208/2017 Coll.

DECREE

date 27 June 2017,

which establishes the scope of technical parameters for devices through which games of chance are operated and requirements for the protection and preservation of gaming and financial data and their technical parameters

In accordance with Section 133, Para. 1 b) of Act No. 186/2016 Coll., on Gambling, the Ministry of Finance hereby establishes:

PART ONE
INTRODUCTORY PROVISIONS

Section 1
Subject Matter of Legislation

(1) This Decree establishes the scope of technical parameters for devices through which games of chance are operated and requirements for the protection and preservation of gaming and financial data and their technical parameters.

PART TWO
GENERAL REQUIREMENTS

Section 2
Devices through which Games of Chance are Operated

(1) A device through which a game of chance is operated (hereinafter referred to as a "device") consists of a coherent set of hardware and software of a gaming operator, which is used for carrying out activities pursuant to Section 5 of the Gambling Act.

(2) A device must contain server used to manage activities pursuant to Section 5 of the Gambling Act, and enabling the storage of financial and gaming data (hereinafter referred to as the "server"). For the identification of the server, the conditions set out in Section 8 shall apply similarly.

(3) Devices through which lottery, bingo, technical game, live game or internet games, in which winning or losing is decided wholly or partially by chance, must contain a random number generator (hereinafter referred to as a "random number generator").

Section 3
Protection and Preservation of Gaming and Financial Data

A device and the method with which an operator of games of chance handles the gaming and financial data contained within it must meet the technical requirements for an information security management system stipulated in ČSN ISO/IEC 27001:2014, unless this Decree or the Gambling Actstipulate otherwise.

Section 4

Location of Server

(1) Server must be located in a specialised space designed for locating information and communications technology in continuous operation and which provides the server with stable operation without ambient influences (hereinafter referred to as a "data centre").

(2) To ensure the physical safety of the server, an operator of games of chance shall take the following measures in the data centre

a) provision of security on the floor of the building in which the data centre is located,
b) prevention of unauthorised access to the data centre,
c) prevention of damage to and interference with the data centre and
d) prevention of damage to, theft or misuse of the server or the interruption of its operation.

(3) In particular, an operator of games of chance shall use the following means of physical security for the measures to ensure the physical security of the data centre pursuant to paragraph 2

a) mechanical barriers,
b) electric security alarms,
c) devices limiting the effects of fire,
d) devices limiting the effects of natural disasters,
e) access control systems,
f) CCTV,
g) equipment for protecting against power failures,
h) equipment for ensuring optimal operating conditions.

Section 5

Random Number Generator

(1) A random number generator that is the source of coincidence in a device pursuant to Section 2 (3) is either a stand-alone device component or an integrated part of a server or terminal device. For the identification of a stand-alone random number generator, the conditions set out in Section 8 shall apply mutatis mutandis.

(2) A random number generator must be such that

a) the random process determining the outcome of a game cannot be influenced and
b) the outcome of the random process
    1. is independent of previous outcomes,
    2. corresponds in the likelihood of attaining individual possible outcomes of a game of chance to theoretical probabilities and
    3. is unpredictable without complete knowledge of the process of determining the outcome of a game, including all settings and initial values.

(3) A random number generator which uses a deterministic algorithm to determine the outcome of a game must

a) operate with a cycle duration of at least 2^{64} ensuring the generation of a random process in such a way that, in the case of a specific game of chance, there is no discernible repetition of outcomes,
b) create a sequence of game outcomes based on initial values which are random or unpredictable, and
c) be an integral part of a server or terminal.

(4) A random number generator which uses a deterministic algorithm to determine the outcome of a game, in the event that it uses

a) macroscopic elements, in particular dice, roulette wheels or lottery draw machines, must use items made of an unalterable material which are not subject to wear during regular use, in order to ensure a random process of creating game outcomes,
b) microscopic elements, especially noises or quantum phenomena, be an integral part of a server or terminal.

