PRIVACY POLICY
LAS VEGAS CASINO TROPICANA/ATLANTIS/CORVIN SÉTÁNY/ATRIUMEUROCENTER

Welcome to the Las Vegas Casino Tropicana/Atlantis/Corvin SétányAtrium EuroCenter Casinos!

In order to use the services available at the casinos – in accordance with legal requirements – you are required to provide us with certain personal data.

The controller of the personal data you provide is LVC Diamond Kft**,** the operator of the Las Vegas Casino Tropicana/Atlantis/Corvin Promenade/Atrium EuroCenter casinos **('Controller').**

The purpose of this Data Protection Notice (hereinafter: **Policy**) is to set out, in accordance with the relevant legal provisions, the data processing principles, purposes and other facts that determine the purpose, duration and manner of processing the personal data you provide, as well as your rights and remedies in relation to such processing.

The security and proper processing of the personal data you provide to us is of paramount importance to us; therefore, please read the contents of this Notice carefully and with attention. If you have any questions or comments regarding the information provided here, please do not hesitate to contact us before accepting this Notice.

I. Who is the Controller of my personal data, and whom can I contact?

Name of the data controller: LVC Diamond Kft.

Registered office and postal address: 1088 Budapest, Rákóczi út 1–3, 3rd floor

Email: adatvedelem@lvcd.hu

Telephone number: +3612662081

Name and contact details of the authorised representative:

Name: Dr Róbert Dravecz, Managing Director

Postal address: 1088 Budapest, Rákóczi út 1–3, 3rd floor

Email: adatvedelem@lvcd.hu

In order to ensure the highest possible level of protection for the personal data processed and to minimise the risks associated with data processing operations, the Controller has appointed a Data Protection Officer.

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

Name: Lajer Law Firm

Registered office and postal address: 1133 Budapest, Pannónia u. 77-79, 1st floor 109

Email: DPO.LVC@lajer.net

II. What do the terms used in this Policy mean?

Below, in accordance with Article 4 of the GDPR, we summarise the most important terms used in this Notice.

1. **Personal data:** any information relating to the Guest which enables the Guest to be identified or to be identifiable. A natural person is considered identifiable if they can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification 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 Controller collects the personal data from the Guest specified separately for each data processing purpose indicated in this Notice.

2. **Data controll:** any operation or set of operations performed on data, irrespective of the procedure used, including, in particular, collection, recording, organisation, storage, alteration, use, retrieval, transmission, disclosure, alignment or combination, restriction, erasure and destruction, as well as the prevention of further use of the data.

3. **Controller:** the data provided by the Guest is processed by LVC Diamond Kft. (registered office and postal address: 1088 Budapest, Rákóczi út 1–3, 3rd floor; company registration number: 01-09-194087 [registered with the Company Registry of the Budapest Metropolitan Court]; tax number: 25002889-4-44; email: adatvedelem@lvcd.hu) shall process the data provided by the Guest; that is, only LVC Diamond Kft. may make and implement decisions relating to the Guest's personal data.

4. **Processing:** any operation or set of operations which is performed on personal data or on sets of personal data, in the name of the Controller irrespective of the place, the mean, and the method the operation is carried out with , insofar as the operation is performed on the data. Accordingly, a data processor is any natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller.

5. **Data transfer:** making data available to a specific third party.

6. **Recipient:** any natural or legal person, public authority, agency or any other body to whom or to which personal data is disclosed, regardless of whether they are a third party.

7. **Casino:** the gaming casino operated by the Controller in accordance with the Szjtv. and the relevant legislation.

8. Act XLVIII of 2008: Act XLVIII of 2008 on the basic conditions and certain restrictions of commercial 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. **Supervisory Authority:** the National Authority for Data Protection and Freedom of Information (address: 1055 Budapest, Falk Miksa utca 9–11; email: ugyfelszolgalat@naih.hu; website: http://naih.hu; telephone: +36 (1) 391-1400).

11. **Website:** www.lasvegascasino.hu

12. **IP address**: a unique network identifier used to identify devices using the TCP/IP network protocol, which is necessary for internet use. Every IT device connected to the internet has a unique IP address through which it can be identified.

13. **Cookie:** a data packet (file) generated by a web content server and transmitted to the web browser. Cookies may contain information about searches carried out on the relevant web server and details entered by the user, which are also stored on the server. The primary purpose of using cookies is to store user profile information, primarily to retain the user's preferred settings, thereby allowing the user to access the website in the usual manner.
    Cookies are stored by the browser in a separate directory on the devices used by the data subject (computer, tablet, smartphone, etc.). A cookie uniquely identifies the user and the device they use on the internet, making them recognisable to the web server. The GDPR classifies cookies and other identifiers stored on the device used by the user as personal data.

14. Web beacon (web bug): images on websites or in emails that are invisible to the human eye, which make it possible to track and measure actions performed by users (e.g. opening a newsletter, clicking on URLs [links], etc.). Web beacons are usually used in conjunction with cookies, thereby providing additional information for the creation of user internet profiles.

15. **Gambling Act:** Act XXXIV of 1991 on the Organisation of Gambling.

16. **Gaming Organisation Decree:** Decree No. 5/2021 (21 October) of the Hungarian Gaming Authority (SZTFH) on the detailed rules of responsible gaming organisation, as currently in force.

17. **SZTFH Decree:** SZTFH Decree No. 20/2021 (29 October) on the performance of tasks relating to the licensing, operation and supervision of certain games of chance, as currently in force.

18. **Pmt.:** Act LIII of 2017 on the prevention and combating of money laundering and terrorist financing.

19. **Terms and Conditions:** The Casino's Terms and Conditions in force at any given time.

20. **Service:** any service available to the Guest at the Casino.

21. **Guest:** any natural person aged 18 or over who uses the Casino's services in accordance with the Rules of Participation and the provisions of the relevant legislation.

22. **Consumer Protection Act:** Act CLV of 1997 on consumer protection

23. **SZTFH2 Decree:** on the implementation of Act LIII of 2017 on the prevention and combating of money laundering and terrorist financing, and Decree 4/2021 (X. 21.) SZTFH on the detailed rules governing the minimum requirements for the development and operation of a screening system pursuant to Act LII of 2017 on the implementation of financial and asset-related restrictive measures ordered by the European Union and the United Nations Security Council.

III. What principles apply to data processing?

The processing principles that theController fully applies throughout the entire duration of data processing are summarised below.

1. **Lawfulness, fairness and transparency:** data processing is in all cases based on statutory requirements (in particular the provisions of the Szjtv.) and, where applicable, on the Guest's

express prior consent given when using the relevant Service. The 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 take place exclusively by lawful and fair means, and in a manner that is transparent to the Guest. The Controller shall make the current version of this Notice available and accessible free of charge, without obligation, on a continuous basis and publicly within the Casino premises. The Controller shall not process the personal data provided for any unfair purposes or for any purposes other than those set out in this Policy; in its data processing activities, it shall at all times act in accordance with the provisions of this Policy and the applicable legislation.

2. **Purpose limitation:** the Controller may process personal data solely for the clear and lawful purposes specified in this Notice and in the relevant legislation (in particular the Pmt., the Szjtv. and the SZTFH Regulation). If the Controller wishes to process the personal data already provided for a purpose other than those specified, the Controller shall inform the Guest of this in advance and in full (primarily by email). To ensure full transparency regarding the specific purposes of data processing, the Controller provides information in this Notice as to the purpose, duration and legal basis for the processing of each item of personal data. The Controller applies all these provisions as binding upon itself.

