Draft Regulation

Reliability and information security of gambling systems under the Gambling Act

Contents

1 Legal framework, scope and definitions

1.1 The supervisory authority's power to issue orders

The right of the supervisory authority to issue a binding order is based on section 44(6) of the Gambling Act (xx/2025). According to said subsection, the supervisory authority may issue more detailed regulations on the reliability of the gambling systems, lottery equipment and lottery methods used in the operation of gambling, on the technical requirements for ensuring the randomness of the draw, on the more detailed form and content of the inspection body's investigation and approval, and on the conditions that the inspection body must meet in order to be approved by the Authority.

According to Section 57 of the Gambling Act, the Supervisory Authority is the Finnish Supervisory Agency. According to section 106 of the Act, the National Police Board shall act as the competent authority referred to in section 57 until 31 December 2026.

1.2 Legislation

The following regulations are relevant to the subject matter of this order:

- Gambling Act (xx/2025)
- Administrative Procedure Act (434/2003)
- Data Protection Act (1050/2018)
- EU General Data Protection Regulation (2016/679)

1.3 Scope

This provision applies to a legal or natural person referred to in Chapter 1, Section 2(1) of the Gambling Act to whom an exclusive licence or a licence for gambling activities has been granted under the Gambling Act.

The exclusive licence is governed by Section 5 of the Gambling Act and the gambling licence is governed by Section 6.

1.4 Definitions

For the purposes of this provision, the following definitions shall apply. For the purposes of this regulation:

- *exclusive licence* means a licence granted for the forms of gambling referred to in section 5 of the Gambling Act
- *gambling licence* means a licence granted for the types of gambling referred to in section 6 of the Gambling Act

- *gambling transaction* means the stake wagered by the player on the game, the outcome option chosen by the player, the choices made by the player which are relevant to the outcome of the game and the results of the markets and draws, as well as any winnings and losses recorded in the gambling system of the holder of an exclusive licence or gambling licence
- *player account transaction* means account entries.
- *gambling system* means an online information system used by or on behalf of the gambling operator for the operation of gambling

2 Accreditation of an inspection body

The licence holder is responsible for the reliability of its lottery devices and gambling systems, as well as for carrying out the audits conducted to ensure that reliability. The assessment of reliability and security is carried out by an external accredited inspection body. The inspection body shall be accredited within the meaning of Regulation (EC) No 765/2008 of the European Parliament and of the Council setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93.

Accreditation can be granted to inspection bodies by the national accreditation body FINAS (Finnish Accreditation Service). A foreign accreditation body may also act as an accreditation body if it is a member of the European Accreditation Organisation's Multi-lateral Recognition Agreement (EA MLA) in the relevant field of competence. The licence holder is obliged to ensure that the external operator carrying out the audit has a valid accreditation.

3 General information security practices

The licence holder is responsible for the information security, data protection and other technical reliability features of its own gambling systems. The licence holder must follow good information security practices in their operations and strive to minimise information security threats, data breaches and other problems that could jeopardise the reliability of gambling systems. The licence holder is also obliged to monitor the above-mentioned factors outside regular inspections referred to in this Regulation, in order to ensure the reliability of its systems.

4 Inspection body conducting information security testing

The licence holder is obliged to carry out security testing on its gambling systems every two years. The outcome of the information security testing shall be submitted to the supervisory authority. Information security testing and its outcome may not be older than two years.

The information security testing shall be carried out by an external inspection body accredited in accordance with ISO/IEC 17025, ISO/IEC 17065 or ISO/IEC 17020, as specified in section 2 of this Regulation. Information security testing shall pay particular attention to the protection and integrity of the random gambling system components, to the protection of components containing personal data, and to the protection of payment-related components.

The inspection body responsible for carrying out information security testing and its personnel shall be competent and suitable to carry out the tests. The necessary competence to carry out information security tests can be demonstrated by, among other things, previous professional experience in information security testing, training or generally recognised industry certificates. The licence holder is obliged to ensure that the persons performing the testing are qualified to perform information security testing and, upon request, to demonstrate their qualifications.

A designated person shall be appointed for the implementation of security testing, who shall be responsible for the appropriate implementation. The final information security test report shall be signed and validated by the designated person and submitted to the supervisory authority.

In the context of information security testing, at least the following components, as well as related vulnerabilities or incidents, shall be tested:

- Possibility of manipulation of the random components
- Access to the customer database
- Ability to influence the outcome of games
- Ability to influence payment systems or payment transactions
- Unauthorised access to servers used to store gambling transactions and player account transactions
- Ability to edit archived gambling event or gambling account event data
- Modification or destruction of logs relating to gambling systems

4.1 Area of competence

The accredited inspection body carrying out the audit shall have the area of competence for gambling in its ISO/IEC accreditation. The area of competence must cover the requirements set by Finnish gambling legislation and the technical regulations of the supervisory authority.

