorgen, dass der externe Prüfer, der die Prüfung durchführt, über eine gültige Akkreditierung verfügt.

## 3 Allgemeine Praktiken der Informationssicherheit

Der Lizenzinhaber ist für die Informationssicherheit, den Datenschutz und andere technische Zuverlässigkeitsmerkmale seiner eigenen Glücksspielsysteme verantwortlich. Der Lizenzinhaber muss in seinem Betrieb gute Informationssicherheitspraktiken befolgen. Er muss sich bemühen, Bedrohungen der Informationssicherheit, Verletzungen des Datenschutzes sowie andere Probleme, die die Zuverlässigkeit von Glücksspielsystemen gefährden könnten, so gering wie möglich zu halten. Der Lizenzinhaber ist auch außerhalb der in dieser Verordnung genannten regelmäßigen Inspektionen dazu verpflichtet, die oben genannten Faktoren zu überwachen, um die Zuverlässigkeit seiner Systeme zu gewährleisten.

## 4 Kontrollstelle, die die Prüfung der Informationssicherheit durchführt

Der Lizenzinhaber ist verpflichtet, alle zwei Jahre Sicherheitstests an seinen Glücksspielsystemen durchzuführen. Das Ergebnis der Prüfung der Informationssicherheit wird der Aufsichtsbehörde vorgelegt. Die Prüfung der Informationssicherheit und ihr Ergebnis dürfen nicht älter als zwei Jahre sein.

Die Prüfung der Informationssicherheit wird durch eine externe Prüfstelle durchgeführt, die nach ISO/IEC 17025, ISO/IEC 17065 oder ISO/IEC 17020 akkreditiert ist, wie in Abschnitt 2 dieser Verordnung festgelegt. Bei der Prüfung der Informationssicherheit ist insbesondere auf den Schutz und die Integrität der Komponenten des Glücksspielsystems, das nach dem Zufallsprinzip funktioniert, sowie auf den Schutz von Komponenten, die personenbezogene Daten enthalten, und auf den Schutz zahlungsbezogener Komponenten zu achten.

Die für die Prüfung der Informationssicherheit zuständige Kontrollstelle und ihr Personal müssen für die Durchführung der Prüfungen kompetent und geeignet sein. Die für die Durchführung von Informationssicherheitstests erforderliche Kompetenz kann beispielsweise durch vorherige Berufserfahrung in diesem Bereich, durch Schulungen oder durch allgemein anerkannte Branchenzertifikate nachgewiesen werden. Der Lizenzinhaber ist verpflichtet, dafür zu sorgen, dass die Personen, die Prüfungen der Informationssicherheit durchführen, hierfür qualifiziert sind und ihre Qualifikationen auf Verlangen nachweisen können.

Für die Durchführung der Sicherheitsprüfung ist eine beauftragte Person zu bestellen, die für die ordnungsgemäße Durchführung verantwortlich ist. Der endgültige Bericht über die Prüfung der Informationssicherheit wird von der benannten Person unterzeichnet und validiert und der Aufsichtsbehörde vorgelegt.

Im Rahmen der Prüfung der Informationssicherheit sind mindestens die folgenden Komponenten sowie damit zusammenhängende Schwachstellen oder Vorfälle zu untersuchen:

- Möglichkeit der Manipulation der Zufallskomponenten
- Zugriff auf die Kundendatenbank
- Fähigkeit, den Ausgang von Spielen zu beeinflussen
- Fähigkeit, Zahlungssysteme oder Zahlungsvorgänge zu beeinflussen
- Unbefugter Zugriff auf Server, die zur Speicherung von Glücksspieltransaktionen und Spielerkontotransaktionen verwendet werden
- Möglichkeit, archivierte Daten zu Glücksspielereignissen oder Glücksspielkonten zu bearbeiten
- Änderung oder Vernichtung von Protokollen im Zusammenhang mit Glücksspielsystemen

### 4.1 Zuständigkeitsbereich

Die akkreditierte Kontrollstelle, die die Prüfung durchführt, muss in ihrer ISO/IEC-Akkreditierung über den Kompetenzbereich für Glücksspiele verfügen. Der Zuständigkeitsbereich muss die durch das finnische Glücksspielrecht und die technischen Vorschriften der Aufsichtsbehörde festgelegten Anforderungen abdecken.