3. **Storage limitation:** the Controller ensures that the Guest's personal data is stored in a form that allows the identification of data subjects only for as long as it is necessary to achieve the purposes of processing the personal data or for the period prescribed by the applicable legislation.
   Personal data processed exclusively on the basis of the Guest's explicit and voluntary consent in accordance with Article 6(1)(a) of the GDPR shall be processed by the Controller until the Guest requests erasure or withdraws their consent.
   Unless otherwise provided by law, the Controller is obliged to retain personal data processed in accordance with the provisions of the Pmt. for a period of 8 years from the termination of the business relationship with the Guest, in all cases pursuant to Sections 56–57 of the Pmt.
   Pursuant to Section 58(1) of the Pmt., notwithstanding Section 56(2) and Sections 57(1)–(3) of the Pmt., the Controller shall retain the data and documents specified therein, at the request of the gambling supervisory authority, the financial intelligence unit, the investigating authority, the public prosecutor's office and the court for the period specified in the request, but for no longer than ten years from the termination of the business relationship or the completion of the transaction. The provisions of this paragraph shall apply to all data processing subject to the Pmt. where the conditions set out in this paragraph are met, even if the retention period applicable as a general rule for the specific data processing is specified.

4. **Data minimisation:** in order to provide the Services to the highest possible standard, the Controller processes only the personal data that is strictly necessary. In all cases, this refers to personal data that is appropriate, relevant and genuinely necessary for the actual use of the Service in question, from the perspective of the purpose of data processing.

5. **Accuracy:** The Controller's aim is to ensure that personal data already recorded is kept up to date at all times in order to provide the highest possible standard of Services and to fulfil its legal obligations (Section 12(1) of the Personal Data Protection Act). The Guest is also obliged to assist in keeping the data up to date; thus, during the existence of the business relationship, the Guest is obliged to notify the Controller within five working days of becoming aware of any changes to the data provided during the customer due diligence process in accordance with the Pmt.

6. **Data protection (integrity and confidentiality):** the Controller attaches the utmost importance to the protection of the personal data provided and the Guest's privacy. The 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 data protection and

confidentiality rules. In order to ensure a high level of data protection, the Controller shall only engage data processors who provide appropriate guarantees regarding the adequacy of data processing and the implementation of appropriate technical and organisational measures to ensure the protection of the rights of Data Subjects (Article 28(1) of the GDPR). The Controller protects personal data by appropriate measures, in particular against unauthorised access, alteration, disclosure, erasure or destruction, as well as against accidental loss or damage, and against becoming inaccessible due to changes in the technology used (including, in particular: password protection; encryption procedures; data recovery in the event of data loss).

IV. What personal data is processed, for what purposes and under what conditions?

Below we summarise the scenarios (data processing purposes) in which the processing of the Guest's personal data takes place in practice.

1. **Issuing access cards, record-keeping, provision of the Service, customer relations:**
   The purpose of data processing, in accordance with the provisions of the Pmt. (Section 7) and the Szjtv. (Section 29/H), is to carry out customer due diligence measures as required by the Pmt., to ensure player protection, and to provide the Service offered by the Controller.

   (A) Customer due diligence, customer identification

   Upon registration:
   Pursuant to the Pmt., the Controller is obliged to identify the player (as a customer) in order to issue an access card, in connection with which it must record their personal data, inspect and copy their identity document, their document proving the right of residence for foreign nationals or their document authorising residence, including their visa. The provision of this data is a prerequisite for visiting the Casino.
   Purpose of data processing: customer identification and screening.
   Personal data processed: surname and first name, surname and first name at birth, nationality, place and date of birth, mother's maiden name, address (or, in the absence thereof, place of residence); as well as the following personal data processed on the documents: ID number, date of issue, validity, issuing authority, photograph, and, depending on the type of document: the Guest's gender and signature; as well as the Guest's risk classification, and, where Section 9/A(2) of the Pmt. applies, the source of funds and assets. This data processing is mandatory; without it, the Guest cannot use the Service.
   Legal basis for data processing: compliance with a legal obligation [GDPR Article 6(1)(c)], Sections 7(2), (3) and (5), Section 3(19)(a), Section 6/A, Section 9/A, Section 16 and Section 16/A of the Pmt., and, with regard to images, Section 7(9) of the Pmt. as well, SZTFH Regulation, Sections 7 and 9.10.
   Duration of data processing: The Controller is entitled to process personal data for a period of 8 years from the termination of the business relationship, in accordance with Section 56(2) of the Personal Data Protection Act.

   Customer identification upon entry:
   Pursuant to Section 39(1) of the SZFTH Regulation, the Controller is obliged to carry out identification in accordance with the provisions of the Pmt. when admitting players, and the time of the player's entry must also be recorded and registered.

   (B) Declaration by public figures

   The player is required to declare whether they qualify as a politically exposed person, a close relative of a politically exposed person, or a person closely associated with a politically exposed person.
   Purpose of data processing: customer due diligence, recording of public figure status.
   Personal data processed: name, public figure status, category as defined in Section 4(2)–(4) of the Pmt., source of funds and assets. This data processing is mandatory; without it, the Guest cannot use the service.

Legal basis for data processing: compliance with a legal obligation [Article 6(1)(c) of the GDPR], Section 9/A of the Pmt.
Duration of data processing: the Controller is entitled to process personal data for a period of 8 years from the termination of the business relationship pursuant to Section 56(2) of the Pmt.

(C) Photograph

The Controller, in order to prevent and obstruct money laundering and the financing of terrorism, to ensure the linkability of data obtained during customer due diligence measures and player transactions, and for the purpose of effectively carrying out supervisory activities, the Controller is entitled to record the Guest's image and store it in its electronic record-keeping system.
Personal data processed: image (photograph). This data processing is mandatory; without it, the Guest cannot use the Service.
Legal basis for data processing: Section 7(8) and (9) of the Pmt.
Duration of data processing: the Controller is entitled to process personal data for a period of 8 years from the termination of the business relationship pursuant to Section 56(2) of the Pmt.

(D) Entry Card

The Controller is obliged to provide Guests with an access card upon their first entry into the Casino.
Purpose of data processing: to issue an entry card and to identify the Guest upon entry.
The entry card and its registration system contain the data specified in Section 41(2) of the SZTFH Decree: the serial number of the entry card; the full name of the person entering (Guest); the date of issue of the entry card; the validity period of the entry card; the Casino's stamp impression or other distinguishing mark.
Legal basis for data processing: compliance with a legal obligation [Article 6(1)(c) of the GDPR], Section 41 of the SZTFH Regulation. This data processing is mandatory; without it, 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) Recording of entries

The Controller is obliged to record and register the time of the Guest's entry, as well as the time of any attempt to enter the Casino despite being listed in the player protection or self-exclusion register.
Personal data processed: name, time of entry, number of entries. This data processing is mandatory; without it, the Guest cannot use the Service.
Legal basis for data processing: compliance with a legal obligation [Article 6(1)(c) of the GDPR], Section 39(1) of the SZTFH Regulation.
Duration of data processing: in accordance with Section 39(1) of the SZTFH Regulation and Section 56(2) of the Pmt., for a period of 8 years from the termination of the business relationship.

