DATA MANAGEMENT INFORMATION

Las Vegas CASINO Tropicana/Sofitel/Atlantis/Corvin Promenade/EuroCenter

I. Introduction

Welcome to the Las Vegas Casino Tropicana/Sofitel/Atlantis/Corvin Promenade/Atrium EuroCenter!

In order to use the services available at Las Vegas Casino Tropicana/Sofitel/Atlantis/Corvin Promenade/Atrium EuroCenter Casino, we require you to provide us with certain personal information as required by law.

The purpose of this Privacy Notice (the "Notice") is to set out, in accordance with applicable law, the data processing principles, purposes and other facts that determine the purposes for which, for how long and how we process the personal data you provide us with and your rights of enforcement and redress in relation to that processing.

The security and proper processing of the personal data you provide to us is of the utmost importance to us, so please read this Notice carefully and carefully. If you have any questions or comments about what is written here, please contact us before accepting this Notice.

II. Definitions of terms used in the Prospectus

The following is a summary of the most important terms used in the Notice, based on Article 4 of the GDPR.

1. Personal Data: any information relating to a Guest which identifies or identifies the Guest. A natural person can be identified, directly or indirectly, in particular by reference to an identifier such as a name, number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. The Data Controller collects personal data about the Guest separately indicated in this Notice for each processing purpose.

2. Data processing: any operation or set of operations which is performed on data, regardless of the procedure used, in particular collection, recording, recording, organisation, storage, alteration, use, consultation, disclosure, transmission, alignment or combination, blocking, erasure and destruction, as well as the prevention of further use of the data.

3.Data Controller: the data provided by the Guest is processed by LVC Diamond Kft. (registered office and mailing address: 1088 Budapest, Rákóczi út 1-3. III. floor; company registration number: 01-09-194087 [registered at the Budapest General Court]; tax number: 25002889-4-44; e-mail: adatvedelem@lvcd.hu), i.e. only LVC Diamond Kft. may make and execute decisions related to the Guest's personal data.

4. Processing of personal data: any operation on personal data related to processing operations carried out on behalf of the Controller, irrespective of the method and means used to carry out the operation and the place of application, provided that the operation is carried out on the data. Accordingly, a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller shall be considered a processor.

5. Transfer: making data available to a specified third party.
6. Recipient: a natural or legal person, public authority, agency or any other body to whom or with which personal data are disclosed, whether or not a third party.
7. Casino: a gaming casino operated by the Controller pursuant to the Act and applicable laws.
8. Grt.: Act XLVIII of 2008 on the Basic Conditions and Certain Restrictions of Economic Advertising Activities.
9. GDPR: Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
10. Authority: the National Authority for Data Protection and Freedom of Information (address: 1055 Budapest, Falk Miksa utca 9-11.; e-mail: ugyfelszolgalat@naih.hu; website: http://naih.hu; telephone: +36 (1) 391-1400).
11. Website: https://lasvegascasino.hu/
12. IP address: a unique network identifier used to identify between devices using the TCP/IP network protocol to access the Internet. Each IT device connected to the Internet has a unique IP address through which it can be identified.
13. cookie: a packet of data (file) that is generated by the Internet content server and delivered to the web browser. Cookies can contain information about searches made on a particular web server, information that is stored on the server. The primary purpose of the use of cookies is to store user profile information, which is used primarily to store the preferences of the user, so that the user can access the website in the way he or she is used to.

Cookies are stored by the browser software in a separate directory on the devices used by the data subject (computer, tablet, smartphone, etc.). The cookie uniquely identifies and allows the web server to recognise the user and the device used to access the internet. The GDPR also includes cookies and other identifiers placed on the device used by the user as personal data.

14. Web beacon (web bug): invisible images on websites or in emails that allow the user's actions (e.g. opening a newsletter, clicking on URLs, etc.) to be tracked and measured. Web beacons are commonly used in conjunction with cookies to provide additional information for profiling users online.
15. Act XXXIV of 1991 on the organisation of games of chance.
16. Gaming Organisation Ordinance: the currently valid Ordinance No. 5/2021 (X. 21.) of the Federal Ministry of Social Affairs and Health on the detailed rules of responsible gaming organisation.

17. SZTFH Decree: the currently valid SZTFH Decree No. 20/2021 (X. 29.) on the implementation of tasks related to the licensing, conduct and control of certain gambling activities.
18. AML Act: Act LIII of 2017 on the Prevention and Suppression of Money Laundering and Terrorist Financing.
19. Rules of Participation:The current Rules of Participation of the Casino.
20. Service: any service that the Guest may use at the Casino.
21. Guest: any natural person over the age of 18 who uses the Casino's services in accordance with the Participation Rules and the applicable laws.

III. Contact details of the Data Controller and the Data Protection Officer

The Controller has appointed a Data Protection Officer to ensure the highest possible level of protection of the personal data processed and to mitigate the risks associated with the processing operations. The contact details of the Data Controller, the Data Controller's representative and the Data Protection Officer are set out in this Chapter.

Contact details of the Data Controller:

Company name: LVC Diamond Ltd.

Registered office and mailing address: 1088 Budapest, Rákóczi út 1-3.

E-mail: adatvedelem@lvcd.hu

Phone number: +3612662081

Name and contact details of the Data Controller's representative:

Name: dr. Dravecz Róbert Managing Director

Address for correspondence: 1088 Budapest, Rákóczi út 1-3.

E-mail: adatvedelem@lvcd.hu

Name and contact details of the Data Protection Officer of the Data Controller:

Name: Lajer Lawyers Association

Address and correspondence address: 1024 Budapest, Lövőház utca 30.

E-mail: DPO.LVC@lajer.net

IV. Data processing principles

The following is a summary of the data management principles that the Data Controller will fully enforce throughout the entire period of data management.

1. Lawfulness, fairness and transparency: data processing is always based on legal requirements (in particular the provisions of the Hungarian Data Protection Act) and, in some cases, on the prior consent of the Customer expressed by using the Service. The Data Controller collects and processes personal data from the Guest in the course of providing the Service. The processing of the Guest's personal data shall be carried out exclusively in a lawful and fair manner and in a transparent manner for the Guest. The Data Controller shall make the current text of the Guide available and accessible to the public free of charge, without obligation, on a continuous basis and in a public manner in the Casino. The Data Controller shall not process the personal data provided for purposes other than those set out in this Policy or for purposes other than those set out in this Policy, and shall at all times act in accordance with this Policy and the applicable laws.

2.Purpose limitation: the Data Controller may process personal data only for the clear and legitimate purposes indicated in the Notice and in the relevant legislation (in particular the Pmt., the Szjtv. and the SZTFH-verordnung). If the Data Controller intends to process personal data already provided for purposes other than these purposes, the Data Controller shall inform the Guest thereof in advance and in full (primarily by e-mail). In order to ensure full clarity of the purposes for which each personal data is processed, the Controller provides information in this Notice on the purposes for which, the duration of the processing and the legal basis on which each personal data is processed. The Controller shall apply all these provisions as binding on itself.

