

## DATA PROCESSING INFORMATION

### GENERAL INFORMATION

Welcome to the Vegas.hu online casino!

In order to use the services available in the Vegas.hu online casino, you must register to the IT system of **LVC Diamond Játékkaszinó Üzemeltető Korlátolt Felelősségű Társaság as data controller (hereinafter: Controller)**. Your data provided during registration and the term of the client relationship are processed by the Controller for separately defined purposes or purposes specified by law.

It is the purpose of this this Data Processing Information Document (hereinafter: **Information document**) to specify - in accordance with the applicable legislative provisions - the data management principles, objectives and relevant other facts which define the purpose, term and manner of managing the personal data your provided, and also your rights to remedies.

The security and appropriate handling of the personal data you provide is of key importance to use, and therefore we kindly request you the carefully and thoroughly read through the provisions of this Information document. Should you have any questions or comments regarding the contents specified herein, please contact our Customer Service or the data protection officer.

### **Contact of the Controller and the data protection officer:**

Controller: LVC Diamond Játékkaszinó Üzemeltető Korlátolt Felelősségű Társaság  
Contact: registered office and mailing address: 1088 Budapest, Rákóczi út 1-3. III. em.  
E-mail: [info@vegas.hu](mailto:info@vegas.hu)  
Web: [www.vegas.hu](http://www.vegas.hu)

Data protection officer: Lajer Ügyvédi Társulás (Lajer Attorneys Partnership)  
Registered office and mailing address: 1024 Budapest, Lövház utca 30.  
E-mail: [DPO.LVC@lajer.net](mailto:DPO.LVC@lajer.net)

### DEFINITION OF THE TERMS USED IN THIS INFORMATION DOCUMENT

We have summarised the most important terms used in the Information document below.

1. **Personal data:** any piece of information relating to an identified or identifiable Player. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, a 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 of the Player indicated separately herein for each purpose of data processing.
2. **Processing:** any operation or the totality of operations performed on the data, irrespective of the procedure applied; in particular, collecting, recording, registering, classifying, storing, modifying, using, querying, transferring, disclosing, synchronising or connecting, blocking, deleting and destructing the data, as well as preventing their further use.
3. **Controller:** The natural or legal person, public authority, agency or other body which (who), alone or jointly with others, determines the purposes and means of the processing of personal data shall be considered the Controller.

The data provided by the Player are processed by **LVC Diamond Játékkaszinó Üzemeltető Korlátolt Felelősségű Társaság** [concise name: **LVC Diamond Kft.**; registered office and mailing address: 1088 Budapest, Rákóczi út 1-3. III. em.; registration number: 01-09-194087 [registered by the Company Registry Court of the Budapest-Capital Regional Court]; mailing address: 1088 Budapest, Rákóczi út 1-3. III. em.; VAT number: 25002889-4-44; e-mail: info@vegas.hu], i.e. only LVC Diamond Kft. makes and executes decisions concerning the personal data of the Player. The Controller also functions as the:

- a) game organiser – according to the definitions used in the Gambling Act and the Money Laundering Act – of the Casino (<https://vegas.hu/>; hereinafter: online casino website) (Gambling Act Section 29/L; Money Laundering Act Section 3 item 45 point b)); as well as the
  - b) “Organiser” according to the terms used in the End-User Licence Agreement (EULA).
4. **Processing performed by a Processor:** any activity related to data controlling activities performed on personal data, implemented on behalf of the Controller, regardless of the method and means applied for executing the actions, as well as the location of application, provided that the activity is performed on the data. Accordingly, processor means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the Controller.
  5. **Processor:** a natural or legal person, public authority, agency or other body which processes personal data on behalf of the Controller.
  6. **Data Subject:** any natural person identified or identifiable based on any information (hereinafter: Player).
  7. **Profiling:** any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.
  8. **Filing System:** any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.
  9. **Recipient:** a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether it is a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with European Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing.
  10. **Third Party:** a natural or legal person, public authority, agency or body other than the data subject, Controller, processor and persons who, under the direct authority of the Controller or processor, are authorised to process personal data.
  11. **Consent of the data subject:** any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him.