(5) If when determining the outcome of a game based on a range of values of a generated sequence of random numbers, further processing of the outcomes of the random process occurs, the software designed for this purpose must be a part of server or a terminal, and it must be ensured that this processing meets the requirements stipulated for the outcome of a random process in paragraph 2.

Section 6
Cryptographic Tools

For the transmission and storage of gaming and financial data, and access to a device's software, the device must use cryptographic algorithms and cryptographic keys which meet the minimum requirements for cryptographic algorithms specified in the Annex to this Decree, so as to ensure the immutability and confidentiality of the gaming and financial data and the device's software.

Section 7
Storage of Gaming and Financial Data

(1) Devices must contain such equipment for in order to prevent its loss. The storing of gaming and financial data for the purposes of this Decree means the data storage and backup.

(2) An operator is required, in order to comply with the obligation under paragraph 1, to back up gaming and financial data stored on the server in order to ensure the complete restoration of game and financial data, in particular to ensure that game and financial data are backed up at a sufficient distance from the data center or otherwise, so that a backup set of financial and game data can not be lost for the same reason that loss of game and financial data stored on the server may occur.

PART THREE
REQUIREMENTS FOR TERMINALS OPERATED IN A GAMING AREA

Section 8
Identification of Terminals

(1) Terminals must be marked with a unique identification label in the form of a registration stamp issued by an authorised person.

(2) The registration stamp must be firmly attached to the front or side of the terminal's outer casing, so that it is visible.

Section 9
External Security of Terminals

(1) Terminals must be constructed so as to prevent violent or otherwise unauthorised entry into a terminal with the use of force of such an intensity as can be reasonably expected during normal operation.

(2) Terminals must be equipped with a sensor or other security device which records attempts at violent or otherwise unauthorised entry into a terminal, disconnection, interference with the power or data cables, or otherwise interfering with its operation. The sensor or other security device must also record all authorised entry in to the outer lockable part of a terminal.

(3) If an attempt is made to enter a terminal in a violent or otherwise unauthorised manner, to disconnect or interfere with its power or data cables, or to otherwise interfere with its operation, the terminal must automatically switch to error status, which shall mean a condition under which it is not permitted to play a technical game or to make another kind of transaction in a user account.

(4) If the sensor or other security device no longer indicates the necessity to maintain the error status, the terminal's operations may be automatically resumed.

(5) Terminals must be equipped with a system which informs the gaming area's attendant (hereinafter referred to as the "attendant") of the continuation of the error status if it is not possible to resume the terminal's operations automatically pursuant to paragraph 4. In the event of a continued error status, a terminal's operations can only be resumed with the authorised intervention of the attendant. If, following the authorised intervention of the attendant, the error status cannot be immediately cancelled, the attendant shall pay out a win to the player after verifying the amount on the appropriate electronic indicators and the player shall log out from his/her user account. This shall not affect the provisions of paragraph 3.

Section 10
Internal Security of Terminals

(1) All parts of a terminal whose manipulation could affect the random process of a game's outcome, the remote transmission of a game's outcome, or the preservation of gaming and financial data and its remote transmission to the server must be located in an internal separately lockable part of the terminal.

(2) The internal separately lockable part must contain at least

a) software used to control the operation of the terminal,
b) a random number generator, if the terminal is equipped with it,,
c) electronic components ensuring a telecommunications data connection with the device's server,
d) electronic components containing a system for displaying a game,
e) electronic components containing a system for recording finances, and
f) a repository for banknotes and coins.

(3) If a terminal contains a random number generator, the internal separately lockable part must also contain counter systems.

(4) The requirement for placement inside an internal separately lockable part of a terminal pursuant to paragraphs 1 to 3 does not apply to a random number generator which is also used for displaying a winning combination or other outcome of a game or to a counter system if it is functionally indivisible from the random number generator. Such a part of a terminal must meets the conditions for external security pursuant to Section 9.

(5) A repository for banknotes and coins must be located inside an internal separately lockable part designed exclusively for this purpose.

(6) Internal separately lockable parts must be equipped with independent protection which meets the conditions of Section 9.