(F) Computerised (reception) records

The Controller uses a computerised (reception) register regarding Guests to facilitate access control, in which it is entitled to process the following personal data – unless stated otherwise in the Data Protection Notice – for a period of 8 years from the termination of the business relationship:

i. Based on points A) to D) above: surname and first name; access card number, status, date of issue and expiry date; type, issuer, number, expiry date and date of issue of the identity document; place and date of birth; birth name; nationality; mother's name; address or place of residence; public figure status; photograph; copy of the identity document; Guest's signature.
ii. The number of entries based on point E) above.

iii. **The Guest's gender:** based on the Controller's legitimate interest [Article 6(1) (f) of the GDPR], the Controller records the gender of all Guests for the purpose of ensuring communication (addressing) appropriate to their gender, and so that this data may also be used in the case of non specific games. The duration of the processing of this data extends until the termination of the business relationship or until the data subject objects. (The Controller's legitimate interest: a business and economic interest linked to the organisation of various types of games and the provision of a high standard of Service. Further information is contained in the data protection impact assessment prepared by the Controller.)

iv. **VIP classification**: the Controller – on the basis of its legitimate interest [Article 6(1) (f) of the GDPR] – may classify the Guest into different VIP tiers according to its own classification system in order to provide various discounts and levels of convenience. The duration of the processing of this data extends until the termination of the business relationship or until the data subject objects. (The Controller's legitimate interest: a business and economic interest linked to the interest in increasing the use of the Service. Further information is contained in the data subject's interests assessment test prepared by the Controller.)

v. **Note regarding the profile:** the Controller is entitled to record in the register containing the Guest's profile other information which may be of an administrative nature; such information may be necessary to ensure compliance with the Casino's rules (e.g. a dress code issue has arisen), or may be of a security nature (the Guest is subject to self-exclusion). The duration of this data processing extends until the termination of the business relationship or until the data subject objects. This data processing is carried out on the basis of the Controller's legitimate interest [Article 6(1) (f) of the GDPR]. (The Controller's legitimate interest: a business and economic interest linked to the interest in ensuring the security of service use, maintaining player trust and long-term effective operation. Further information is contained in the data protection impact assessment prepared by the Controller.)

vi. **Email address, telephone number**: based on the Guest's consent, they may voluntarily provide their email address or telephone number – pursuant to Article 6(1) (a) of the GDPR. The purpose of data processing is to maintain contact and to notify the Guest. The duration of the processing of this data lasts until the termination of the business relationship or the withdrawal of the Guest's consent. (The withdrawal of consent does not affect the lawfulness of data processing carried out on the basis of consent prior to withdrawal.)

vii. **Risk classification:** the Controller is obliged to determine the Guest's low, medium or high risk level upon the establishment of the business relationship and to record this in writing [Article 6(1)(c) of the GDPR], pursuant to Section 6/A of the Pmt. This data processing is mandatory; without it, the Guest may not use the Service. Pursuant to Section 56(2) of the Decree, this data processing shall continue for 8 years from the termination of the business relationship.

2. **Recording of unclaimed tokens (orphans):**
The purpose of data processing is to keep a record of refunded sums of money. Orphans include, for example, unclaimed chips found on the Casino premises (e.g. left on a gaming table or forgotten there during play) that can be used as stakes, where the Organiser has not identified the lawful owner by the end of the gaming day, as well as anything defined in Section 44 of the SZTFH Regulation. Any Guest who proves their ownership of the unclaimed items shall be reimbursed this sum of money – in the case of chips, the amount corresponding to their value – and the reimbursed sum shall be recorded in the register of unclaimed items.
The register of orphans shall contain the following personal data: the name of the Guest entitled to the value of the orphans; their place of residence; the date of repayment; the amount; and, in the case of a ticket, its unique identifier. If the organiser has conducted an investigation to determine the legitimacy of the claim made by the person claiming the value of the orphan, the minutes containing the results of the investigation relating to the incident must be attached to

the register of orphans. This data processing is mandatory; without it, the Guest cannot use the Service.
The legal basis for data processing, as set out above, is compliance with a legal obligation in accordance with Article 6(1)(c) of the GDPR.
Duration of data processing: 6 years pursuant to Section 7a(1) of the Accounting Act, followed by a further 2 years in accordance with the Accounting Act in force at the time (i.e. 8 years from the date of the accounting event).

3. **Prize certificate:**
The purpose of data processing – at the request of the Guest entitled to the prize – is to issue a certificate attesting to the legal title and forint value of any prize exceeding 2 million forints or the equivalent amount in foreign currency.
The prize certificate contains the following personal data: the Guest's identification details, the place and time of the win and the collection of the prize (Section 1(8) of the Act on the Protection of Personal Data). This data processing is mandatory; without it, the certificate cannot be issued.
The legal basis for data processing is, as stated above, 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 1(7a) of the Accounting Act, followed by a further 2 years in accordance with the Accounting Act in force at the time (i.e. 8 years from the date of the accounting event).

4. **Deposit register:**
The purpose of data processing is to keep a record of the chips and cash deposited by the Guest, as set out in the Rules of Participation.
The deposit register contains the following personal data: the identifying details of the Guest making the deposit, the denomination and amount of the chips and cash deposited, and the date of deposit.
Legal basis for data processing: the Controller's legitimate interest [Article 6(1)(f) of the GDPR]. (The Controller's legitimate interest: a business and economic interest linked to the need to prove, ensure the security of, and keep a record of the use of the deposit service. Further information is contained in the data protection impact assessment prepared by the Controller.)
Duration of data processing: 5 years (until the limitation period under the Civil Code expires).

5. **Exclusion register:**
Legal basis for data processing: compliance with a legal obligation pursuant to Section 1(5c) of the Gambling Act. The Controller maintains a register for the purpose of effectively enforcing the refusal of entry and participation in gambling (hereinafter: exclusion) against Guests who seriously breach the Rules of Participation.
The ban register – pursuant to Section 1(5c) of the Gambling Act – contains the following personal data:
   a) the Guest's details as specified in Section 29/H(1) of the Gambling Act: surname and first name, surname and first name at birth, mother's name; address, or place of residence if no address is available; nationality; type and number of identity document; place and date of birth;
   b) the fact of the ban, the reason for it, and the date it was imposed; and
   c) the ad hoc nature of the ban or its fixed duration of up to 5 years.

The Controller may transfer the data from the exclusion register to other casinos operated by the Controller, and may also apply the exclusion imposed on the Guest to these casinos in accordance with Section 25(2) of the Gaming Organisation Regulation.
The Controller may process the data in the exclusion register for a period of 6 years from the date the exclusion was ordered; after this 6-year period has elapsed, the data shall be erased [Section 1(5c) of the Act on the Protection of Personal Data].
The legal basis for data processing, as set out above, is the fulfilment of a legal obligation in accordance with Article 6(1)(c) of the GDPR. This data processing is mandatory.

