PERSONAL DATA PROTECTION

Scope of Application

Personal data may be processed exclusively by authorized persons. Authorization to process personal data derives from the job description or from a specific decision issued by the Director of the Company. Employees of the Company authorized to process personal data are responsible for the lawful and conscientious processing of personal data within the scope of the duties they perform.

The Company ensures that its employees are familiar with the fundamental principles of personal data protection and the obligations arising therefrom.

Purpose, Measure, and Scope of Personal Data Processing

The Company collects and processes personal data for the purpose of carrying out its business activities, to the extent and within the scope prescribed by the applicable regulations. Collected personal data shall be updated as necessary in order to ensure their accuracy.

The employee who has access to and authorization for processing personal data within the sector/service/department in which such data are processed shall be responsible for the processing and updating of personal data.

Personal data shall be stored in a form that is most appropriate for the purpose for which they are collected and processed.

The Company processes data contained in personal data records to the extent determined by the regulations that constitute the legal basis for maintaining such records.

Lawfulness of Personal Data Processing

Personal data processing within the Company shall be carried out exclusively in accordance with the Law and only if at least one of the following conditions is met:

- if the data subject has given consent to the processing for one or more specific purposes;
- if the processing is necessary for the performance of a contract or for taking steps prior to entering into a contract;
- if the processing is necessary for compliance with legal obligations;
- if the processing is necessary to protect the vital interests of the data subject or another natural person.

The Company is obliged to:

- process personal data in a fair, lawful, and transparent manner;
- process personal data collected for specified, explicit, and lawful purposes only in a manner consistent with those purposes;
- ensure that personal data processed are adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed;
- process only reliable and accurate data and update them as necessary;

- rectify or erase personal data that are inaccurate or incomplete in relation to the purpose for which they were collected or further processed;
- store personal data in a form which permits identification of the data subject for no longer than is necessary for the purposes for which the personal data are processed;
- process personal data in a manner that ensures appropriate security, including protection against unauthorized or unlawful processing and against accidental loss, destruction, or damage, by applying appropriate technical or organizational measures;
- ensure the principles of reliability and compliance in personal data processing and the ability to demonstrate such compliance.

Consent

The Company may collect and process personal data exclusively on the basis of the prior consent of the data subject, except in cases where another legal basis for processing exists in accordance with applicable regulations.

Where the processing of personal data is based on consent, the Company shall be obliged to ensure and demonstrate that such consent has been validly obtained.

The Company may process personal data without the prior consent of the data subject in the following cases:

- if it processes the data in accordance with the law or where such processing is necessary to fulfill obligations prescribed by law;
- when the Company collects personal data in accordance with statutory regulations or in order to perform its legal obligations;
- when the data subject, at his or her own request, enters into negotiations regarding a contractual relationship or where processing is necessary to fulfill obligations agreed with the Company.

The data subject has the right to withdraw his or her consent at any time, in the same manner in which the consent was given, in written form.

Upon receipt of the notification of withdrawal, processing based on such consent shall cease immediately, without prejudice to the lawfulness of processing carried out prior to the withdrawal. All such actions shall be documented in the appropriate records where the processing of personal data was based on such consent, in order to ensure a trace of the date and time of withdrawal.

Transparent Information, Communication, and the Exercise of Data Subject Rights

The data subject has the right to obtain from the Company, as the processor, the following information and to exercise the following rights in relation to the processing of his or her personal data:

- access to his or her personal data being processed;

- information regarding the processing (the purpose of processing, the categories of personal data being processed, and the manner in which they are processed);
- the right to request rectification, erasure, or restriction of processing, as well as the right to object;
- the right to lodge a complaint with the Personal Data Protection Agency or to seek protection before the competent court;
- information about the source of the data, where the data were not collected directly from the data subject.

Access to personal data may be restricted only where such restriction is prescribed by a specific law for the purpose of respecting the rights and freedoms of other persons.

Right of the Data Subject to Access Personal Data

When the data subject requests access to personal data, upon receipt of the request, the Company shall be obliged to provide information regarding the processing of his or her personal data within 30 days from the date of receipt of the request, provided that the request is justified. That period may, where necessary, be extended by an additional 60 days, taking into account the complexity and number of requests received. In such a case, the Company shall inform the data subject of any such extension within 30 days from the date of receipt of the request, stating the reasons for the delay.