3.Personal data processed solely pursuant to Article 6(1)(a) of the GDPR on the basis of the Customer's explicit and voluntary consent shall be processed by the Controller until the Customer's request for erasure or until the consent is withdrawn.

The Data Controller shall in any case, unless otherwise provided by law, keep the personal data processed in accordance with the provisions of the Pmt. for 8 years from the termination of the business relationship with the Guest pursuant to Articles 56-57 of the Pmt.

4. Data economy: the Data Controller processes only the personal data that is necessary to provide the highest possible quality of the Services.

In any case, this is personal data that is adequate, relevant and genuinely necessary for the actual use of the Service for the purposes for which it is processed.

5. Accuracy: the Data Controller aims to ensure that the personal data already recorded are kept up to date in order to provide the highest possible quality of the Services and to fulfil its legal obligations (Article 12 (1) of the Act on the Protection of Personal Data).The Customer is also obliged to facilitate the up-to-dateness of the data, and is therefore obliged to notify the Data Controller within five working days of becoming aware of any changes to the data provided during the customer due diligence pursuant to the Act on the Protection of Personal Data.

6.Data protection (integrity and confidentiality): the Data Controller attaches the utmost importance to the protection of the personal data provided and the privacy of the Guest. The Data Controller shall in all cases ensure the security of personal data and shall take the technical and organisational measures and establish the procedural rules necessary to enforce the data protection and confidentiality rules. In order to ensure a high level of data protection, the Data Controller shall only use data processors that offer adequate guarantees as to the adequacy of the processing, to implement appropriate technical and organisational measures to ensure the protection of the rights of the Guests (Article 28(1) GDPR). The Data Controller shall take appropriate measures to protect personal data, in particular against unauthorised access, alteration, disclosure, transmission, disclosure, erasure or destruction, accidental destruction or damage and inaccessibility resulting from changes in the technology used (in particular: password protection; encryption procedures; data recovery, data loss).

V. Purposes of data processing, data management process

The following is a summary of the situations (purposes of processing) in which, in practice, the processing of the Guest's personal data takes place.

1.The purpose of the processing is to carry out customer due diligence measures in accordance with the provisions of the Pmt. (§ 7) and the Szjtv. (§ 29/H), to ensure player protection and to provide the Service provided by the Data Controller.

(A) Customer due diligence, customer identification At

registration:

The Data Controller is obliged to identify the player (as a customer) in order to issue the access card, to record personal data, to view and copy his/her identity document, foreign citizen's residence document or residence permit, including foreign citizen's visa. The recording of this data is a prerequisite for access to the Casino.

Purpose of processing: identification and screening of the customer.

Personal data processed: name and surname, surname and given name at birth, nationality, place and date of birth, mother's name at birth, address (or residence if not); and the following personal data processed on documents: number of the card, date of issue, validity, issuing authority, photograph, depending on the type of document: the gender and signature of the Guest; and the Guest's risk level, source of funds and assets in case of application of Article 9/A (2) of the Act on the Protection of Personal Data. This data processing is mandatory, without this data processing the Guest cannot use the Service.

Legal basis for data processing: fulfilment of a legal obligation [Article 6 (c) GDPR], § 7 (2), (3), (5), § 3.19.a), § 6/A, § 9/A, § 16, § 16/A, and also § 7 (9) Pmt.

Duration of processing: the Data Controller is entitled to process personal data for 8 years from the termination of the business relationship pursuant to Art.

Customer identification on login:

Pursuant to Article 39 (1) of the OFTA Regulation, the Data Controller is obliged to carry out the identification required by the Pmt. when players enter the game, including recording and registering the time of the player's entry.

(B) Public player declaration

The player is required to declare whether he/she is a major public figure, a close relative of a major public figure or a person closely associated with a major public figure.

Purpose of data processing: customer due diligence, record of public figure status.

Personal data processed: name, status as public figure, category according to Article 4 (2) - (4) of the Public Procurement Act, source of funds and assets. This processing is mandatory, without this processing the Guest cannot use the service.

Legal basis for processing: fulfilment of a legal obligation [Article 6(c) GDPR], Art.

Duration of processing: the Data Controller is entitled to process personal data for 8

years from the termination of the business relationship pursuant to Section 56 (2) of the Act.

(C) Photo

In order to prevent and combat money laundering and terrorist financing, to ensure the interconnectivity of the data obtained in the course of customer due diligence measures and player transactions, and to ensure the effective performance of its supervisory activities, the Data Controller is entitled to record the Customer's image and to store it in its electronic image registration system.

This processing is mandatory and without this processing the Guest cannot use the Service.

Legal basis for processing.

Duration of data processing: the Controller is entitled to process personal data for 8 years from the termination of the business relationship pursuant to Section 56 (2) of the Personal Data Protection Act.

(D) Access card

The Controller shall provide Guests with an access card upon first entry to the Casino.

The purpose of the processing is to create an access card and to identify the Guest in connection with the access.

The access card and its registration system contain the data pursuant to Article 41 (2) of the SZTFH Decree: the serial number of the access card; the full name of the person (Guest) entering; the date of issue of the access card; the period of validity of the access card; the stamp or other distinguishing mark of the Casino.

Legal basis for data processing: fulfilment of a legal obligation [Article 6(c) GDPR], § 41 of the SZTFH Regulation. Without this processing, the Guest cannot use the Service.

The access card is valid for a maximum of 2 years pursuant to Section 41 (1) of the SZTFH Regulation (which may be extended).

(E) Registration of accesses

The Data Controller shall record and register the time of the Guest's entry and the time of the attempt to enter the Casino despite the entry in the Player Protection Register or the Self-Disclosure Register.

Personal data processed: name, date of entry, number of entries. This processing is mandatory, without this processing the Guest cannot use the Service.

Legal basis for processing: fulfilment of a legal obligation [Article 6(c) GDPR], Article 39(1) of the GDPR.

Duration of data processing: subject to Section 39 (1) paragraph (1) of the SZTFH Regulation, pursuant to Section 56 (2) of the Hungarian Data Protection Act, 8 years from the termination of the business relationship.

(F) Computer (receptionist) records

The Data Controller uses a computerised (receptionist) register of Guests to facilitate access control, in which the following personal data may be processed for a period of 8 years after the termination of the business relationship, unless otherwise provided for in the Data Processing Notice:

i.Based on (A) to (D) above: surname and first name; ID card number, status, issue and expiry date; type, issuer, number, expiry date, issue date of identity document; place and date of birth; name at birth; nationality; mother's name; address or residence; status as a public figure; photograph; copy of identity document, Guest's signature.

ii. the number of entries under point E) above.

iii. Guest's gender: on the basis of the Data Controller's legitimate interest [Article 6(f) GDPR], the Data Controller records the gender of each Guest in order to provide gender-appropriate communication (addressing) and to allow the use of this data for non-specific games. (Legitimate interest of the Data Controller: commercial, economic interest linked to the interest to organise different types of games and to provide a high level of Service. For more information, see the interest balancing test prepared by the Data Controller.)

iv. VIP classification: the Data Controller may - on the basis of its legitimate interest [Article 6(f) GDPR] - classify the Guest into different VIP categories based on its own classification system in order to provide different discounts and comfort levels. (Legitimate interest of the Data Controller: business, economic interest linked to the interest to enhance the use of the Service. For more information, see the interest balancing test prepared by the Data Controller.)