6. **Handing over of promotional prizes:**
The Controller organises promotions from time to time on the Casino premises, during which gift tokens and gift tickets are handed over to Guests, which is recorded in the reception register.
Scope of data processed: fact of receipt of gift tokens, gift tickets, physical prizes (advertising gifts, promotional gifts), date and time, name.
Purpose of data processing: recording the receipt of promotional prizes, verifying the fulfilment of the promotion.
Legal basis for data processing: Legitimate interest of the Controller – [GDPR Article 6(1)(f)]. (The Controller's legitimate interest: a business and economic interest linked to the need to prove the handover of prizes, as well as the operation of sound accounting practices. Further information is contained in the data protection impact assessment prepared by the Controller.)
Duration of data processing: 8 years in accordance with the Accounting Act.

7. **Record of self-restrictions and self-exclusions:**
Purpose of data processing: to keep a record of self-restrictions/self-exclusions, to ensure player protection, and to provide data to the gambling supervisory authority.
Scope of personal data processed: name; place and date of birth; mother's name; address; number of identity document suitable for identification; duration, fact/subject, period, date of lifting. This data processing is mandatory; without it, the Guest cannot make a declaration.
Legal basis for data processing: compliance with a legal obligation – Article 6(1)(c) of the GDPR, Sections 16–17 of the Gaming Organisation Regulation, Section 29/I(2) of the Szjtv.
Duration of data processing: 6 years from the date the data is generated.

8. Player protection register:
Pursuant to Section 1 (6b) of the Gambling Act, the gambling supervisory authority maintains a register of persons who have made a significant self-restriction declaration and of persons placed under guardianship by a court that fully restricts their legal capacity or partially restricts their legal capacity in relation to legal declarations concerning gambling.
Pursuant to Section 1(6b) of the Gambling Act, the 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 data subjects in gambling.
Pursuant to Section 1(6d) of the Gambling Act, the player protection register contains:
a) separately, the personal identification data of persons who have made a significant self-restriction declaration and of persons referred to in paragraph (6) (surname and first name, surname and first name at birth, mother's name, place and date of birth, type and number of identity document, address),
b) the nature of the data processing (restriction based on a voluntary decision or a court order),
c) the date of termination (whether the data processing is for a fixed or indefinite period).
The Controller may access the player protection register solely for the purpose of fulfilling its verification obligations, using an electronic extract. The extract contains an unbreakable alphanumeric code generated from personal data. The SZTFH shall make the procedure for generating the alphanumeric code available to the Controller electronically. The Controller compares the alphanumeric code generated from the player's personal data with the alphanumeric code appearing in the extract. If the two codes match, the Controller shall refuse to register the player or shall not allow the registered player to play.
Purpose of data processing: access to the player protection register.
Legal basis for data processing: compliance with a legal obligation – Article 6(1)(c) of the GDPR, Section 20 of the Gaming Organisation Regulation. This data processing is mandatory; without it, the Guest cannot use the service.
Duration of data processing: the date of the check; the Controller shall retain the notification of refusal of entry provided to the player for 5 years.

9. **Suspicion of money laundering and terrorist financing:**
Scope of data processed: name, birth name, mother's name, place and date of birth, nationality, address, type, number and expiry date of the identity document. [Pursuant to Section 30(2)(a) of the Pmt., the Controller is obliged to include in the report the data specified in Sections 7–14 of the Pmt. (see: Point 1.A of this chapter of the Information Notice), as well as the circumstances forming the basis of the report.]
Purpose of data processing: to fulfil the notification obligation.
Legal basis for data processing: compliance with a legal obligation – Article 6(1)(c) of the GDPR, Section 30(1)(a)–(b) of the Personal Data Protection Act. This data processing is mandatory.
Duration of data processing: 8 years from the termination of the business relationship [pursuant to Section 56(2) of the Pmt.].

10. **Reporting of counterfeit or suspicious banknotes:**
Scope of data processed: name, birth name, mother's name, place and date of birth, nationality, address, type, number and expiry date of identity document. [Pursuant to Section 30(2)(a) of the Pmt., the Controller is obliged to include in the report the data specified in Sections 7–14 of the Pmt. (see: Section 1.A of this chapter of the Information Notice), as well as the circumstances forming the basis of the report.]
Legal basis for data processing: compliance with a legal obligation – Article 6(1)(c) of the GDPR, Section 30(1)(c) of the Pmt. This data processing is mandatory.
Duration of data processing: 8 years from the termination of the business relationship (pursuant to Section 56(2) of the Pmt.).

11. **Verification of financial and asset-freezing measures ordered by the EU/UN Security Council:**
Pursuant to Section 6 of Act LII of 2017, the service provider must have a filtering system capable of ensuring the implementation of EU legal acts and UN Security Council resolutions imposing financial and asset-freezing measures, and which IT system is capable of regularly comparing the personal data of the service provider's entire customer base with the data of persons designated by the restrictive measures.
Purpose of data processing: to identify persons subject to financial and asset-related restrictive measures.
Legal basis for data processing: compliance with a legal obligation [Article 6(1)(c) of the GDPR] – Act LII of 2017, and Act LIII of 2017 on the implementation of Act LII of 2017 on the prevention and combating of money laundering and terrorist financing for operators of casinos and card rooms, and organisers of betting not classified as remote gambling, remote gambling and online casino games, and on the detailed rules regarding the minimum requirements for the development and operation of a screening system pursuant to Act LII of 2017 on the implementation of financial and asset-related restrictive measures ordered by the European Union and the United Nations Security Council, as set out in Decree 4/2021. Duration of data processing: the service provider is obliged to retain data generated during the performance of screenings for a period of 8 years from the date of the screening. This data processing is mandatory.

12. **Video surveillance system:**
The Controller processes data for the purposes of protecting and identifying Guests, ensuring the integrity and safe conduct of gaming, maintaining order and protecting property, and to perform the tasks prescribed in the Pmt. (as the purpose of data processing), the Casino operates a closed-circuit security camera system ('closed circuit television', CCTV) capable of transmitting both video and audio.

Pursuant to Section 37(2) of the SZTFH Decree, the casino is required to ensure the integrity of gaming, its safe conduct, order and the protection of property, and to carry out the tasks

prescribed in Act LIII of 2017 on the prevention and combating of money laundering and terrorist financing, the casino must have a video system that meets the following conditions.

Pursuant to Section 7(9) of the Pmt., the Controller is entitled, for the purposes of preventing and combating money laundering and terrorist financing, ensuring the linkability of data obtained during customer due diligence measures and player transactions, and for the purpose of effectively carrying out supervisory activities, is entitled to record the image of a natural person customer and to make video recordings of their activities within the premises, as well as to store the image in its electronic record-keeping system.

The legal basis for data 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 prescribed by both Section 37(7) and Section 51(4) of the SZTFH Decree, as well as Section 7(9) of the Pmt. This data processing is mandatory.
The gambling supervisory authority may access the data recorded by the video system in order to perform its statutory duties.

