POLIISI

Regulation
26 February 2026
Document: ID-26138756 Subject: POL-2026-27824

Period of validity
1 March 2026

Legal basis
Gambling Act (10/2026) Section 44

Amends/Repeals
-

Target groups
-

Reliability and data security of gaming systems in accordance with the Gaming Act

Contents

1 Regulatory background, scope of application and definitions

1.1 Regulatory authority's power to issue orders

The supervisory authority's right to issue a binding order is based on Section 44(6) of the Gaming Act (10/2026). According to the aforementioned subsection, the supervisory authority may issue more detailed orders concerning the reliability of gaming systems, lottery equipment and lottery methods used in the implementation of gambling, the technical requirements for ensuring the randomness of lottery results, the more detailed form and content of the investigation and approval carried out by the inspection body, and the conditions that the inspection body must meet in order for the authority to approve it.

According to Section 57 of the Gaming Act, the supervisory authority is the Licensing and Supervisory Authority. 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 provision:

- Gambling Act (10/2026)
- Administrative Procedure Act (434/2003)
- Data Protection Act (1050/2018)
- EU General Data Protection Regulation (2016/679)

1.3 Scope

This provision applies to legal persons or natural persons referred to in Chapter 1, Section 2, Paragraph 1 of the Gaming Act who have been granted an exclusive licence or a gaming licence under the Gaming Act.

Exclusive licences are provided for in section 5 of the Gaming Act and gaming licences in section 6.

1.4 Definitions

The following definitions are used in this regulation. In this regulation, the following terms have the following meanings:

- an exclusive licence granted for the forms of gambling referred to in section 5 of the Gambling Act
- a gambling licence granted for the forms of gambling referred to in section 6 of the Gambling Act
- a gaming event: the stake placed by the player, the outcome option selected by the player, the choices made by the player that are relevant to the outcome of the game, and the object- and the results of the draw and any winnings and losses recorded in the gaming system of the holder of the exclusive licence or gaming licence

- gaming account transaction: entries in the gaming account
- gaming system means an electronic information system used by or on behalf of the gaming operator in the operation of games of chance

2 Accreditation of the inspection body

The licence holder is responsible for the reliability of its lottery equipment and gaming systems and for conducting audits to ensure reliability. The reliability and security assessment is carried out by an external accredited inspection body. The inspection body must be accredited in accordance with Regulation (EC) No 765/2008 of the European Parliament and of the Council setting out the requirements for accreditation and repealing Regulation (EEC) No 339/93.

Accreditation for inspection bodies may be granted 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 Multilateral Recognition Agreement (EA MLA) in the relevant field of competence. The licence holder is obliged to ensure that the external body conducting the audit has 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 gaming systems. The licence holder must follow good information security practices in their operations and strive to minimise information security threats, data breaches and other issues that could compromise the reliability of gaming systems. The licence holder is also obliged to monitor the above factors outside the regular inspections referred to in this regulation in order to ensure the reliability of its systems.

4 Inspection body as the implementer of information security testing

The licence holder is obliged to carry out information security testing on its gaming systems every two years. The results of the information security testing must be submitted to the supervisory authority. Information security testing and its results must not be more than two years old.

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. In information security testing, particular attention shall be paid to the protection and integrity of components that generate randomness in the gaming system, the protection of components containing personal data, and the protection of components related to payments.

The inspection body responsible for carrying out the security testing and its personnel must be competent and suitable for carrying out the tests. The necessary competence to carry out security tests can be demonstrated, for example, by previous work experience.

information security testing, training or generally recognised industry certifications. The data controller is obliged to ensure that the persons performing the testing are competent to perform information security testing and, upon request, to demonstrate their competence.

A person responsible for the implementation of information security testing must be appointed to ensure that it is carried out appropriately. The person responsible must sign and confirm the final report on the information security testing, which must be submitted to the supervisory authority.

The information security testing must cover at least the following components and any related vulnerabilities or deviations:

- Possibility of manipulation of 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 game events and game account events
- Ability to modify archived game event or game account event data
- Modification or destruction of logs related to gaming systems

4.1 Scope of competence

The accredited inspection body conducting the audit must have a scope of accreditation covering gambling in its ISO/IEC accreditation. The scope of accreditation must cover the requirements set out in 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 the technical regulations issued for the Danish or Swedish gambling systems.