v. Profile related note: the Data Controller is entitled to record other information in the register containing the Guest's profile, which may be of an administrative nature, necessary to enforce the Casino's rules (e.g. a dress code problem has arisen) or security-related (the Guest is under self-restraint). The duration of the processing of this data is until the termination of the business relationship. This processing is based on the legitimate interest of the Data Controller [Article 6(f) GDPR] (Legitimate interest of the Data Controller: commercial, economic interest linked to the interest in guaranteeing the security of the service, maintaining the confidence of the players and long-term efficient operation. For more information, see the interest balancing test prepared by the Data Controller.)

vi. E-mail address, telephone number: the Guest may voluntarily provide his/her e-mail address or telephone number, subject to his/her consent, in accordance with [Article 6(a) GDPR]. The purpose of data processing is to keep in contact with the Guest and to inform him/her. (Withdrawal of consent does not affect the lawfulness of the processing carried out on the basis of the consent prior to its withdrawal.)

vii. Risk level classification: the Data Controller is obliged to determine the low, average or high risk level of the Guest at the time of establishing the business relationship and to record it in writing [Article 6(c) GDPR], pursuant to Article 6/A of the GDPR. This processing is mandatory, without this processing the Guest cannot use the Service.

2. Registration of orphaned chips (orphans):

The purpose of the processing is to keep a record of the amount of money returned. Orphans include, for example, stray chips found in the Casino (e.g. left on the gaming table or forgotten during the game) that can be used as a bet, whose rightful owner has not been identified by the Promoter by the end of the gaming day, and all chips that are not identified by the Promoter in accordance with the provisions of the SZTFH
Regulation 44. §-The Guest who proves his ownership of the orphans shall be refunded the amount of money - in the case of chips, the amount corresponding to the value - and the refunded amount of money shall be recorded in the orphans' register.

The register of orphans contains the following personal data: the name of the Guest entitled to the consideration for the orphans; his/her place of residence; the date of repayment; the amount; and, in the case of a ticket, his/her unique identifier. If the organiser has carried out an investigation to establish the legitimacy of the claim of the person claiming the orphan's consideration, the register of orphans shall be accompanied by a report containing the results of the investigation of the event. This processing is mandatory, without this processing the Guest cannot use the Service.

The legal basis for the processing is the fulfilment of a legal obligation in accordance with Article 6(1)(c) of the GDPR.

Duration of data processing: 6 years pursuant to Section 7a (1) 7a of the Act on the Protection of Personal Data, and thereafter for a further 2 years pursuant to the Accounting Act in force (i.e. 8 years from the accounting event).

3. Winning certificate:

The purpose of data processing is - upon request of the Guest entitled to the prize - to issue a certificate certifying the title and value in HUF of the prize exceeding HUF 2 million or the equivalent amount in HUF.

The prize certificate contains the following personal data: the Guest's identification data, the prize and the place and date of receipt of the prize (Section 1 (8) of the Act on the Protection of the Right to Information). This data processing is mandatory, without this data processing the certificate cannot be issued.

The legal basis for the processing is the fulfilment of a legal obligation in accordance with Article 6(1)(c) of the GDPR.

Duration of data processing: 6 years pursuant to Section 7a (1) 7a of the GDPR and 2 years thereafter pursuant to the Accounting Act in force (i.e. 8 years from the accounting event).

4. Deposit records:

The purpose of the data management is to keep a record of the chips and funds deposited by the Guest, as set out in the Rules and Regulations.

The deposit register contains the following personal data: the identification data of the depositing Guest, the denomination and amount of the deposited chips and funds, the date of deposit.

Legal basis for processing: legitimate interest of the Data Controller [Article 6(1)(f) GDPR] (Legitimate interest of the Data Controller: business, economic interest linked to the interest in the proof, security and record keeping of the use of the deposit service. For more information, see the interest balancing test prepared by the Data Controller.)

Duration of processing: 5 years (~ until the statute of limitations according to the Civil Code).

5. Expulsion records:

Legal basis for data processing: fulfilment of a legal obligation pursuant to Section 1 (5c) of the Data Protection Act. The Data Controller shall keep records for the purpose of effective enforcement of the prohibition of entry and participation in gambling (hereinafter referred to as "banning") against a Guest who seriously violates the Rules of Participation.

Pursuant to Section 1 (5c) of the Act on the Protection of Personal Data, the following personal data shall be included in the record of the expulsion:

a) the data of the Guest pursuant to Section 29/H (1) of the Act: name and surname, name and surname at birth, mother's name; address, or in the absence thereof, place of residence; nationality; type and number of a document suitable for identification; place and date of birth;

(b) the fact, reason and date of the ban; and

(c) the ad hoc nature of the ban or its definite duration, which may not exceed 5 years.

The Data Controller may transfer the data of the banning register to other casinos operated by the Data Controller and may also apply the ban imposed on the Guest to these casinos pursuant to the Gaming Ordinance, Article 25 (2).

The Data Controller may process the data of the banning register for a period of 6 years from the date of the banning order, after the expiry of the 6-year period, the Data Controller shall delete the data [Section 1 (5c) para.]

The legal basis for the processing of the data is the fulfilment of a legal obligation in accordance with Article 6(1)(c) of the GDPR. This processing is mandatory.

6. Giveaway of promotional prizes:

From time to time, the Data Controller will organise promotions in the Casino area, during which gift tokens and gift tickets will be given to Guests, which will be recorded in the receptionist's records.

The data processed are: the date and time of receipt of the gift tokens, gift tickets, prizes (promotional gifts, giveaways), and the name of the person receiving the gift tokens.

Purpose of data processing: recording the receipt of a promotional prize, verification of the fulfilment of the promotion.

Legal basis for processing: legitimate interest of the controller - [Article 6(1)(f) GDPR] (Legitimate interest of the controller: business, economic interest linked to the interest in providing proof of the delivery of the prizes and the operation of sound accounting). For more information, see the interest balancing test prepared by the Data Controller.)

Duration of processing: 8 years in accordance with the Accounting Act.

7. Register of self-limitation, self-exclusion:

Purpose of data management: to register self-limitations/self-exclusions, to ensure player protection and to provide data to the gambling supervisory authority.

Personal data processed: name; place and date of birth; mother's name; address; ID card number; duration, fact/subject, period, date of unblocking. This processing is mandatory, without this processing the Guest cannot make a declaration.

Legal basis for data processing: fulfilment of legal obligations - GDPR Article 6 (1) (c), §§ 16-17 of the Game Organisation Regulation, § 29/I (2) of the Act on the Protection of Personal Data.

Duration of data processing: 6 years from the date of data creation.

8. Player protection register:

Pursuant to Section 1 (6b) of the Gambling Supervision Act, the Gambling Supervision Authority shall keep a register of persons who have made a significant self-restrictive declaration and persons who have been placed under guardianship by a court of law with a total restriction of capacity or a partial restriction of capacity with regard to their legal declarations in connection with gambling.