Pursuant to Section 37(7) of the SZTFH Decree, the video system must meet the following conditions:

a) All games available in the Casino must be observable The cameras must be capable of ensuring that the stakes (colours and legibility of chips), the gaming equipment and auxiliary gaming equipment (dice, cards, balls, etc.), as well as the course of the game, must be clearly visible and followable on the screen.
b) It must be ensured that the loading and emptying of slot machines, the payment of jackpots, the separate room used for the accounting of gaming equipment, and the route leading to the accounting area can be observed and monitored. If the accounting of gaming machines takes place in a separate room, this room must also be equipped with a camera, and the route leading to the accounting area must also be observable.
c) Any disturbances within the Casino premises, as well as the observability and recordability of the security measures in place, must be clearly visible throughout the entire gaming area and at all gaming stations (gaming tables, slot machines, etc.).
d) The process of the Guest's entry and identification must be verifiable.
e) The cameras must be capable of displaying the date and time in the transmitted image with second-by-second detail and accuracy, as well as, depending on their positioning, the bets placed, and the receipt of cash and tips, in such a way that events occurring on the gaming machines remain visible at all times. Audio must also be transmitted alongside the video. Events that must be documented, as well as those taking place at the cashier's desk, must be recorded using a close-up view (zoom camera).
f) The images from the cameras are kept under constant surveillance by the Controller in accordance with the monitoring system set out in the Casino's gaming plan. The footage provided by the cameras must be recorded simultaneously and retained for the period specified in Section 51(4) of the SZTFH Decree.

Duration of data processing:

- in accordance with the SZTFH Decree, the Controller shall determine the period for the retention of video recordings and the submission of accounting documents in such a way that, following the submission of the accounting documents, video recordings serving to substantiate the content of any submitted document remain available to the gambling supervisory authority has at least five working days to view the video recordings supporting the content of any submitted document. The Controller is obliged to retain video recordings and other documents relating to extraordinary events occurring in the casino and measures taken against players for at least thirty days.
- Pursuant to Section 7(9) of the Pmt., the Controller is obliged to retain video recordings for 45 days from the date of recording; the Controller is obliged to extend this period, upon

notification by the supervisory authority, until the conclusion of the supervisory authority's proceedings.

In the case of CCTV surveillance, data subjects may include the Casino's guests, players and employees working on the Casino premises.
The Controller sets out the detailed data processing rules relating to the use of the video system in a separate information notice for its employees, the security service and the video surveillance staff, and ensures compliance with these rules.
The video system is operated by the Controller, and the Controller's staff (casino director, manager, department head, camera operator, camera operator's assistant, and persons designated by management) are authorised to access the recordings.
The Controller uses live monitor surveillance and also records the footage.
Storage location of recordings: the video servers are located in a dedicated, air-conditioned room designed for this purpose, the server room.
The cameras operate continuously every day, 24 hours a day.

13. **Credit card transactions**:
If a Guest purchases gaming credits (tickets or chips) at the Casino's cashier's desk using a credit card, the Controller verifies the cardholder's identity. The purpose of data processing is to comply with the requirements of the credit card acceptance partner, to verify the cardholder, and thereby to assist in the prevention or detection of credit card fraud. The Controller records the number and type of the identification document (identity card or passport) used for verification, the cardholder's name, and the first 4 digits of the card number.
The Controller retains the transaction receipt for 60 months.
Legal basis for data processing: the Controller's legitimate interest [Article 6(1)(f) of the GDPR]. (The Controller's legitimate interest: performance of the contract with the bank, reduction in the number of criminal offences. Further information is contained in the data protection impact assessment prepared by the Controller.)
The bank card acceptance partner involved in the transactions is entitled to view the transaction records.

14. **Sending newsletters containing general marketing offers:**
The purpose of data processing is – in accordance with the provisions of Section 6 of the Grt. – to contact data subjects who have given their prior and explicit consent via a newsletter containing marketing information about news, bonuses, promotions and current events relating to the Controller's offline casino gaming services.

Scope of data processed: surname and first name, date of birth, email address, telephone number (if the data subject also requests SMS notifications).

Given that, in the context of sending the newsletter, the Controller also advertises a service in which, pursuant to Section 1(5b) of the Szjtv., persons under the age of 18 may not participate, and which may conflict with the restriction set out in Section 8(1) of the Grt., therefore, in accordance with Section 6(2) of the Grt., it is also necessary to record the date of birth. Furthermore, in order to ensure player protection, the data subject must declare that they are not subject to any restrictions based on the data in the player protection register.

The newsletter is generally sent by email, but the data subject has the option to provide their telephone number so that they may also receive, on a supplementary basis via SMS – given the nature of the channel – shorter messages, primarily containing information from the Controller regarding current events.

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

The duration of data processing shall be until the withdrawal of consent; in the absence of such withdrawal, it shall continue until the end of the Controller's provision of the newsletter service for marketing purposes. Consent may be withdrawn at any time, free of charge and without restriction or justification, by emailing lvc_diamond@lvcd.hu , by post to the Controller's registered office, or by clicking the 'unsubscribe' link in the newsletter. Furthermore, the data subject may also opt out of the SMS communication channel at any time by using the link at the end of the SMS message. In order to ensure the accuracy of the personal data provided during the subscription process and to prevent erroneous subscriptions, the Controller sends a message containing a confirmation link to the e-mail address provided by the data subject. The subscription can be finalized by clicking the confirmation link.If the subscription is not finalized, the Controller will send a reminder within 24 hours. If the subscription is still not confirmed within 5 calendar days, the personal data provided during the subscription process will be deleted.

15. **Raffle**:
The Controller organises prize draws from time to time on the premises of the Casinos. The prize draw ticket contains the ticket number, as well as the name and card number of the ticket holder. Providing the name and card number, and having the name read out, are conditions for participation in the draw.
Scope of data processed: name, card number.
Purpose of data processing: to announce the winner's name during the raffle draw (thereby identifying the winner).
Legal basis for data processing: the Controller's legitimate interest [Article 6(1)(f) of the GDPR]. (The Controller's legitimate interest is a commercial and economic interest linked to the interest in maintaining the prize draw. Further information is contained in the data protection impact assessment prepared by the Controller.)
Duration of data processing: the winner's name will be announced verbally at the time of the draw.

16. **Taking photographs and video recordings**:
The Controller organises events, competitions and tournaments from time to time.
Photographs and video recordings may be taken of participants in the event or competition, as well as of those present at the venue. The Controller will display information regarding this at the event venue.
The purpose of data processing is to document events organised by the Controller through images, to promote the Controller's activities and to make them known to others.
The primary legal basis for data processing is the consent of the data subjects [Article 6(1)(a) of the GDPR] in the case of persons participating in the event as competitors or players. (Withdrawal of consent does not affect the lawfulness of data processing carried out on the basis of consent prior to withdrawal.)
Where it is not possible to obtain consent (excluding cases 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 event venue, but are not participating in the specific competition or cup, the secondary legal basis for data processing is the data controller's legitimate interest [Article 6(1)(f) of the GDPR]. (The Controller's legitimate interest: a business interest related to the presentation and promotion of the competitions. Further information is contained in the data protection impact assessment prepared by the Controller.)
Scope of personal data processed: name, image/video and audio recordings.
Duration of data processing: until the data subject withdraws their consent or the purpose is fulfilled.
Data subjects have the right to object to the recording at any time.