Section 11

Display Devices

(1) Each gaming position must be fitted with a screen or other display device.

(2) If a gaming position is equipped with a touch screen, the screen must be accurate and must not contain any hidden or unlabelled buttons or touch points which could affect the game, with the exception of cases specified in the game plan.

(3) A terminal which contains a random number generator which also serves for displaying a winning combination or other outcome of a game, or a mechanical or electromechanical part serving exclusively for displaying a winning combination or other outcome of a game, must be designed in such a way that the displayed outcomes match the indicators on the gaming position's screen. If this is not the case, the terminal must automatically switch to error status.

Section 12

Telecommunications Data Connection

(1) Each terminal must be equipped with a telecommunications data connection used to transmit gaming and financial data for individual gaming positions after each technical game has been played.

(2) A terminal which does not contain a random number generator must be equipped with a telecommunications connection which operates with a response time of less than 0.3 seconds when transmitting the outcome of a game.

Section 13

Printer

(1) Every terminal must be equipped with a printer or be connected to a printer. After a button located on the touch screen or outer casing of a terminal is pressed, the printer must allow for proof of the user's account balance to be printed.

(2) Proof of the user's account balance must contain at least

a) identification details of the operator,
b) identification of the establishment,
c) the production number of the gaming position,
d) identification information of the player,
e) the date and time of printing, and
f) a unique identifier of the proof of the user's account balance.

(3) The screen of a playing position on a terminal must display information if an event or error which prevents printing occurs.

Section 14

Counter Systems

(1) A terminal which contains a random number generator must be fitted with at least two counter systems independent of one another, namely

a) electronic and
b) electromechanical or pulse,

which record the totals of individual groups of gaming and financial data intended for storage on site.

(2) Counter system must be able to store and display values at least 7 valid digits. If a gambling game operated by an end device allows the production of game and financial data also containing parts of money units, the counter systems must be able to store and display values of at least 9 valid digits; in the case of electromechanical and pulse counter systems, it is sufficient to display values expressed in whole monetary units of at least 7 valid digits.

(3) A terminal must store data pursuant to paragraph 1 in such a manner that allows for statistical tests to verify the values of the parameters of a terminal or game of chance, which are set out in the Gambling Act, to be carried out at any time.

Section 15

Banknote and Coin Acceptor

(1) If a terminal is equipped with a banknote and coin acceptor, it must be designed in such a manner which protects it against vandalism, abuse or other fraudulent activities.

(2) A banknote and coin acceptor must be capable of determining the direction and speed of banknotes or coins when inserted into the acceptor. If a banknote or coin is inserted otherwise than in the conventional manner, the terminal must automatically switch to error status.

(3) All accepted banknotes and coins must be deposited into the banknote and coin repository in the terminal.

(4) The value of each accepted banknote or coin must be immediately displayed on the indicator of the user account’s balance. In the event that the operator of a technical game using secure and reliable methods allows for money to be deposited into a user account by cashless payment, the first sentence shall also apply to thus accepted funds.

(5) A banknote and coin acceptor must not permit the insertion of banknotes or coins, or must reject and return inserted banknotes and coins if the terminal is malfunctioning or in error status.

(6) The screen of a playing position on a terminal must display information that there has been an error that prevents the receipt of a banknote or a coin.

PART FOUR

TRANSITIONAL AND FINAL PROVISIONS

Section 16

This Decree was notified in accordance with Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services, as amended.

Section 17

The operator of gambling operated on the basis of an authorization pursuant to Act no. 202/1990 Coll., as amended ffective before the effective date of law on gambling, which is required to operate this gambling under the law on gambling is obliged to meet the technical specifications for equipment, requirements for the protection and storage of game and

financial data and their technical parameters according to this Decree no later than one year after the date of its entry into force.

PART FIVE

EFFECTIVENESS

Section 18

This Decree shall enter into force on the day of its publication.