Pursuant to Section 1 (6b) of the Act, the Data Controller, as the organiser, may obtain, process and use the data in the Player Protection Register solely for the purpose of restricting the participation of the persons concerned in gambling.

Pursuant to Section 1 (6d) of the Act, the Player Protection Register contains:

(a) separately, personal identification data (name and surname, name and surname at birth, mother's name, place and date of birth, type and number of identification document, address) of persons who have given a significant self-restriction declaration and of persons pursuant to paragraph (6),

(b) the nature of the processing (restriction based on a voluntary decision or a judicial decision),

(c) the date of termination (whether the processing is of a fixed or indefinite duration).

The Data Controller may access the Player Protection Register using an electronic extract for the sole purpose of fulfilling its obligation to verify. The extract shall contain a non-reversible alphanumeric code generated from personal data. The DPA shall make available to the Data Controller, by electronic means, the procedure for the generation of the alphanumeric code. The Data Controller shall compare the alphanumeric code generated from the personal data of the player with the alphanumeric code contained in the extract. If the two codes match, the Data Controller shall refuse to register the player or shall not provide the registered player with a playing opportunity.

Purpose of processing: access to the player protection register.

Legal basis for processing: fulfilment of a legal obligation - Article 6 (1) (c) GDPR, § 20 of the Regulation on the organisation of games. Without this processing, the Guest cannot use the service.

Duration of data processing: the date of the check and the Data Controller shall store the notification of refusal of access given to the Player for 5 years.

9. Suspicion of money laundering and terrorist financing:

Data processed: name, name at birth, mother's name, place and date of birth, nationality, address, type, number and expiry date of identification documents. [Pursuant to Article 30(2)(a) of the Personal Data Protection Act, the Data Controller is obliged to indicate in the notification the data pursuant to Articles 7 to 14 of the Personal Data Protection Act (see Section 1(A) of this Chapter of the Information Notice) and the circumstances on the basis of which the notification was made.]

Purpose of processing: to fulfil the notification obligation.

Legal basis for processing: fulfilment of a legal obligation - Article 6(1)(c) GDPR, Article 30(1)(a)-(b) Pmt. This processing is mandatory.

Duration of data processing: 8 years from the termination of the business relationship [pursuant to Art].

10. Reporting counterfeit, suspect banknotes:

Data processed: name, name at birth, mother's name, place and date of birth, nationality, address, type, number and expiry date of identification document. [Pursuant to Article 30(2)(a) of the Hungarian Data Protection Act, the Data Controller is obliged to include in the notification the data pursuant to Articles 7 to 14 of the Hungarian Data Protection Act (see Section 1(A) of this Chapter of the Information Notice) and the circumstances on the basis of which the notification was made.]

Legal basis for data processing: fulfilment of a legal obligation - Article 6 (1) (c) GDPR, Article 30 (1) (c) Pmt.

Duration of data processing: 8 years from the termination of the business relationship (pursuant to Art. 56 (2) Pmt.)

11. Monitoring of financial and property restrictive measures imposed by the EU/UNSC:

Pursuant to Article LII (6) of Act LII of 2017, the service provider must have a filtering system in place to ensure the implementation of EU legal acts and UNSC Resolutions imposing financial and property restrictive measures, and an IT system capable of regularly comparing the personal data of the entire customer file registered by the service provider with the data of the persons identified by the restrictive measures.

Purpose of data processing: to identify persons subject to financial and property restraint measures.

Legal basis for processing: to comply with a legal obligation [Article 6 (1) (c) GDPR] - Act LII of 2017 and the Act on the Prevention and Combating of Money Laundering and Terrorist Financing of 2017 on the prevention and combating of money laundering and terrorist financing for operators of casinos, card rooms, betting not constituting remote gambling, remote gambling and online casino games. 19. Duration of data management: the provider is obliged to keep the data generated during the screening for 8 years from the date of screening. This data management is mandatory.

12. Video system:

The Data Controller operates a closed circuit television ("CCTV") system in the Casino for the protection and identification of the Guests, the cleanliness and safe conduct of the game, the protection of order and property and the performance of the tasks provided for in the Pmt.

Pursuant to Article 37 (2) paragraph 2 of the CCTV Ordinance, the casino must have a video system that meets the following requirements in order to perform the tasks provided for in Act LIII of 2017 on the Prevention and Prevention of Money Laundering and Terrorist Financing,

in order to ensure the cleanliness and safe conduct of the game, the protection of order and property, and the prevention and suppression of money laundering and terrorist financing.

Pursuant to Article 7 (9) of the Money Laundering and Terrorist Financing Prevention Act, the Data Controller is entitled to record the image of the natural person's customer and to video record the activity of the customer inside the establishment and to store the image in the electronic image recording system in order to prevent and deter money laundering and terrorist financing, to ensure the interconnectivity of the data obtained during customer due diligence measures and player transactions, and to perform surveillance activities effectively.

The legal basis for the processing is the fulfilment of a legal obligation in accordance with Article 6 (1) (c) of the GDPR, as the obligation to make video recordings is provided for in both Section 37 (7) of the SZTFH Decree and Section 7 (9) of the Pmt. This data processing is mandatory.

The Gambling Supervisory Authority may inspect the data recorded by the video system in order to perform its statutory duties.

Pursuant to Section 37 (7) of the Gambling Control Authority Ordinance, the video system must comply with the following conditions:

(a) All games available in the Casino must be capable of being observed The cameras must be capable of clearly showing and following the stakes (chip colours and legibility), the game devices and additional game devices (dice, cards, balls, etc.), as well as the course of the game on the screen.

(b) Ensure that the loading and unloading of the slot machines, the payment of the jackpot and the separate room for the settlement of the gaming devices and the route to the settlement point can be observed and controlled. If the settlement of gaming devices takes place in a separate room, this room must also be equipped with a camera and the route to the settlement must be monitored.

c) The Casino must have a clear view of any possible disorder in the Casino area and the security measures applied must be observable and recordable throughout the gaming area and at all gaming locations (gaming tables, slot machines, etc.).

d) The Guest's entry and identification process must be verifiable.

e) The cameras must be capable of transmitting images that include the date, time, bets placed, cash and tips received, in detail and with accuracy to the second, so that all events on the gaming equipment are visible at all times. Audio shall be transmitted with the image. A close-up camera (zoom camera) shall be used to record the events that must be documented and those that take place at the cash desk.

f) The images from the cameras shall be kept under constant surveillance by the Controller in accordance with the control system laid down in the Casino's game plan. The footage provided by the cameras shall be recorded simultaneously and shall be kept for the period of time specified in Article 51(4) of the CCTV Regulation.

Duration of processing:

- The period of time for which the video recordings are retained and the settlement proofs are sent shall be set by the Data Controller in accordance with the GSA Regulation so that the GSA has at least five working days after the settlement proofs have been sent to view the video recordings to support the content of any proofs sent. Video recordings and other documents containing the occurrences of incidents in the casino and the measures taken against players shall be kept by the Data Controller for at least 30 days.

- Pursuant to Article 7 (9) Pmt., the Data Controller is obliged to keep the video recordings for 45 days from the date of recording, which period shall be extended by the Data Controller until the conclusion of the supervisory body's proceedings upon the supervisory body's indication.