12. **Personal data breach:** a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.
13. **Cross-border processing of personal data:**
- a) processing of personal data in the European Union, which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union where the controller or processor is established in more than one Member State; or
  - b) processing of personal data in the European Union, which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State.
14. **Supervisory Authority** (in privacy issues): an independent public authority which is established by a Member State pursuant to Article 51 of the GDPR.
- Hungarian National Authority for Data Protection and Freedom of Information, Nemzeti Adatvédelmi és Információszabadság Hatóság (address: 1055 Budapest, Falk Miksa utca 9-11.; mailing address: 1363 Budapest, Pf. 9.; e-mail: [ugyfelszolgalat@naih.hu](mailto:ugyfelszolgalat@naih.hu); website: <http://naih.hu>; phone: +36 (1) 391-1400) (hereinafter: Authority).
- Supervisory authority concerned:** a supervisory authority which is concerned by the processing of personal data because:
- a) the controller or processor is established on the territory of the Member State of that supervisory authority;
  - b) data subjects residing in the Member State of that supervisory authority are substantially affected or likely to be substantially affected by the processing; or
  - c) a complaint has been lodged with that supervisory authority.
15. **Data transfer:** ensuring access to the data for a third party.
16. **Chat service:** service available for use within the customer service of the online casino, primarily for the purposes of general information exchange between the Controller and the Player. However, if the Player's identity is clearly established, it is suitable for using identical services with those offered by the phone customer service.
17. **Chatbot:** The Player can use the Chatbot within the Chat service in order to get information. The Chatbot is primarily suitable to answer general questions, without identifying the Player. Upon the request of the Player, the Chatbot can redirect to a customer service administrator, and in this case, the e-mail address of the Player will be requested from the Player for identification purposes.
18. **Cookie:** file (data series) that may be created on the computer of the visitor of the online casino website by the online casino website display program, and which stores information about the User, and the connection of the User and its web server.
19. **E-Commerce Act:** Act CVIII of 2001 on certain aspects of electronic commerce services and information society services.

20. **User:** the natural or legal person or other entity which uses or demands the electronic communications activities, including the electronic communications services.
21. **Consumer Protection Act:** Act CLV of 1997 on consumer protection.
22. **Consumer Protection Authority:** Budapest Capital Government Office, Consumer Protection Department (address: 1051 Budapest, Sas u. 19. III. em.; e-mail: [fogyved\\_kmf\\_budapest@bfkh.gov.hu](mailto:fogyved_kmf_budapest@bfkh.gov.hu)), contact data of the consumer protection authorities are available through the link on the following website: [https://fogyasztovedelem.kormany.hu/#/fogyasztovedelmi\\_hatosag](https://fogyasztovedelem.kormany.hu/#/fogyasztovedelmi_hatosag).
23. **Gambling Authority:** Supervisory Authority of Regulatory Affairs (1123 Budapest, Alkotás utca 50.)
24. **Business Advertising Act:** Act XLVIII of 2008 on essential conditions of and certain limitations to business advertising activity.
25. **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).
26. **Player:** any natural person who is at least 18 years old, and
- a) who is considered a player according to the definition used in the Gambling Act (Gambling Act Section 37 item 6); or
  - b) whose customer due diligence or customer identification process pursuant to the Money Laundering Act has begun; or
  - c) whose registration pursuant to section 3 item 45 point b) of the Money Laundering Act has begun; or
  - d) regarding whom the business relationship pursuant to the Money Laundering Act and/or this Information document exists; or
  - e) regarding whom the player identification or personal identification process pursuant to the Game Organisation Decree has begun; or
  - f) who is in a client relationship with the Controller, pursuant to the definition of the Freedom of Information Act; or
  - g) regarding whom the registration process pursuant to this Information document or the EULA has begun (i.e. including preliminary registration as well); or
  - h) who is considered “Client”, “Player”, “real cash Player”, “identified Player” or “banned” player pursuant to the EULA; or
  - i) who uses the services of the Online Casino (the online casino website) in accordance with the EULA, as well as the applicable legislation.
27. **Online Casino:** the online casino operated by the Controller, based on the Gambling Act and the applicable legislation, accessible on the online casino website (the Vegas.hu website). According to the terms used in the EULA, each software is considered part of the online casino website.
28. **Game Organisation Decree:** Decree 5/2021 (XI. 21.) SZTFH on the detailed rules of responsible game organisation (and any amendments in effect thereof).