5 Renewal of information security testing

The licence holder must submit the results of an approved information security test to the supervisory authority. The licence holder may not commence the operation of gambling services before passing the information security test. The results of the information security test must not be more than two years old.

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

6 Failed security test

The inspection body conducting the information security testing must assess the vulnerabilities identified in the information security testing and their significance for the reliability of the gaming system. The vulnerabilities identified in the assessment must be assessed in accordance with NIST (National

Institute of Technology) using the CVSS v3 (Common Vulnerability Scoring System Calculator version 3) calculator. For the CVSS v3 calculator, the severity of the vulnerability must be assessed using Base Score Metrics. If vulnerabilities with a calculated CVSS value of more than 5.0 are detected during the security testing, the inspection cannot be considered passed.

If the licence holder's security testing is not approved, the licence holder must take immediate action to remedy the security vulnerabilities detected. The licence holder must report the failed security test to the supervisory authority.

The licence holder must carry out a new information security test within 90 days of the failed information security test. The new information security test does not need to be carried out on the entire gaming system; instead, the information security test can be targeted at the deficiencies that led to the failure. In connection with the renewed information security test, the inspection body must ensure that the vulnerabilities previously identified as leading to the failure have been corrected.

The implementation of gambling games may not begin before an approved and valid security test has been carried out.

7 Vulnerability scanning

In addition to information security testing, licence holders are required to monitor the security of their own systems through regular vulnerability scanning. The purpose of vulnerability scans is to ensure that the gaming systems used by the licence holder do not have any external information security vulnerabilities that could be exploited to carry out attacks on the gaming systems.

The licence holder is obliged to carry out an external vulnerability scan once a year and report on it to the supervisory authority. The vulnerability scan may be carried out by an external inspection body accredited in accordance with section 2 of this regulation in accordance with the ISO/IEC 17025, ISO/IEC 17065 or ISO/IEC 17020 standards.

The licence holder is obliged to fix any vulnerabilities found during the vulnerability scan with updates or other urgent mitigation measures if no corrective updates are available. The assessment method described in section 6 shall be applied to information security vulnerabilities detected during vulnerability scans. If the calculated CVSS value of a detected external vulnerability is greater than 5.0, the licence holder must take immediate action to fix the vulnerabilities.

The inspection body responsible for performing the vulnerability scan and its personnel must be competent and suitable for performing the tests. The necessary competence to perform vulnerability scans can be demonstrated, for example, by previous work experience in information security testing, experience in using vulnerability scanners, training or generally recognised industry certifications. The licence holder is obliged to ensure that the persons performing the testing are competent to perform vulnerability scans and, upon request, to demonstrate their competence.

A person responsible for the proper implementation of the vulnerability scan must be appointed. The person responsible must sign and confirm the final report of the vulnerability scan, which must be submitted to the supervisory authority.

8 Vulnerability scanning carried out in connection with information security testing

The licence holder may carry out a vulnerability scan as part of information security testing. The same requirements apply to vulnerability scans carried out in connection with information security testing as to other vulnerability scans.

9 Fixing vulnerabilities

The licence holder is obliged to regularly monitor the security of its own gaming systems, even outside of security testing, and to fix vulnerabilities that compromise reliability as soon as fixes or other mitigation methods become available.

If it is not possible to fix vulnerabilities quickly, the licence holder must endeavour to use the means available to combat vulnerabilities and minimise their impact.

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

10 Use of issued certificates

An accredited inspection body approved by the supervisory authority and responsible for conducting information security testing or vulnerability scanning may utilise certificates or other attestations issued to the gaming software licence holder as part of its inspection. If the inspection body utilises 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 gaming software licence holder's gaming system.

11 Deviations

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

Licence holders are not required to report minor deviations related to information security or data protection to the gambling supervisory authority if the estimated impact of the deviation is minor in nature or if the deviation is not estimated to have a significant impact on the reliability of the gaming systems.

12 Entry into force

This regulation shall enter into force on 1 March 2026.

Ilkka Koskimäki, Chief Superintendent

Anna Hyppönen, Head of Lottery Administration

This document has been electronically signed in the case management system. Police 26 February 2026 at 13:32. The authenticity of the signature can be verified at the registry.

National Police Board Lottery Administration
Konepajankatu 2, PO Box 50, 11101 Riihimäki
Telephone +358 295 480 181, poliisi.fi