In the case of CCTV surveillance, this may include guests and players of the Casino, as well as employees working in the Casino.

The Data Controller shall provide and comply with detailed data management rules for the use of the video system for its employees, security and video staff in a separate information notice.

The video system is operated by the Controller and the Controller's employees (casino manager, manager, department manager, camera operator, assistant camera operator, person designated by management) are entitled to access the recordings.

The Data Controller uses live video surveillance and records the recordings.

Location of the recordings: the video servers are located in the dedicated, separate, airconditioned room in the server room.

The cameras operate continuously from 0-24 hours every day.

13. Credit card transactions:

If a Guest purchases a gaming right (ticket or chip) at the Casino's cashier by credit card, the Data Controller will verify the identity of the cardholder. The purpose of the processing is to comply with the requirements of the card accepting partner, to verify the cardholder and thereby to help prevent or detect credit card fraud. The Data Controller records the number and type of the identification document (identity card or passport) used for the verification, the name of the cardholder, the first 4 digits of the card number.

The transaction receipt shall be kept by the Data Controller for 60 months.

Legal basis for processing: legitimate interest of the Controller [Article 6(1)(f) GDPR] (Legitimate interest of the Controller: performance of the contract with the bank, reduction of the number of criminal offences. For more information, see the interest test prepared by the Data Controller.)

The credit card acquiring partner involved in the transactions is entitled to view the transaction receipts.

14. Sending a newsletter containing general marketing offers:

The purpose of the processing is - in accordance with the Grt.In accordance with the provisions of Art. 6 of the GDPR, the Data Controller shall send a newsletter containing marketing information about new features, bonuses, promotions and current events related to its offline casino gaming services to data subjects who have given their prior and explicit consent.

The data processed include: name and surname, date of birth, e-mail address, telephone number (if the data subject requests an SMS notification).

In view of the fact that in the context of sending the newsletter, the Data Controller also advertises a service in which, pursuant to Section 1 (5b) of the Act on the Protection of Personal Data, persons under the age of 18 may not participate, or which is prohibited by the Act on the Protection of Personal Data. Article 8 (1), therefore the Grt.6(2), it is also necessary to record the date of birth.

Furthermore, in order to ensure player protection, the data subject must declare that he/she is not subject to any restrictions based on the data in the player protection register.

The newsletter is sent by e-mail in principle, but the data subject has the option of providing his or her telephone number to receive, as an additional option, shorter information by SMS, in particular about current events of the Data Controller, given the characteristics of the channel.

The legal basis for the processing is the data subject's voluntary, explicit and informed consent in accordance with Article 6(1)(a) of the GDPR (the withdrawal of consent does not affect the lawfulness of processing based on consent prior to its withdrawal).

The duration of the processing shall last until the withdrawal of consent or, in the absence thereof, until the end of the provision of the newsletter service for marketing purposes by the Controller.

Consent may be withdrawn at any time, without restriction and without giving any reason, free of charge, by sending an e-mail to lvc_diamond@lvcd.hu or by post to the Data Controller's head office, or by clicking on the "unsubscribe" link in the newsletter. In addition, the data subject may also unsubscribe at any time by using the link at the end of the SMS message. To ensure the accuracy of the personal data provided during subscription and to prevent incorrect sign-ups, the Data Controller sends a message containing a “confirmation link” to the email address provided by the data subject. The subscription is finalized by clicking on the confirmation link. If the subscription is not confirmed, the Data Controller will send a reminder within 24 hours. If the subscription is still not confirmed within 5 calendar days, all personal data provided in connection with the subscription will be deleted.

15. Raffle:

The Data Controller will from time to time organise a raffle draw in the Casino area.

The raffle ticket will contain the serial number of the raffle and the name and card number of the raffle ticket holder. Filling in the name and card number details and reading the name is a condition of participation in the draw.

Data processed: name, card number.

Purpose of the processing: to publish the name of the winner in the raffle draw, i.e. to read it out (thus identifying the winner).

Legal basis for processing: legitimate interest of the Data Controller [Article 6(f) GDPR] (The legitimate interest of the Data Controller is a commercial, economic interest linked to the interest in maintaining the raffle game.For more information, see the interest balancing test prepared by the Data Controller.)

Duration of processing: the name of the winner will be published orally at the time of the draw.

16. Taking photos and videos:

From time to time, the Data Controller organizes events, competitions and cups.

Photographs and videos may be taken of the participants of the event or competition or of the persons present at the competition venue. The Data Controller will place information about this at the venue of the event.

The purpose of the data management is to document the events organised by the Data Controller with images, to promote the activities of the Data Controller and to make them known to others.

The primary legal basis for the processing is the consent of the data subjects [Article 6(1)(a) GDPR] for persons participating in the event as competitors or players.)

Where it is not possible to obtain consent (not including where the data subject does not wish to give consent) and the legal conditions are met, and in respect of all other persons present at the venue of the event but not participating in the specific tournament or cup, the secondary legal ground for processing is the legitimate interest of the controller [Article 6(1)(f) GDPR].

For more information, see the interest balancing test prepared by the Data Controller.) Scope of

personal data processed: name, image/moving image and sound recording.

Duration of processing: until the data subject's consent is withdrawn or the purpose is achieved.

Data subjects have the right to object to the recording at any time.

Publication of photographs and videos:

Purpose of processing: the Data Controller may publish the recordings on its own Meta platforms (Facebook, Instagram), YouTube and TikTok channels or website, and may transmit them to television and the press for publication. The Data Controller will inform the data subjects in advance, on a case-by-case basis, of the exact methods and places of publication on the spot. The purpose of the publication of the recordings is to promote the Data Controller, its services and events, to present them to others and to make them known.

The primary legal basis for the processing is the consent of the data subjects [Article 6(1)(a) GDPR] for persons participating in the event as a competitor or player (withdrawal of consent does not affect the lawfulness of processing based on consent prior to its withdrawal).

Where it is not possible to obtain consent (not including where the data subject does not wish to give consent) and the legal conditions are met, and in respect of all other persons present at the venue of the event but not participating in the specific tournament or cup, the secondary legal ground for processing is the legitimate interest of the controller [Article 6(1)(f) GDPR]. For more information, see the interest balancing test prepared by the Data Controller.)

Scope of personal data processed: name, image/moving image and sound recording.

Duration of the processing: until the data subject's consent is withdrawn, until the purpose is achieved or, in the case of publication on a social networking site, until the site is operational.

Data subjects have the right to object at any time to any use of the recording.

17. Data processing related to the use of the Website Cookies, web

beacons:

The Website (https://lasvegascasino.hu/) uses cookies and web beacons in the operation of the Website.

A cookie is a small text file that is placed on your computer when you visit a website. Cookies can have a variety of functions, including collecting information, remembering user preferences, allowing the website owner to understand user habits, and some cookies are necessary for the operation and functionality of the website. You can manage your cookie preferences at any time in your browser settings.

Cookies cannot be used to launch programs or to install viruses on your computer.