If the data subject submits the request electronically, the information shall be provided electronically, where possible, unless the data subject requests otherwise.

The Personal Data Protection Officer shall verify the identity of the data subject, collect all relevant records, and provide them to the data subject in a clear and comprehensible manner (e.g., in PDF format or in written form).

Right of the Data Subject to Rectification and Erasure of Personal Data

If the data subject notices that his or her personal data are inaccurate, incomplete, or outdated, he or she has the right to request their rectification or completion.

The Company shall ensure a simple, transparent, and easily accessible procedure for rectifying or supplementing such records without undue delay.

In the case of erasure ("right to be forgotten"), it is necessary to verify whether there are objective reasons (e.g., legal obligations for retention) and then permanently remove the data from all systems and backups.

The Company shall erase personal data without undue delay if any of the following conditions are met:

- the personal data are no longer necessary for the purposes for which they were collected;
- the data subject has withdrawn consent and there is no other legal basis for processing;
- the data subject has submitted a valid objection to the Company;
- the data have been processed unlawfully.

The procedure for rectification or erasure of personal data shall be transparent in such a way that the data subject is informed of the steps taken.

The procedure for rectification and erasure of personal data is transparent, ensuring that the data subject is fully informed of all steps undertaken.

Right of the Data Subject to Restrict Processing

The data subject has the right to request restriction of processing if any of the following conditions are met:

- the data subject disputes the accuracy of the personal data;
- the processing is unlawful, and the data subject objects to the erasure of the personal data and instead requests the restriction of its processing;
- the Company no longer needs the personal data for processing purposes, but the data subject requires it for the establishment, exercise, or defence of legal claims;
- the data subject has submitted a valid objection.

If processing is restricted, the personal data may only be processed with the consent of the data subject.

The Company shall inform the data subject who has exercised the right to restrict processing before lifting the restriction.

Right of the Data Subject to Object and Method of Submitting Requests

The data subject has the right to lodge an objection with the Company at any time if he or she considers that his or her personal data are not being processed in accordance with the Law.

The data subject exercises the rights described above exclusively by submitting a written request on the prescribed form, either personally or through an authorized representative, duly signed and accompanied by a valid identification document, so that there is no doubt that the request originates solely from the data subject.

The Request Form is available on the Company’s website.

The request may be submitted in writing, by registered mail addressed to the Company’s headquarters and marked for the attention of the Director, or via e-mail: **dpo@coloseum-club.com**.

If the data subject submits the request electronically, the information shall be provided electronically where possible, unless the data subject requests otherwise.

Oral information may only be provided by the Personal Data Protection Officer.

Upon receipt of a written request, it shall be forwarded to the Personal Data Protection Officer.

After receiving the request, the Personal Data Protection Officer shall, upon making a decision regarding the request, complete the prescribed form documenting the resolution of the request.

Verification of the Identity of Users Submitting Requests via E-mail

Before any modification or processing of personal data based on a request submitted via e-mail is carried out, it is necessary to verify the identity of the person submitting the request.

In order to protect the rights of the data subject, preserve system security and integrity, and prevent unauthorized access to data, the following procedure is established for verifying the identity of the requester:

- **Verification of e-mail address** – if the person uses an official e-mail address already registered and linked to their identity (e.g., user account, previous correspondence), this can serve as an initial indicator but is not sufficient on its own;
- **Request for additional identification** – if the identity of the requester cannot be reliably confirmed through existing records or the official e-mail address, the requester will be asked to provide additional identification, i.e., a scanned copy of a valid identification document (e.g., identity card), with the following recommendations: only the information necessary to confirm identity (name, surname, date of birth) should be visible, while other details (e.g., document number, address) may be obscured unless required for the procedure. A statement/consent from the requester may also be requested confirming that the document is provided exclusively for identity verification in accordance with the Law on Personal Data Protection of Bosnia and Herzegovina. The requester may also be asked to submit a signed request in PDF format containing basic identification data and signature, as well as any other information necessary to confirm their identity.