Bis zum 1. Januar 2027 kann die Aufsichtsbehörde eine Akkreditierung akzeptieren, die einen Kompetenzbereich umfasst, welcher auf Basis technischer Vorschriften für die dänischen bzw. schwedischen Glücksspielsysteme bewertet und erteilt wurde.

## 5 Erneuerung der Prüfung der Informationssicherheit

Der Lizenzinhaber legt der Aufsichtsbehörde die Ergebnisse der genehmigten Prüfung der Informationssicherheit vor. Der Lizenzinhaber darf den Betrieb von Glücksspielen nicht beginnen, bevor er die Sicherheitsprüfung erfolgreich bestanden hat. Das Ergebnis der Prüfung der Informationssicherheit darf nicht älter als zwei Jahre sein.

Die Aufsichtsbehörde kann nach eigenem Ermessen zusätzliche Zeit für die Durchführung von Sicherheitsprüfungen gewähren. Während dieser Zeit kann der Betrieb von Glücksspielen fortgesetzt werden.

## 6 Abgelehnte Prüfung der Informationssicherheit

Die Inspektionsstelle, die die Prüfung der Informationssicherheit durchführt, sollte die dabei festgestellten Schwachstellen sowie deren Bedeutung für die Zuverlässigkeit des Glücksspielsystems bewerten. Die bei der Bewertung festgestellten Schwachstellen sollten mit dem vom Nationalen Technologieinstitut (NIST) bereitgestellten Rechner CVSS v3 (Common Vulnerability Scoring System Calculator Version 3) bewertet werden. Für den CVSS v3-Rechner wird die Schwere der Schwachstelle anhand von Grundpunktmetriken bewertet. Wenn während des Sicherheitstests Schwachstellen mit einem berechneten CVSS-Wert über 5,0 erkannt werden, kann der Test nicht als erfolgreich angesehen werden.

Wird der Test des Lizenzinhabers zur Überprüfung der Informationssicherheit nicht genehmigt, muss der Lizenzinhaber unverzüglich Maßnahmen ergreifen, um die festgestellten Schwachstellen in der Informationssicherheit zu beheben. Der Lizenzinhaber muss den abgelehnten Informationssicherheitstest der Aufsichtsbehörde melden.

Der Lizenzinhaber muss innerhalb von 90 Tagen nach dem abgelehnten Informationssicherheitstest einen neuen Sicherheitstest durchführen. Eine erneute Prüfung der Informationssicherheit muss nicht am gesamten Glücksspielsystem durchgeführt werden, sondern kann die Prüfung der Informationssicherheit auf die Mängel abzielen, die die Ablehnung verursacht haben. Im Rahmen der erneuten

Prüfung der Informationssicherheit muss die Prüfstelle gewährleisten, dass die zuvor als Ablehnungsgrund ermittelten Schwachstellen behoben wurden.

Die Durchführung von Glücksspielen darf nicht beginnen, bevor genehmigte und gültige Sicherheitstests durchgeführt wurden.

## 7 Schwachstellenscanning

Zusätzlich zu den Sicherheitsprüfungen sind die Lizenzinhaber verpflichtet, die Sicherheit ihrer eigenen Systeme durch regelmäßige Schwachstellenscans zu überwachen. Der Zweck von Schwachstellenscans besteht darin, sicherzustellen, dass die vom Lizenzinhaber verwendeten Glücksspielsysteme keine externen Sicherheitslücken aufweisen, die für Angriffe auf die Glücksspielsysteme ausgenutzt werden könnten.

Der Lizenzinhaber ist verpflichtet, einmal jährlich eine externe Schwachstellenanalyse durchzuführen und die Ergebnisse der Aufsichtsbehörde zu melden. Die Schwachstellensuche kann von einer externen Prüfstelle durchgeführt werden, die gemäß ISO/IEC 17025, ISO/IEC 17065 oder ISO/IEC 17020 akkreditiert ist, wie in Absatz 2 dieser Verordnung festgelegt.

Der Lizenzinhaber ist verpflichtet, beim Scannen auf Schwachstellen festgestellte Sicherheitslücken durch Updates oder andere dringende Abhilfemaßnahmen zu beheben, wenn keine korrigierenden Updates verfügbar sind. Die in Abschnitt 6 beschriebene Bewertungsmethode ist auf Sicherheitslücken anzuwenden, die bei Schwachstellenscans entdeckt wurden. Wenn der berechnete CVSS-Wert der identifizierten externen Schwachstelle 5,0 überschreitet, muss der Lizenzinhaber unverzüglich Maßnahmen zur Behebung der Schwachstellen ergreifen.