Cookies may be internal cookies or they may come from third parties depending on whether they are linked to the domain of the website visited by the user. Third-party cookies are linked to a domain that is different from the domain of the website visited by the user.

The Website uses the following cookies:

Cookie name: wpml_browser_redirect_test

Type: technical, essential

Operated by LVC Diamond Kft.

Function: the website uses this to test whether the browser is able to store cookies.

Purpose: if a cookie is created, the website will try to determine the visitor's language preference (English/Hungarian), save it in another cookie, and then redirect the visitor if necessary.

Value: "0"

Personal data to which it has access: -

Expiration: session

Cookie name: _icl_visitor_lang_js

Type: technical, essential

Operator: LVC Diamond Kft.

Function: contains the visitor's language preference (English/Hungarian).

Purpose: to store the visitor's preference when the page is reopened within the expiry time.

Value: "en_US" or "hu_HU"

Expiry date: 24 hours

Cookie name: cookie_notice_accepted

Type: technical, convenience

Hosted by: LVC Diamond Kft.

Function: the cookie is created after the user accepts the warning.

Purpose: if it exists, the cookie usage warning will not be displayed again to the visitor.

Value: "true"

Personal data accessed: -

Expiry date: 1 month

Cookie name: _GRECAPTCHA

Type: technical, essential

Operator: Google reCaptcha

Function: to reduce automated (spam) submissions of contact forms on the website.

Purpose: to provide the visitor with a unique identifier to help Google reCaptcha work.

Value: unique identifier

Personal data accessed: player's actions on the website based on IP address

Expiry date: 6 months

Cookie name: _ga*, _gat*, _gid

Type: analytical

Powered by: Google Analytics

Function: Google Analytics visitor statistics, used to distinguish users.

Purpose: the cookie monitors which website the user came from, how they use the website, what content they view, what they click on, how they scroll the website.

Value: unique identifier

Personal data accessed: player's actions on the website based on IP address

Expiry: 6 months for _ga*, 1 day for _gat*, _gid

Google's privacy policy is available at the following link: https://policies.google.com/privacy?hl=hu

Cookie name: _fbp

Type: analytical

Powered by: Facebook Pixel

Function: Facebook Pixel conversion tracking statistics, used to distinguish users.

Purpose: the cookie monitors which website the user came from, how they use the website, what content they view, what they click on, how they scroll the website.

Value: unique identifier

Personal data accessed: player's actions on the website based on IP address

Expiry date: 3 months

You can set your browsers to use cookies (enable/disable) as follows:

- Internet Explorer: https://support.microsoft.com/hu-hu/help/17442/windows-internetexplorer-delete-manage-cookies

- Microsoft Edge: https://support.microsoft.com/hu-hu/help/10607/microsoft-edgeview-delete-browser-history

- Firefox: https://support.mozilla.org/hu/kb/weboldalak-altal-elhelyezett-sutik-torleseszamito

-GoogleChrome: https://support.google.com/chrome/answer/95647?hl=hu&co=GENIE.Platform=Deskt op

- Safari: https://support.apple.com/hu-hu/guide/safari/sfri11471/mac

In the case of cookies that are necessary for the operation of the website, the processing of personal data is based on the legitimate interest of the Data Controller (the legitimate interest of the Data Controller is the proper operation of its website, which is a business, economic, marketing interest). The consent is given voluntarily.

*

In the course of the processing, the Data Controller will only provide information about the personal data recorded, except for the fulfilment of a legal obligation, with the consent of the Data Subject. The electronic register or programme system containing personal data relating to the Data Subject shall not be linked to any other register or programme system of a different nature or external system. By accessing the website, a log file is created of certain parameters of the Data Subject's computer and its Internet address (IP address), which data is used solely for statistical purposes.

The Controller will disclose user data only in a statistically processed form, not linked to a unique (personal) identifier.

The website may also contain links to other websites, but the Data Controller accepts no responsibility for the content and functioning of other websites.

Considering that the Internet is an open network with security risks, the Data Controller shall not be liable for any damage caused by the destruction, delayed arrival or other failure of data and information transmitted electronically from the website. Furthermore, the Data Controller shall not be liable for any damage resulting from the use of the information on the website, including damage resulting from the partial or total unavailability, obsolescence or loss of data of the website.

Marketing:

Facebook Ads: our company uses the services of Facebook [Meta Platforms Ireland Ltd., 4 Grand Canal Square, Grand Canal Harbour, Dublin 2, Ireland] to serve targeted ads on Facebook. Meta is the data controller for these ads and will ensure that consent is obtained. We do not process any personal data in connection with the advertisements. For more information, please visit https://hu-hu.facebook.com/business/gdpr#faqs. https://www.facebook.com/business/help/170456843145568?id=2469097953376494

Facebook Pixel: our company has integrated the Facebook Pixel code into its website, which is a service of Meta. This allows Facebook to track the activity of users registered on Facebook on our website. We can create target audiences and get analytics data on how visitors use our website. With Facebook Pixel, we can optimise our ads and provide personalised offers to visitors to our website. The data is stored and processed by Facebook, our company does not process any personal data, Facebook does not transfer any personal data to our company.

Google Tag Manager: the website uses Google Tag Manager. Google Tag Manager is a solution that allows marketing professionals to manage the administration of tags on the website in a consolidated way, through a single interface. The tool is a cookie-free domain and does not collect any personal data, it only takes care of activating other tags which, under certain

circumstances, collect data on their part. Google Tag Manager does not have access to such data. If the feature is disabled at the domain or cookie level, it will remain in effect for all tracking tags that have been implemented with Google Tag Manager. More information on how Google Tag Manager works can be found at https://support.google.com/tagmanager/#topic=3441530) Visitor measurement:

Data processed: the IP address of visitors to the Website (https://lasvegascasino.hu/), the time of the visit, the pages viewed, the name of the browser program used.

Purpose of data processing: the software that analyses the website traffic data is run on the website of the Data Controller.

Legal basis for the processing: consent of the data subject [Article 6(1)(a) GDPR]. (Withdrawal of consent does not affect the lawfulness of processing based on consent prior to its withdrawal.)

Duration of processing: until the purpose is fulfilled, but no later than the date of erasure at the request of the data subject.

The web server and web storage space of the website of the Data Controller are operated by Rendszerinformatika Zrt. (1134 Budapest, Váci út 19. ; company register number:
01-10-046912; tax number: 23095942-2-41) as data processor.

18. Personal data processing in connection with the use of electronic mail (e-mail):

The Data Subject has the possibility to contact the Data Controller by e-mail at mail@vegas.hu or by sending a message to the Data Controller via the interface available under the "Contact" section of the Website
(https://lasvegascasino.hu/kapcsolat/).

If the e-mail contains other personal data, the communicator is obliged to obtain the prior consent of the Data Subject, which the Data Controller presumes to have been obtained.

The scope of the data processed: name, e-mail address.

Purpose of processing: to contact the Data Controller.

Legal basis for processing: consent of the data subject [Article 6(1)(a) GDPR]. (Withdrawal of consent does not affect the lawfulness of processing based on consent prior to its withdrawal.)

Duration of processing: until the purpose is fulfilled or until erasure at the request of the data subject.