17. **Publication of photographs and video recordings**:
Purpose of data processing: the Controller may publish the recordings on its own social media platforms (Facebook, Instagram), YouTube and TikTok channels or website, or may transfer them to television or the press for publication. The Controller will inform data subjects in advance, on a case-by-case basis, of the exact methods and locations of publication at the venue. The purpose of publishing the recordings is to promote the Controller and its services and events, and to present and introduce them to others.
The primary legal basis for data processing is the consent of the data subjects [Article 6(1)(a) of the GDPR] in the case of persons participating in the event as competitors or players. (Withdrawal of consent does not affect the lawfulness of data processing carried out on the basis of consent prior to withdrawal.)
Where it is not possible to obtain consent (excluding cases 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 event venue but are not participating in the specific competition or cup, the secondary legal basis for data processing is the data controller's legitimate interest [Article 6(1)(f) of the GDPR]. (The Controller's legitimate interest: a business interest related to the presentation and promotion of the competitions. Further information is contained in the data protection impact assessment prepared by the Controller.)
Scope of personal data processed: name, image/video and audio recordings.
Duration of data processing: until the data subject withdraws their consent, until the purpose is fulfilled, or, in the case of publication on a social media site, until the site ceases to operate.
Data subjects have the right to object at any time to any use of the recording.

18. **Data processing related to the use of the website**

Cookies, web beacons:
The Website (www.lasvegascasino.hu) uses so-called cookies and web beacons during its operation. Detailed information can be found in the cookie policy located under the Processing menu item on the website.

Marketing:
Facebook advertisements: our company uses the services of Facebook [Meta Platforms Ireland Ltd. (4 Grand Canal Square, Grand Canal Harbour, Dublin 2, Ireland)] for the display of targeted advertisements on Facebook. In relation to these advertisements, Meta acts as the controller and is responsible for obtaining consent for data processing. Our company does not process any personal data in connection with these advertisements. Further information is available at the following link: 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, a service provided by Meta, into our website. This enables Facebook to track the activity of users registered on Facebook whilst they are on our website. We can create target audiences and receive analytical data on how visitors use our website. With the help of Facebook Pixel, we can optimise our advertisements and provide personalised offers to visitors to the website. The data is stored and processed by Facebook; our company does not handle personal data, and Facebook does not transfer personal data to our company.

Google Tag Manager: the website uses the Google Tag Manager function. Google Tag Manager is a solution that allows marketing professionals to manage tags placed on the website centrally via a single interface. The tool is a cookie-free domain and does not collect personal data; it merely ensures the activation of other tags, which may collect data on their own behalf under certain circumstances. Google Tag Manager does not have access to such data. If the function has been disabled at domain or cookie level, this applies to all tracking tags implemented via

Google Tag Manager. Further information on how Google Tag Manager works is available at the following link: https://support.google.com/tagmanager/#topic=3441530)

Traffic measurement:
Scope of data processed: the IP address of visitors to the Website (www.lasvegascasino.hu), the time of the visit, details of the pages viewed, and the name of the browser used.
Purpose of data processing: software that analyses website traffic data runs on the Controller's website.
Legal basis for data processing: the data subject's consent [Article 6(1)(a) of the GDPR]. (Withdrawal of consent does not affect the lawfulness of processing carried out on the basis of consent prior to withdrawal.)
Duration of data processing: until the purpose is fulfilled, but no later than upon deletion at the data subject's request.

19. **Processing of personal data in connection with the use of electronic mail (email):**
The Data Subject may contact the Controller via the email addresslvc_diamond@lvcd.hu on the Controller's website or send a message to the Controller via the interface available under the "Contact" menu item on the Website.
If the email contains other personal data, the person providing the data is obliged to obtain the Data Subject's prior consent, which the Controller presumes to have been given.
Scope of data processed: name, email address.
Purpose of data processing: to maintain contact with the Controller.
Legal basis for data processing: the data subject's consent [Article 6(1)(a) of the GDPR]. (Withdrawal of consent does not affect the lawfulness of data processing carried out on the basis of consent prior to withdrawal.)
Duration of data processing: until the purpose is fulfilled or until deletion upon the data subject's request.

20. **Processing of personal data in connection with the use of social media**
Scope of data processed: name, comment, follow, message, rating.
Purpose of data processing: to inform data subjects via the Controller's Facebook and Instagram pages about the Controller's operations, events and programmes, and to promote the Controller.
Legal basis for data processing: the data subject's consent [Article 6(1)(a) of the GDPR]. (Withdrawal of consent does not affect the lawfulness of data processing carried out on the basis of consent prior to withdrawal.)
Data subject: a person engaging in activity in connection with the website.
Duration of data processing: until deletion at the data subject's request, but no later than the duration of the page's operation.

The Controller's Facebook pages:
https://www.facebook.com/LVCEuroCenter
https://www.facebook.com/lasvegastropicana
https://www.facebook.com/lasvegascorvin
https://www.facebook.com/lasvegasatlantis
https://www.facebook.com/eurocenterpoker

The Controller's Instagram page:
https://www.instagram.com/lasvegascasinos_official/

To use the Facebook and Instagram pages, the Data Subject must have their own account on the social media platform. The operators of the social media platforms process data as independent data controllers in accordance with their own privacy policies. The datacontroller for 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 confirms that they have
and has read and accepted the terms and conditions and privacy policy set out therein
:
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 casino's social media page under the data subject's IP address.
With regard to the data the Data Subject wishes to post (name, photograph, comment, review), they may exercise their rights directly with Facebook or Instagram, or contact the Controller.
The Controller is entitled to request the deletion of any data that infringes upon the reputation or rights of the Controller or any other person.
Data processing for statistical purposes carried out during the use of Meta products is a joint data processing operation between the Controller and Meta Platforms Ireland Ltd. (4 Grand Canal Square, Grand Canal Harbour, D2 Dublin, Ireland). Detailed information on website analytics is available via the following link: https://www.facebook.com/legal/terms/page_controller_addendum

The Controller's YouTube channel: https://www.youtube.com/@lasvegascasinobudapest
With regard to the YouTube channel, YouTube LLC acts as the independent data controller, with its parent company being Google LLC (1600 Amphitheatre Parkway, Mountain View, CA 94043, United States). In accordance with its Privacy Policy and Terms of Service, which can be viewed at the following link: https://policies.google.com/privacy?hl=hu. For data protection matters, you can contact the Data Protection Officer via the following link: https://support.google.com/policies/contact/general_privacy_form.

The Controller's TikTok channel:
https://www.tiktok.com/@lvc_budapest?_t=ZN-8ub9syUDQiE&_r=1
To use TikTok, the Data Subject must have their own account. TikTok Technology Limited (The Sorting Office, Ropemaker Place, Dublin 2, Dublin, D02 HD23, Ireland; hereinafter: TikTok Ireland) acts as an independent data controller and collects data on individuals visiting individual TikTok accounts in accordance with its own privacy policy. TikTok Ireland acts as a joint controller with TikTok Information Technologies UK Limited (4 Lindsey Street, London, EC1A 9HP, United Kingdom) in relation to the processing of personal data carried out for the technical operation of the TikTok platform. TikTok Ireland's relevant general data processing notice is available at https://www.tiktok.com/legal/privacy-policy?lang=en#privacy-eea.
For data protection matters, you can contact the Data Protection Officer via the following link: https://www.tiktok.com/legal/report/privacy?lang=en

21. **Processing of personal data in connection with the use of the Wi-Fi network:**
The Controller provides free and open internet access on the premises of the Casinos, but accepts no liability for any risks arising from the use of wireless internet.
By connecting to the Wi-Fi network, the Data Subject expressly consents to the Controller recording the MAC address of the device used by the Data Subject, which serves to uniquely identify the device, for the duration of its use.
Scope of data processed: MAC address, device name.
Purpose of data processing: to use the service provided by the Controller.
Legal basis for data processing: the Data Subject's consent [Article 6(1)(a) of the GDPR]. (Withdrawal of consent does not affect the lawfulness of data processing carried out on the basis of consent prior to withdrawal.)
Duration of data processing: until the purpose is fulfilled, but no later than the deletion of the data at the Data Subject's request.