Minister of Finance:

Annex to Decree No. …/… **Coll.**

Minimum Requirements for Cryptographic Algorithms

(1) Symmetric Algorithms

a) Block and stream ciphers for the protection of confidentiality and integrity

1. Advanced Encryption Standard (AES) using 128, 192 and 256-bit key length, Triple Data Encryption Standard (3DES) using 168-bit key lengths, limited use with a key size of under 10 GB only, gradually change to AES,
2. Triple Data Encryption Standard (3DES) using 112-bit key lengths, limited use with a key size of under 10 MB only, gradually change to AES. Recommended use of a unique key for each message,
3. Blowfish using a minimum key length of 128 bits, limited use with a key size of less than 10 GB only,
4. Kasumi using a key length of 128 bits, limited use with a key size of less than 10 GB only,
5. Twofish using a key length of 128 to 256 bits,
6. Serpent using a key length of 128, 192 and 256 bits,
7. Camellia using a key length of 128, 192 and 256 bits,
8. SNOW 2.0 and SNOW 3G using a 128 and 256-bit key length.

b) Cipher modes with integrity protection

1. CCM,
2. EAX,
3. OCB,
4. “Encrypt-then-MAC” type composite diagram.

Note:

An “encrypt-then-MAC” type diagram must only use the specified cipher modes for ciphering and only the specified integrity protection modes for a MAC calculation.

c) Cipher modes

1. CTR,
2. OFB,
3. CBC,
4. CFB,

Note:

CBC and CFB modes must be used with a random initialisation vector which is unpredictable for an attacker, when using OFB mode the initialisation vector value must not be repeated for a particular key, when using CTR mode the counter value must not be repeated for a particular key, and if CBC mode is used for ciphering without integrity protection, the resistance of the CBC mode padding must be verified.

d) Integrity protection modes

1. HMAC,
2. CBC-MAC-X9.19, limited to the use of a load smaller than 109 MAC,
3. CBC-MAC-EMAC,
4. CMAC.

(2) Asymmetric Algorithms

a) For digital signature technology

1. Digital Signature Algorithm (DSA) using a key length of 2048 bits and above, and a cyclic subgroup parameter length of 224 bits and above,
2. Elliptic Curve Digital Signature Algorithm (EC-DSA) using a key length of 224 bits and above,
3. Rivest-Shamir-Adleman Probabilistic Signature Scheme (RSA-PSS) using a key length of 2048 bits and above,

b) For key agreement and key ciphering processes

1. Diffie-Hellman (DH) using a key length of 2048 bits and above, and a cyclic subgroup parameter length of 224 bits and above,
2. Elliptic Curve Diffie-Hellman (ECDH) using a key length of 224 bits and above,
3. Elliptic Curve Integrated Encryption System - Key Encapsulation Mechanism (ECIES-KEM) using a key length of 256 bits and above. 4. Provably Secure Elliptic Curve - Key Encapsulation Mechanism (PSEC-KEM) using a key length of 256 bits and above,
5. Asymmetric Ciphers and Key Encapsulation Mechanism (ACE-KEM) using a key length of 256 bits and above,
6. Rivest Shamir Adleman - Optimal Asymmetric Encryption Padding (RSA-OAEP) using a key length of 2048 and above,
7. Rivest Shamir Adleman - Key Encapsulation Mechanism (RSA-KEM) using a key length of 2048 and above.

(3) Hash function algorithms

a) SHA-2

1. SHA-224,
2. SHA-256,
3. SHA-384,
4. SHA-512,
5. SHA-512/224,
6. SHA-512/256.

b) SHA-3

1. SHA3-224,
2. SHA3-256,
3. SHA3-384,
4. SHA3-512,
5. SHAKE-128,
6. SHAKE-256.

c) Other hash functions

1. Whirlpool,
2. RIPEMD-160,
3. SHA 1 with limited use.

Note No. 1:

SHA-1 must not be used to generate new digital signatures, timestamps or any other applications requiring a non-collisional SHA-1.

Note No. 2:

SHA-1 may only be used for verifying existing digital signatures and timestamps, generating and verifying HMAC-SHA-1, and functions for deriving keys and pseudo-random number generators.