19. Personal data processing in connection with the use of the Community Site Data

processed: name, comment, follow, message, rating.

Purpose of data processing: to inform the data subjects about the operation, events and programmes of the Data Controller via the Facebook and Instagram pages of the Data Controller, and to promote the Data Controller.

Legal basis for processing: consent of the data subject [Article 6(1)(a) GDPR]. (Withdrawal of consent does not affect the lawfulness of processing based on consent prior to its withdrawal.)

Data subject: person who carries out activities in relation to the site.

Duration of the processing: until the deletion of the data subject's request, but at the latest until the site is operational.

Facebook pages of the Data Controller: https://www.facebook.com/LVCEuroCenter

https://www.facebook.com/lasvegastropicana https://www.facebook.com/lasvegassofitel

https://www.facebook.com/lasvegascorvin https://www.facebook.com/lasvegasatlantis

https://www.facebook.com/eurocenterpoker Instagram page of the Data Controller:

https://www.instagram.com/lasvegascasinos_official/

To use the Facebook and Instagram pages, the Data Subject must have an account on the social networking site.

The operators of the social media sites carry out processing as independent data controllers in accordance with their own privacy policy. The data controller of Facebook and Instagram is Meta Platforms Ireland Ltd., 4 Grand Canal Square, Grand Canal Harbour, D2 Dublin Ireland. By using Facebook and Instagram, the data subject declares that he or she has read and accepted the Facebook and Instagram terms of use and privacy policy:

https://www.facebook.com/policy.php https://www.instagram.com/terms/accept/?hl=hu

Facebook and Instagram receive the information that the data subject wishes to post on the social networking site of the gaming casino under the IP address of the data subject.

With regard to the data (name, photo, comment, rating) that the Data Subject wishes to post, he/she can exercise his/her rights directly to Facebook or Instagram or contact the Data Controller.

The Data Controller is entitled to initiate the deletion of data that violate the reputation or rights of the Data Controller or any other person.

The processing of data for statistical purposes in connection with the use of MetaProducts is carried out jointly by the Data Controller and Meta Platforms Ireland Ltd., 4 Grand Canal Square, Grand Canal Harbour, D2 Dublin Ireland. Detailed information about the site analytics is available at the following link:

https://www.facebook.com/legal/terms/page_controller_addendum YouTube channel

of the Data Controller:

https://www.youtube.com/@lasvegascasinobudapest

For detailed information on the processing of data on the YouTube channel, please refer to the Google Privacy Policy and Terms & Conditions: https://policies.google.com/privacy?hl=hu

The Data Controller's TikTok channel:

https://www.tiktok.com/@lvc_budapest?_t=ZN-8ub9syUDQiE&_r=1

To use TikTok, the Data Subject must have an account. The operators of TikTok carry out data processing as independent data controllers in accordance with their own data processing policy. The data controller of TikTok is TikTok Technology Limited - a social media service (registered office: 2 Cardiff Lane Grand Canal Dock, Dublin; Website: https://www.tiktok.com/)

TikTok's privacy policy is available at the following link: https://www.tiktok.com/legal/page/eea/privacy-policy/hu

20. Personal data processing in connection with the use of WiFi networks:

The Data Controller provides free and open internet access in the Casinos area, without any liability for the risks involved in the use of wireless internet.

By connecting to the wifi network, the Data Subject expressly consents to the Controller recording the MAC address of the device used by the Data Subject for the purpose of uniquely identifying the Data Subject for the duration of the use.

The scope of the data processed: MAC address, device name.

Purpose of the processing: the use of the service provided by the Data Controller.

Legal basis for the processing: consent of the data subject [Article 6(1)(a) GDPR]. (Withdrawal of consent does not affect the lawfulness of processing based on consent prior to its withdrawal.)

Duration of processing: until the purpose is fulfilled, but no later than the date of erasure at the request of the Data Subject.

21. Recording calls to a central telephone number:

Purpose of processing: to prevent unlawful acts and to ensure lawful operation.

Data processed: time of call (day, hour, minute); caller number, extension called; voice of the parties involved in the conversation, any personal data/information recorded during the conversation.

Legal basis: legitimate interest of the Data Controller [Article 6(1)(f) GDPR]. The Data Controller has carried out an interest balancing test in a separate document.

Duration of processing: 7 calendar days after the recording was made. If the data subject objects to the processing of his/her personal data subject to the processing and there are no overriding legitimate grounds, the Controller shall erase the personal data.

If a public authority, including the Hungarian Police, sends a request to the Controller, the Controller shall comply with the request on the basis of a legal obligation. In certain cases, the Data Controller may initiate proceedings with the authorities.

22. Event pre-registration

Purpose of processing. The purpose of our collection of data is to enable the Data Controller to identify the person who has pre-registered in order to ensure the necessary capacity.

Data processed: name and e-mail address of the Guest who pre-registered, the selected event and its date and the number of persons accompanying the Guest.

Legal basis: the data subject's consent [Article 6(1)(a) GDPR]. (Consent may be withdrawn at any time, but this does not affect the lawfulness of the processing carried out on the basis of consent before its withdrawal.)

The duration of processing is until the consent is withdrawn or, in the absence thereof, until the end of the selected event.

VI. Transfer of data:

Pursuant to Section 36 of the Gambling Supervision Act, the Gambling Supervision Authority is entitled to request statements, data, supporting documents, inspection materials and to carry out on-site inspections at any time concerning activities falling within the scope of the Gambling Supervision Act.

In cases of suspected money laundering, the National Tax and Customs Administration shall act.

AMATIC Industries Gmbh (A-4845 Austria, Rutzenmoos, Traunsteinstrasse 12.; office@amatic.com, tel: +43 (0)7672 29600; company registration number: FN 33564i; website: https://www.amatic.com/company/profile/) acts as a data processor, providing back-office IT services for the following tasks:

- during player registration;

- for the registration of players in the register of players

- during access control,

- ticket, token and money exchange;

- player protection register (data concerning a player under self-imposed restriction, player on the player protection register).

VII. Enforcement and redress

The following is a summary of the rights that the Guest may exercise against the Controller.

1. Communication with the Data Controller, right of access: communication between the Guest and the Data Controller takes place at the Casino in person, orally or in writing (in the form of a private document with full probative value) or, if the e-mail is identifiable, by e-mail. The Guest has the right to request feedback from the Controller at any time as to whether his/her personal data is being processed and, if it is being processed, the Data Subject has the right of access to the personal data processed, to the extent set out below.

The Customer shall have the right to request clarification from the Controller regarding the processing of the data, including the following information, which the Controller shall provide without undue delay and at the latest within 1 month of the request for information. In particular, the information provided by the Controller in the context of the access to the processing may include:

a) the purposes of the processing;

b) the personal data processed;

c) the recipients of the transfers;
d) the expected duration of the processing or, where it is not possible to determine this, the criteria for determining the duration;
e) the rights of the Customer under the Infotv. and the GDPR and the means of enforcing them;
f) the right to lodge a complaint with the Authority;
g) the source and legal basis of the information collected by the Data Controller;
h) in the case of transfers of personal data processed, the recipients of the transfers, including recipients in third countries and international organisations;
i) where automated decision-making or profiling is used, the fact that it is used.