22. **Recording of calls received at the central telephone number:**
Purpose of data processing: to prevent unlawful acts and ensure lawful operation.
Scope of data processed: date and time of the call (day, hour, minute); caller's number, extension dialled; voices of those participating in the conversation; all data/information constituting personal data uttered during the conversation.
Legal basis: the Controller's legitimate interest [Article 6(1)(f) of the GDPR]. The Controller has carried out a balancing test in a separate document.
Duration of data processing: 7 calendar days following the recording. If the data subject objects to the processing of their personal data and there is no overriding legitimate ground, the Controller shall erase the personal data.
If an authority – including, but not limited to, the Hungarian Police – sends a request to the Controller, the Controller shall comply with the request in accordance with its legal obligations. In certain cases, the Controller may initiate proceedings with the authorities.

23. **Event pre-registration**
Purpose of data processing: Guests have the option to pre-register for certain events organised by the Controller via the Website, thereby indicating their intention to attend. The purpose of our data collection is to enable the Controller to identify pre-registered individuals in order to ensure the necessary capacity.
Scope of data processed: the name and email address of the pre-registering Guest, 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) of the GDPR]. (Consent may be withdrawn at any time; however, this does not affect the lawfulness of data processing carried out on the basis of consent prior to withdrawal.)
Data will be processed until consent is withdrawn or, in the absence of such withdrawal, until the end of the selected event.

24. Data processing relating to consumer complaints
Purpose of data processing: To investigate and respond to complaints submitted by guests.
Scope of data processed: In accordance with Section 17/A(5) of the Consumer Protection Act, the Guest's full name, address or email address, the place, time and method of submitting the complaint, c) a detailed description of the consumer's complaint, a list of the documents and other evidence presented by the consumer, the business's statement regarding its position on the consumer's complaint, provided that the complaint can be investigated immediately, the signature of the person recording the report and – except in the case of a verbal complaint made by telephone or using another electronic communications service – the consumer's signature, the place and time of the report's recording, and, in the case of a verbal complaint made by telephone or using another electronic communications service, the complaint's unique identification number.
Legal basis: compliance with a legal obligation [Article 6(1)(c) of the GDPR] – Compliance with the legal obligations set out in Section 17/A of the Consumer Protection Act and Section 35 of the Services Act.
Duration of data processing: the Controller shall retain the record of the complaint, or in the case of a complaint submitted in writing, the submitted document and the response to the complaint, for five years pursuant to Section 17/A(7) of the Consumer Protection Act.

25. Abuse reporting system
Purpose of data processing: To investigate reports received through the internal whistleblowing system established in accordance with Act XXV of 2023 on complaints, reports in the public interest and rules relating to the reporting of misconduct (hereinafter: **the Complaints Act**), answering queries and remedying the conduct that is the subject of the report.
Scope of data processed: in the case of a whistleblower who discloses their identity, the data provided by them. The data provided in the report concerning the person whose conduct or omission gave rise to the report. The data of the person necessary for the investigation who may

have relevant information regarding the contents of the report (e.g. a person named as a witness). Other personal data provided in the report and personal data collected during the investigation and the clarification of the facts. Only personal data strictly necessary for the investigation of the report may be processed.
Legal basis: The legal basis for data processing is the fulfilment of a legal obligation pursuant to Article 6(1)(c) of the GDPR. If the report also contains special categories of data, the additional legal basis is Article 9(2)(b) of the GDPR. The legal obligation is laid down in Section 18 of the Complaints Act.
Duration of data processing: 5 years following the conclusion of the investigation conducted on the basis of the report. If, as a result of or in connection with the investigation, court or administrative proceedings are initiated, until their final conclusion.

V. Is the disclosure of my personal data permitted?

Data transfer to authorities:

a. Pursuant to Section 36 of the Gambling Act, the gambling supervisory authority is entitled at any time to request and inspect statements, data, documents and investigation materials relating to activities falling within the scope of the Gambling Act, and to conduct on-site inspections.

b. Pursuant to Sections 261–265 of Act XC of 2017 on Criminal Procedure (Be.), in criminal proceedings, the court, the public prosecutor's office, the investigating authority, or the body conducting the preparatory proceedings may request the provision of data from any legal person (data controller). Within the framework of a data request, the transfer of data, the transfer of electronic data or documents, or the provision of information may be requested. In the case of a request for the provision of data to be fulfilled electronically, a deadline of at least 1 and no more than 30 days may be set; in the case of a request to be fulfilled by other means, a deadline of at least 8 and no more than 30 days may be set. Unless otherwise provided by law, the organisation to which the request for information is addressed is obliged to comply with the request within the set deadline or, upon becoming aware of any obstacle to compliance, to notify the requesting authority without delay.

c. The National Tax and Customs Administration acts in cases where suspicion of money laundering arises. If another authority – including the National Tax and Customs Administration – sends a request to the Controller, the latter shall provide the requested information in accordance with its legal obligations.

d. In certain cases, the Controller may initiate proceedings with the authorities. In accordance with the provisions of its anti-money laundering policy, the Controller shall, in all cases where there are circumstances indicating money laundering, notify the competent authorities, in particular the National Tax and Customs Administration's Office for Combating Money Laundering and Terrorist Financing or the gambling supervisory authority.

Data transfer to data processors engaged by the Controller:

a. 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 and provides back-office IT services in relation to the following tasks:
    1. during player registration;
    2. in the case of high-profile public figures;

3. during admission;
4. during ticket, token and currency exchange;
5. in connection with the player protection register (data relating to players subject to self-exclusion or listed in the player protection register).

b. The web server and web hosting for the LAS VEGAS CASINO website are provided by Rendszerinformatika Zrt. (1139 Budapest, Váci út 81; company registration number: 01-10-046912; tax number: 23095942-2-41) as a data processor.

VI. What are my rights in relation to data processing?

Below is a summary of the Guest's rights that may be exercised vis-à-vis the Controller.

1. **Communication with the Controller, right of access:** communication between the Guest and the Controller takes place in person at the Casino, either verbally or in writing (as a private document of full probative value), or – where the email can be identified – by email. The Guest is entitled to request feedback from the Controller at any time as to whether the processing of their personal data is in progress; and if such processing is in progress, the Data Subject has the right of access to their processed personal data to the extent set out below.
   The Guest is entitled to request information from the Controller regarding data processing, covering the following details, which the Controller is obliged to provide without undue delay, but no later than one month from the date of the request for information. The information provided by the Controller regarding data processing within the scope of access may include, in particular, the following:
   a) the purposes of the data processing;
   b) the personal data being processed;
   c) the recipients of the data transfer;
   d) the expected duration of the data processing, or, if this cannot be determined, the criteria for determining the duration;
   e) a description of the rights to which the Guest is entitled under the Infotv. and the GDPR, and how to exercise those rights;
   f) the right to lodge a complaint with the **Supervisory** Authority;
   g) the source and legal basis of the information collected by the Controller;
   h) in the event of the transfer of personal data, the recipients of the data transfer – including recipients in third countries and international organisations;
   i) the fact that automated decision-making or profiling is used, where applicable.