All documentation provided for user identification shall form an integral part of the personal data processing records.

Documents shall be stored in accordance with internal archiving and data protection rules and shall be accessible exclusively to authorized personnel.

Record of Providing Personal Data to the Data Subject

The Company maintains a record of personal data provided to the data subject and the purpose for which such data were provided.

The record must include the following information: the employee processing the personal data, the date on which the personal data were provided, the type of personal data, the legal basis, and the purpose for which the personal data are provided.

The record is maintained electronically using a designated form.

Record of Rejected Data Subject Requests

The Company maintains a record of rejected requests submitted by data subjects.

The record is maintained electronically using a designated form and must include the following information: the name and surname of the data subject, the number and date

of the request, the content of the request, the number and date of the decision rejecting the request, and the reason for rejection.

Management of Records

The aforementioned records are completed and collected at the Company's headquarters and submitted to the Personal Data Protection Officer for further processing, in accordance with the Law.

The contents of the electronic records are finalized on the last day of the calendar year, after which they are printed and signed by the Personal Data Protection Officer and the responsible person of the Company.

The Company shall, upon request by the Agency, allow access to the aforementioned records.

Obligation to Maintain the Confidentiality of Personal Data

Employees of the Company who process personal data, as well as those who come into contact with personal data in the course of their duties within the Company's premises, are obliged to maintain confidentiality and adhere to established protective measures.

The personal data of employees processed by the Company constitute a business secret.

An employee who misuses personal data shall be held liable under disciplinary, financial, or criminal measures.

Misuse of personal data is considered any disclosure, transfer, use, or provision to third parties without the consent of the data subject and in violation of the Law.

Audio-Video Surveillance

The Company uses audio and video surveillance in accordance with the provisions of the Law and other applicable legal regulations governing the protection of personal data, the organization of games of chance, and the implementation of technical systems for the protection of human life and health, as well as property.

Recording through audio and video surveillance (with both video and audio) ensures continuous and direct monitoring of casino games for the purpose of supervision and ensuring their fairness, while video surveillance without audio is implemented for the purpose of technical protection of human life and health, and property, in accordance with the regulations.

The processing of personal data through audio-video or video surveillance refers to the collection and further processing of personal data, including the creation of recordings that constitute, or are intended to constitute, part of a storage system.

The audio-video and video surveillance system is protected against unauthorized access, and only authorized personnel have access rights.

Each access to recordings obtained through audio-video or video surveillance, as well as their processing, is separately recorded via an automated logging system indicating the time, location of access, and the identity of the person who accessed the recordings.

Audio-video and video surveillance cover only rooms or parts of rooms where monitoring is necessary to achieve the legally prescribed purpose.

Parts of the premises under video surveillance must be marked in such a way that the sign is visible at the latest upon entering the field of view of the camera. The sign includes a notice that the area is under video surveillance, information about the Company, and contact details through which the data subject or a third party can exercise their rights.

Recordings obtained via video surveillance are stored for a minimum of 30 days.

Data Protection Officer (DPO)

The decision on the appointment of the Data Protection Officer of Hit Coloseum d.o.o., including a description of their duties and responsibilities, has been published on the Company's website.

Transfer of Data to Third Parties

The provision of data contained in personal data records is carried out in accordance with the Law, if public authorities request it and if such data are necessary for the exercise of jurisdiction established by the Law.

The Company may provide personal data to a third party if it is necessary for the fulfilment of legal obligations of the third party, or if it is necessary to achieve the legitimate interests of the third party. The Company shall not transfer personal data for the purposes of direct marketing.

Refusal of Third-Party Requests

Personal data shall not be provided to or disclosed to third parties unless such disclosure is based on the Law.

Transfer of Data Abroad

Personal data contained in records maintained by the Company shall not be provided to persons or institutions outside Bosnia and Herzegovina, except in cases of business cooperation, compliance with legal obligations, or the protection of the vital interests of the Company's founder. In such cases, data may be provided to the founder and transferred to the Republic of Slovenia, which, as a member of the European Union, ensures an adequate level of personal data protection.