The Data Controller shall provide a copy of the personal data subject to the processing to the Customer upon request. The Controller may charge a reasonable administrative fee for additional copies requested by the Guest.

a) The Data Controller shall examine and reply to an e-mail sent by the Customer in connection with the processing if it is sent from an e-mail address previously provided by the Customer (unless the Customer refers in the message to a change of e-mail address or the Customer's identity can be clearly identified from the e-mail address).

b) The Data Controller shall inform the Customer of any action taken with regard to personal data without delay and at the latest within 1 month after the action has been taken.

c) If the Data Controller does not take action on the request of the Guest, the Data Controller shall inform the Guest without delay, but at the latest within 1 month of receipt of the request, of the reasons for the failure to take action and of the possibility for the data subject to lodge a complaint with the Authority and to exercise his or her right of judicial remedy.

d) The record relating to the ban may be consulted by the banned Guest in relation to the details of the ban affecting the Guest. At the same time as the inspection, the Guest may request the issue of a document on the recorded data, which the Casino shall provide free of charge at the same time as the inspection, but no later than the following working day (Section 1 (5c) of the Act on the Protection of the Rights of the Child).

2. Correction: the Customer is entitled and obliged to notify the Data Controller (in writing or in person) within 5 working days of becoming aware of any changes to the data provided during the customer due diligence (i.e. the issuing of the access card) during the business relationship and in accordance with Article 12 (3) of the Pmt. If the Customer fails to notify the change in his/her personal data without delay, the consequences thereof shall be borne by the Customer.

If the personal data provided is not accurate and the accurate personal data is available to the Data Controller, the Data Controller shall automatically correct the personal data.

3.Request for erasure: the Guest has the right to request the erasure of personal data relating to him/her by the Data Controller without undue delay, and the Data Controller is obliged to erase personal data relating to the Guest without undue delay, in particular if one of the following grounds applies:

a) the personal data are no longer necessary for the purposes for which they were collected or otherwise processed;

b) the Customer withdraws his consent to the processing and there is no other legal basis for the processing;

c) the Data Subject objects to the processing based on legitimate interests;

d) the personal data have been unlawfully processed by the Controller;

(e) the personal data must be erased in order to comply with a legal obligation under Union or Member State law to which the controller is subject;

(f) the personal data have been collected in connection with the provision of information society services referred to in Article 8(1) of the GDPR.

Even in the above cases, the Controller is not obliged to delete the personal data processed, if the processing is necessary:

a) for the exercise of the right to freedom of expression and information;

(b) to comply with an obligation under Union or Member State law to which the controller is subject to which requires the processing of personal data, or in the public interest;

(c) for statistical or archiving purposes or for scientific or historical research purposes, where deletion is likely to render such processing impossible or seriously jeopardise it;

(d) on grounds of public interest in the field of public health pursuant to Article 9(2)(h) and (i) and Article 9(3) of the GDPR;

(e) for the establishment, exercise or defence of legal claims.

4.Right to restriction of processing: the Guest has the right to have the Controller restrict processing at his/her request, if one of the following conditions is met.

a) The Customer contests the accuracy of his/her personal data, in which case the restriction shall apply for the period of time necessary to allow the Controller to verify the accuracy of the personal data.

b) The processing is unlawful and the Customer opposes the erasure of the personal data and requests instead the restriction of their use.

(c) The Controller no longer needs the personal data to fulfil the purpose of the processing, but the Customer requires them for the establishment, exercise or defence of legal claims.

d) The Guest has objected to the processing, in which case the restriction shall apply for a period of time until it is established whether the legitimate grounds of the Controller prevail over the legitimate grounds of the Guest.

Where processing is restricted as described above, such personal data may be processed, except for storage, only with the consent of the Guest or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person, or for important public interests. If the restriction of processing is lifted, the Customer requesting the restriction shall be informed in advance by the Controller of the fact of the restriction.

5.Objection to processing: the Data Subject has the right to object, on grounds relating to his or her particular situation, at any time to the processing of his or her personal data under this Notice on the basis of legitimate interest. In such a case, the Controller may no longer process the personal data, unless the Controller proves that the processing is justified by compelling legitimate grounds which override the interests, rights and freedoms of the Data Subject or are related to the establishment, exercise or defence of legal claims.

6. Right to data portability: with regard to personal data processed on the basis of the consent of the Guest or for the performance of the contract, the Guest has the right to have the personal data concerning him/her that he/she has provided to the Controller in a structured, commonly used, machine-readable format, and the right to transmit such data to another controller without hindrance from the Controller to whom he/she has provided the personal data. This right may be exercised only in respect of personal data processed on the basis of consent or on the legal basis of the performance of a contract.

7. Initiation of the Authority's procedure: the Guest may lodge a complaint with the Authority to initiate an investigation on the grounds that there has been or is an imminent threat of a breach of rights in relation to the processing of his/her personal data. The Authority's investigation is free of charge and the costs of the investigation are advanced and borne by the

Authority. No person shall suffer prejudice as a result of having made a notification to the Authority. The Authority may disclose the identity of the person lodging the complaint only if it would not be possible to carry out the investigation if this were not done. If the notifier so requests, the Authority may not disclose the identity of the notifier even if the investigation cannot be carried out without it. Contact details of the Authority: 1055 Budapest, Falk Miska u. 9-11.; e-mail: ugyfelszolgalat@naih.hu; website: http://naih.hu; telephone: +36 (1) 391-1400.

8. Enforcement before the court: the Guest may bring an action against the Data Controller for violation of his/her rights before the court, the court having jurisdiction. As a general rule, the competent court is the court in the place where the Data Controller is established. The jurisdiction of the court can be checked by using the "Court Search" application on the website www.birosag.hu. The tribunal will decide the case out of turn.

9:

a. causes damage to the Guest or to another person, the Data Controller is obliged to compensate the damage (compensation);

b. infringes the personal rights of the Guest, the Guest may claim damages from the Data Controller.

The Controller shall be exempted from liability for the damage caused and from the obligation to pay compensation if it proves that the damage or the infringement of the Guest's personality right was caused by an unforeseeable cause outside the scope of the processing. No compensation shall be due and no damage fee shall be payable if the damage or the infringement of the right to privacy was caused by the intentional or grossly negligent conduct of the Guest (the victim) (Art. 24 of the Data Protection Act).

VIII. Miscellaneous Provisions

1. Pursuant to Section 29/T of the Gambling Act, the Data Controller is entitled to apply a unified entry and identification system for the land-based casinos and online casinos operated by the Data Controller.

2. This Privacy Notice is governed by Hungarian law. In the event of any dispute related to this Privacy Notice, the Hungarian version shall prevail.

3. For matters not regulated in this Privacy Notice, the Casino Participation Rules and the relevant provisions of Hungarian law shall apply.

4. The full and currently effective text of this Privacy Notice is continuously and freely accessible at the Casino.

5. The Data Controller reserves the right to unilaterally amend this Privacy Notice at any time. Budapest, 29 October 2025

LVC Diamond Ltd.