

REGULATION  
ON THE INFORMATION AND COMMUNICATION SYSTEM FOR THE ORGANIZATION  
OF SPECIAL GAMES OF CHANCE IN CASINOS

“Official Gazette of the Republic of Serbia”, No. 47/2026, dated 21 May 2026.

**1. Introductory provision**

Article 1

This regulation prescribes in more detail the technical and functional characteristics of the information and communication system (hereinafter: ICS) for organizing special games of chance in casinos, the method and procedure for testing the fulfillment of the technical and functional characteristics of the ICS, and the detailed conditions for storage, archiving and the method of data exchange with the Games of Chance Administration (hereinafter: the Administration).

**2. Technical and functional characteristics of the ICS  
for the organization of special games of chance in casinos**

Article 2

The organizer is obliged to use the ICS for the organization of special games of chance in casinos, which enables the storage, archiving and exchange of data electronically with the software solution of the Administration for the purpose of conducting real-time supervision.

The organizer's ICS consists of information and communication technology resources intended for the organization of special games of chance in casinos.

The ICS referred to in paragraph 2 of this Article must meet the following conditions:

1) the ICS software is obtained in one of the ways referred to in Article 44, paragraph 3 of the Law on Games of Chance ("Official Gazette of the Republic of Serbia", No. 18/20 and 94/24 - hereinafter referred to as: the Law);

2) it provides appropriate capacity - speed of response and availability of the system for secure electronic data exchange with the software solution of the Administration for the purpose of supervision;

3) it enables precise record keeping on the calculation, monitoring and control of the status of chips and money on the tables and in the cash register of the casino;

4) it enables direct and secure data exchange with the software solution of the Administration;

5) it has a system of protection against unauthorized use of the ICS and data loss;

6) it ensures security mechanisms for sending the obtained unique secret key that must be sent with each request for entering a transaction, through the authorization header of the transactional Application Programming Interface (hereinafter: API) request.

Article 3

The ICS for games of chance in casinos must be designed in such a way as to contain a module for calculating, monitoring and controlling transactions per individual table, as well as for all tables in the casino in total.

The module referred to in paragraph 1 of this article is intended for calculating and reporting on the turnover of cash and tokens per individual table, for all tables in total, as well as for identifying possible errors.

The module referred to in paragraph 1 of this article contains the following components:

- 1) opening a table (Open);
- 2) pausing a table (Pause);
- 3) replenishing tokens on the table (Fill);
- 4) returning chips from the table (Credit);
- 5) closing a table (Close);
- 6) the table result at the end of the day, which is obtained by applying the following formula:

table result = closer (closing chip balance) + drop (counted money and chips in the drop box) + credit (chips returned from the table) – fill (chips replenished on the table) – open (initial chip balance);

- 7) the total result of all tables at the end of the day.

### **3. Method and procedure for testing compliance with technical and functional characteristics of the IC**

#### Article 4

The testing of the compliance with the technical and functional characteristics of the ICS within the meaning of Articles 2 and 3 of this Regulation shall be carried out by a laboratory authorised by the Minister of Finance, based on testing and control, namely:

- 1) compliance with the conditions referred to in Article 2, paragraph 3, item 1) of this Regulation;
- 2) the organizer's ICS (software, hardware specification);
- 3) the database (protection measures against unauthorized use of the ICS, as well as loss and recovery of data, address of the database location);
- 4) data on authorized persons referred to in Article 6, paragraph 2, item 5) of this Regulation;
- 5) the security system for the integrity of transaction data in the event of a communication connection (Internet) interruption;
- 6) the communication connection between the ICS and the API through which data is forwarded to the Administration;

Based on the performed control, the laboratory referred to in paragraph 1 of this Article shall issue a certificate of compliance with the technical and functional characteristics of the ICS, which the organizer is obliged to submit to the Administration before putting the ICS into use.

For each change in the characteristics of the ICS, the organizer is obliged to submit to the Administration a supplementary certificate of compliance with the technical and functional characteristics of the ICS.

The costs of testing the compliance of the ICS shall be borne by the organizer.

### **4. Conditions for storing and archiving data**

#### Article 5

The organizer is obliged to keep all transactions from the ICS for at least ten years from the date of the transaction in accordance with the regulations governing the prevention of money laundering and financing of terrorism, after which the organizer may archive them, provided that, upon request by the Administration, they must be submitted in their original form within five days from the date of receipt of the request.

### **5. Method of data exchange with the Administration**

#### Article 6

Communication between the organizer and the Administration, for the purpose of electronic reporting, is realized via broadband, cable or optical technology.

The organizer is obliged to:

- 1) provide a connection from one permanent (static) IP address from which data exchange with the ICS is carried out exclusively, the transmission speed of which meets the needs of the expected traffic and which must not be less than 50 Mb/s;
- 2) provide the necessary methods and organize and maintain a private communication network (VPN);
- 3) protect all its computer equipment and local computer network from unauthorized use by third parties;
- 4) ensure the sending of verified secure data that must not endanger the software solution of the Administration;
- 5) authorize and report to the Administration two responsible persons for reporting to the Administration.

The Organizer is obliged to ensure the integrity of the ICS, the protection of data, information and processes from unauthorized or unforeseen changes, by disabling privileged access to the ICS.

The Organizer is obliged to ensure that in all cases of connection interruption, data storage is ensured from the moment of connection interruption until the moment of connection establishment and to deliver this data to the Administration immediately upon connection establishment.

The Organizer is obliged to enable the Administration to access the ICS remotely via a private communication network (VPN).

#### Article 7

An electronic transaction is the recording of each individual data item from Article 3 of this Regulation through the organizer's ICS.

An individual electronic transaction is sent simultaneously, i.e. in real time, to the organizer's ICS, secured by secure protocols.

Data integrity in the event of loss or degradation of the communication connection must be ensured by data storage systems and backup copies on a data storage medium.

An electronic transaction from paragraph 1 of this Article is entered into the Administration's software solution simultaneously, i.e. in real time, by generating a request for entering the transaction.

The request for entering the transaction into the Administration's software solution consists of an API header for authorization forwarded by encryption certificate protection (SSL), while the transaction details are sent in the message body.

The Administration's software solution sends feedback to the organizer's ICS confirming the success of the transaction entry into its system.

The Administration shall provide the information technology details of the transaction referred to in paragraph 5 of this Article and the details of sending the information referred to in paragraph 6 of this Article in appropriate technical instructions.

The organizer shall submit monthly reports to the Administration by the fifth day of the month for the previous month, electronically by connecting to the Administration's web service.

## 6. Final provision

#### Article 8

This regulation shall enter into force on the eighth day after its publication in the "Official Gazette of the Republic of Serbia".