Until 1 January 2027, the supervisory authority may accept accreditation that includes a scope of competence assessed and granted on the basis of technical regulations issued for the Danish or Swedish gambling systems.

5 Renewal of information security testing

The licence holder shall submit the results of the approved information security testing to the supervisory authority. The licence holder may not commence the operation of gambling before it has successfully passed security testing. The outcome of the information security test shall not be more than two years old.

The supervisory authority may, at its discretion, grant additional time for the implementation of security testing, during which the operation of gambling may continue.

6 Rejected information security test

The inspection body carrying out the information security test should assess the vulnerabilities identified during the information security testing and their importance for the reliability of the gambling system. The vulnerabilities identified during the assessment should be assessed using the CVSS v3 (Common Vulnerability Scoring System Calculator version 3) calculator provided by the National Institute of Technology (NIST). For the CVSS v3 calculator, the severity of vulnerability shall be assessed using Base Score Metrics. If vulnerabilities with a calculated CVSS value higher than 5.0 are detected during security testing, the test cannot be considered successful.

If the licence holder's information security test is not approved, the licence holder must immediately take measures to remedy the identified information security vulnerabilities. The licence holder shall report the rejected information security test to the supervisory authority.

The licence holder must carry out a new security test within 90 days of the rejected information security test. Renewed information security testing does not need to be carried out on the entire gambling system; instead, information security testing can be targeted at the deficiencies that caused the rejection. In connection with the renewed information security testing, the inspection body must ensure that the vulnerabilities previously identified as grounds for rejection have been corrected.

The implementation of games of chance may not commence before approved and valid security testing has been carried out.

7 Vulnerability scanning

In addition to security testing, licence holders are obliged to monitor the security of their own systems by means of regular vulnerability scans. The purpose of vulnerability scans is to ensure that the gambling systems used by the licence holder do not have any external security vulnerabilities that could be exploited to carry out attacks against the gambling systems.

The licence holder is obliged to carry out an external vulnerability scan once a year and report the results to the supervisory authority. Vulnerability scanning may be carried out by an external inspection body accredited in accordance with ISO/IEC 17025, ISO/IEC 17065 or ISO/IEC 17020, as specified in paragraph 2 of this Regulation.

The licence holder is obliged to fix vulnerabilities detected during vulnerability scanning with updates or other urgent mitigation measures if corrective updates are not available. The assessment method described in section 6 shall be applied to security vulnerabilities detected during vulnerability scans. If the calculated CVSS value of the identified external vulnerability exceeds 5.0, the licence holder shall take immediate action to remedy the vulnerabilities.

The inspection body responsible for conducting the vulnerability scan and its personnel must be competent and suitable for conducting the tests. The necessary competence to carry out vulnerability scans can be demonstrated by previous professional experience in information security testing, experience in the use of vulnerability scanners, training or generally recognised industry certificates, among others. The licence holder is obliged to ensure that the persons performing the testing are qualified to perform vulnerability scans and, upon request, to demonstrate their qualifications.

A person responsible for carrying out the vulnerability scan must be appointed to ensure that it is carried out appropriately. The final vulnerability scan report shall be signed and validated by the responsible person and submitted to the supervisory authority.

8 Vulnerability scans performed in connection with information security testing

The licence holder may carry out vulnerability scans as part of information security testing. The same requirements apply to vulnerability scans performed as part of information security testing as to other vulnerability scans.

9 Fixing vulnerabilities

The licence holder is obliged to regularly monitor the information security of its own gambling systems, even outside of information security tests, and to fix vulnerabilities that compromise reliability when fixes or other mitigation methods become available.

If it is not possible to promptly remedy the vulnerabilities, the licence holder shall seek to use available means to combat the vulnerabilities and minimise the impact.

If the CVSS v3 Base Score value of the detected external vulnerability is less than 5.0, the licence holder may use their own discretion in implementing corrections and assessing the urgency of the need for them.

10 Use of issued certificates

An accredited inspection body approved by the supervisory authority responsible for conducting information security testing or vulnerability scanning may use certificates or other attestations granted to the gambling software licence holder as part of its inspection. If the inspection body uses existing certificates as part of the inspection, it must assess whether the certificates can be considered sufficiently reliable evidence of the reliability and information security of the gambling software licence holder's gambling system.

11 Discrepancies

The licence holder is obliged to report any information security or data protection breaches they detect to the supervisory authority without delay if there is reason to suspect that the reliability of the gambling systems or lottery equipment used by the licence holder has been compromised.

Licence holders shall not be required to report minor security or data protection incidents to the gambling supervisory authority where the estimated effectiveness of the incident is limited in nature or where the incident is not assessed to have a significant impact on the reliability of gambling systems.

12 Entry into force

This Regulation shall enter into force on X [month] 2026.

The National Police Board
Gambling administration
Konepajankatu 2, PL 50, 11101 Riihimäki
Telephone +358 295 480 181, poliisi.fi