Die für die Durchführung des Schwachstellenscans zuständige Kontrollstelle und ihr Personal müssen für die Durchführung der Tests kompetent und geeignet sein. Die erforderliche Kompetenz zur Durchführung von Schwachstellenscans kann unter anderem durch Berufserfahrung in Informationssicherheitstests, Erfahrung mit dem Einsatz von Schwachstellenscannern, entsprechende Schulungen oder allgemein anerkannte Branchenzertifikate nachgewiesen werden. Der Lizenzinhaber ist verpflichtet, sicherzustellen, dass die Personen, die die Prüfungen durchführen, für die Durchführung von Schwachstellenscans qualifiziert sind, und auf Verlangen ihre Qualifikationen nachzuweisen.

Es muss eine Person benannt werden, die für die Durchführung der Prüfung der Schutzbedürftigkeit zuständig ist, um sicherzustellen, dass sie ordnungsgemäß durchgeführt wird. Der endgültige Bericht über die Schwachstellenanalyse muss von der verantwortlichen Person unterzeichnet und validiert und der Aufsichtsbehörde vorgelegt werden.

## 8 Im Zusammenhang mit der Prüfung der Informationssicherheit durchgeführte Schwachstellenscans

Der Lizenzinhaber kann im Rahmen von Informationssicherheitstests Schwachstellenscans durchführen. Für Schwachstellenscans, die im Rahmen von Informationssicherheitstests durchgeführt werden, gelten die gleichen Anforderungen wie für andere Schwachstellenscans.

## 9 Beheben von Schwachstellen

Der Lizenzinhaber ist verpflichtet, die Informationssicherheit seiner Glücksspielsysteme auch außerhalb von Tests zur Informationssicherheit regelmäßig zu überwachen. Er muss Schwachstellen, die die Zuverlässigkeit beeinträchtigen, umgehend beheben, sobald Korrekturen oder andere Abhilfemaßnahmen verfügbar sind.

Wenn es nicht möglich ist, die Schwachstellen unverzüglich zu beheben, hat der Lizenzinhaber sich darum zu bemühen, die verfügbaren Mittel zu nutzen, um die Schwachstellen zu bekämpfen und die Auswirkungen zu minimieren.

Liegt der CVSS-v3-Basiswert der erkannten externen Schwachstelle unter 5,0, kann der Lizenznehmer Korrekturen nach eigenem Ermessen vornehmen und die Dringlichkeit der erforderlichen Maßnahmen beurteilen.

## 10 Verwendung der ausgestellten Bescheinigungen

Eine akkreditierte Kontrollstelle, die von der für die Durchführung von Informationssicherheitsprüfungen oder Schwachstellenanalysen zuständigen Aufsichtsbehörde zugelassen wurde, kann im Rahmen ihrer Inspektion Zertifikate oder andere Bescheinigungen verwenden, die dem Lizenzinhaber für Glücksspielsoftware ausgestellt wurden. Verwendet die Kontrollstelle im Rahmen der Kontrolle vorhandene Zertifikate, muss sie prüfen, ob diese als hinreichend zuverlässiger Nachweis für die Zuverlässigkeit und Informationssicherheit des Glücksspielsystems des Lizenzinhabers der Glücksspielsoftware angesehen werden können.

## 11 Abweichungen

Der Lizenzinhaber ist verpflichtet, alle von ihm festgestellten Verstöße gegen die Informationssicherheit oder den Datenschutz unverzüglich der Aufsichtsbehörde zu melden, sofern Grund zu der Annahme besteht, dass die Zuverlässigkeit der von ihm verwendeten Glücksspielsysteme oder Lotterieausrüstungen beeinträchtigt wurde.

Die Lizenzinhaber sind nicht verpflichtet, geringfügige Sicherheits- oder Datenschutzvorfälle der Glücksspielaufsichtsbehörde zu melden, wenn die geschätzte Wirksamkeit des Vorfalls begrenzt ist oder wenn nicht davon ausgegangen wird, dass der Vorfall erhebliche Auswirkungen auf die Zuverlässigkeit der Glücksspielsysteme hat.

## 12 Inkrafttreten

Diese Verordnung tritt am X [Monat] 2026 in Kraft.

**Nationales Polizeiamt**
**Glücksspielverwaltung**
Konepajankatu 2, PL 50, 11101 Riihimäki
Telefonnummer +358 295 480 181, poliisi.fi