   The Controller shall provide a copy of the personal data subject to processing at the Guest's request. The Controller may charge a reasonable administrative fee for any further copies requested by the Guest.

   a) The Controller shall examine and reply to the Guest's email regarding data processing if it is sent from the email address previously provided by the Guest (unless the Guest refers to a change of email address in the message, or the Guest's identity can be clearly identified from it).

   b) The Controller shall inform the Guest of any action taken concerning personal data without delay, but no later than one month after the action has been taken.

   c) If the Controller does not take any action in response to the Guest's request, it shall inform the Guest without delay, but no later than one month from receipt of the request, of the reasons for failing to take action, and that the data subject may lodge a complaint with the **Supervisory** Authority and exercise their right to judicial remedy.

d) The banned Guest may inspect the records relating to the ban in respect of the details of the ban affecting the Guest. At the same time as inspecting the records, the Guest may request a certificate of the recorded data, which the Casino shall provide free of charge at the time of inspection, but no later than the following working day (Section 1(5c) of the Act).

2. **Right to rectification:** During the term of the business relationship, the Guest is entitled and, pursuant to Section 12(3) of the Pmt., obliged to notify the 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 process (i.e. the issue of an entry card). If the Guest fails to report a change in their personal data without delay, the Guest shall bear the consequences thereof. If the personal data provided does not correspond to reality and the Controller has access to personal data that does correspond to reality, the Controller shall automatically rectify the personal data.

3. **Request for erasure:** the Guest is entitled to request that the Controller erase personal data relating to them without undue delay, and the Controller is obliged to erase personal data relating to the Guest without undue delay, in particular where any of the following grounds apply:
   a) the personal data are no longer necessary for the purposes for which they were collected or otherwise processed;
   b) the Guest withdraws their consent to the processing of data, and there is no other legal basis for the processing;
   c) the Data Subject objects to the processing based on legitimate interests;
   d) the Controller has processed the personal data unlawfully;
   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 were collected in connection with the offering of information society services referred to in Article 8(1) of the GDPR.

   Even where the above circumstances apply, the Controller is not obliged to erase the personal data processed if the processing is necessary:
   a) for the purposes of exercising the right to freedom of expression and information;
   b) to comply with a legal obligation under Union or Member State law to which the Controller is subject, or for reasons of public interest;
   c) for statistical purposes or for archiving purposes, or for scientific or historical research purposes, insofar as erasure is likely to render such processing impossible or seriously impair it;
   d) on grounds of public interest in the area of public health, in accordance with 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 is entitled to request that the Controller restrict the processing of data if one of the following conditions is met.
   a) The Guest disputes the accuracy of their personal data; in this case, the restriction applies for the period necessary to allow the Controller to verify the accuracy of the personal data.
   b) The processing is unlawful, and the Guest objects to the erasure of the personal data and requests the restriction of their use instead.
   c) The Controller no longer needs the personal data to fulfil the purpose of data processing, but the Guest requires it to establish, exercise or defend legal claims.
   d) The Guest has objected to the processing; in this case, the restriction applies for the period until it is determined whether the Controller's legitimate grounds take precedence over the Guest's legitimate grounds.

Where data processing is restricted as described above, such personal data may, with the exception of storage, only be processed with the Guest's consent or for the purpose of establishing, exercising or defending legal claims, or for the protection of the rights of another natural or legal person, or for reasons of substantial public interest. If the restriction on data processing is lifted, the Controller shall notify the Guest who requested the restriction of this fact in advance.

5. **Objection to data processing:** The Data Subject has the right to object at any time, on grounds relating to their particular situation, to the processing of their personal data based on legitimate interests as set out in this Notice. In this case, the Controller may no longer process the personal data, unless the Controller demonstrates that the processing is justified by compelling legitimate grounds which override the interests, rights and freedoms of the Data Subject, or which 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 Guest's consent or for the performance of a contract, the Guest is entitled to receive the personal data concerning him or her, which he or she has provided to the Controller, in a structured, commonly used and machine-readable format, and is also entitled to transmit such data to another data controller without hindrance from the Controller to whom the personal data were provided. This right may only be exercised in respect of personal data processed on the legal basis of consent or the performance of a contract.

7. **Initiation of proceedings by the Supervisory Authority:** the Guest may initiate an investigation by lodging a complaint with the **Supervisory** Authority, claiming that an infringement of their rights has occurred or that there is an imminent risk thereof in connection with the processing of their personal data. The **Supervisory** Authority's investigation is free of charge; the **Supervisory** Authority advances and bears the costs of the investigation. No one may suffer any disadvantage as a result of a complaint lodged with the **Supervisory** Authority. The **Supervisory** Authority may only disclose the identity of the complainant if the investigation cannot be conducted without doing so. If the complainant so requests, the **Supervisory** Authority may not disclose their identity even if the investigation cannot be conducted without doing so . Contact details of the **Supervisory** Authority: 1055 Budapest, Falk Miska u. 9–11.; email: ugyfelszolgalat@naih.hu; website: http://naih.hu; telephone: +36 (1) 391-1400.

8. **Enforcement of rights before the courts:** in the event of a breach of their rights, the Guest may bring a claim against the Controller before the courts; the adjudication of the claim falls within the jurisdiction of the regional court. As a general rule, the court with jurisdiction over the case is the court where the Controller has its registered office, but – at the Guest's discretion – proceedings may also be brought before the court where the Guest resides or is staying. The jurisdiction of the court can be checked using the "Court Finder" application available on the www.birosag.hu website. The court shall hear the case as a matter of priority.

9. **Compensation and damages:** if the Controller, through the unlawful processing of the Guest's personal data or a breach of data security requirements:
    a. causes damage to the Guest or to another person, it shall be obliged to compensate for such damage (compensation);
    b. infringes the Guest's right to privacy, the Guest may claim compensation for non-pecuniary damage from the Controller.

   The Controller shall be exempt from liability for the damage caused and from the obligation to pay compensation for non-pecuniary damage if it proves that the damage or the infringement of the Guest's right to privacy was caused by an unavoidable cause outside the scope of data processing. No compensation for damages shall be payable, and no compensation for non-pecuniary damage may be claimed, to the extent that the damage or the infringement of the

right to privacy resulted from the Guest's (the injured party's) intentional or grossly negligent conduct (Section 24 of the Information Act).

VII. Final provisions

1. Pursuant to Section 29/T of the Szjtv., in the case of gaming casinos and online casinos operated by the Controller, the Controller is entitled to use a standardised access and identification system.

2. This Policy is governed by Hungarian law. In the event of any dispute arising in connection with this Policy, the Hungarian text of this Policy shall prevail.

3. In matters not covered by this Policy, the Casino's Terms and Conditions of Participation and the relevant provisions of Hungarian law shall apply.

4. The full text of the Notice, as currently in force, is available at all times, free of charge, at the Casino and on the Website.

5. The Controller reserves the right to unilaterally amend the Notice at any time in compliance with the relevant legislation, and shall notify the data subject of such amendments by publishing the amended Notice on the website www.lasvegascasino.hu.

Date of entry into force of this Notice: 1 April 2026.