29. **SZTFH Decree:** Decree 20/2021 (X. 29.) SZTFH on the implementation of tasks concerning the authorisation, organisation and control of certain gambling activities (and any amendments in effect thereof).
30. **Money Laundering Act:** Act LIII of 2017 on the prevention and combating of money laundering and terrorist financing.
31. **Registration:** data recording and high-level client due diligence procedure (according to the terms used in the Money Laundering Act) commencing with the filling in of the “registration form” (and provision of the username) according to the terms used in the EULA.
- a) Simultaneously, the finalised registration of the Player also constitutes establishing business relationship between the Controller - as the organiser of the Casino (LVC Diamond Kft.) - and the Player (Money Laundering Act Section 3 item 45 point b); Section 6 (1) point a)).
  - b) Registration is completed after finalising the high-level client due diligence procedure and the registration of records pursuant to the provisions of the EULA.
32. **End-User Licence Agreement (EULA):** the EULA of the Online Casino (and any amendments in effect thereof). The unabridged text of the EULA in effect is constantly and freely available on the online casino website.
33. **Computer:** any piece of electronic communications terminal equipment - pursuant to Section 188 item 21 of Act C of 2003 on electronic communications - available to the Player, such as computer equipment, mobile phone, computer, tablet that is suitable to receive so-called cookies (data packages).
34. **Gambling Act:** Act XXXIV of 1991 on gambling organisation (and any amendments in effect thereof).
35. **Service:** any service available for the Player’s use on the online casino website, including (but not limited to) any “Demo Game”, “Game”, “Service” pursuant to the terms used in the EULA, as well as any service available in the offline casinos of the Controller.

## **PRINCIPLES OF CONTROLLING DATA**

You can find a summary of the principles of data controlling below, completely enforced by the Controller during the entire term of data controlling, and considered obligatory on behalf of the Controller.

36. **Lawfulness, fairness and transparency:** Data processing can be based on:
- a) compulsory legislation requirement (including especially provisions of the Gambling Act and the Money Laundering Act), or
  - b) considering the type of business relationship, legislative provisions enabling optional data controlling (including especially Section 13/A (1)-(2) of the E-Commerce Act), as well as
  - c) (regarding data controlled in a non-compulsory manner, without applicable legislative requirements) the preliminary, voluntary consent of the Player, provided with knowledge of the EULA and this Information document, expressed through commencing registration and the use of the specific Service (including especially the registration obligation based on voluntary consent and obligatory for the Controller, stipulated in the SZTFH Decree and the Game Organisation Decree); the performance of the contract between the Parties with accepting the EULA and using the Service, as well as the steps requested by the Player, required for concluding this contract;
  - d) legitimate interest of the Controller (GDPR Article 6 (1) point f)).



- i. Upon commencing registration, the Player acknowledges that compulsory data supply and data supply based on legislative provisions enabling optional data controlling are preconditions to finalising the registration, i.e. using the Service.
  - ii. In the course of providing the Service, the Controller collects the processed personal data from the Player. Processing of the personal data of the Player can only be performed for lawful and fair purposes, in a manner that provides transparency for the Player. The Controller makes available the Information document in effect on the online casino website free of charges and obligations, continuously and publicly. The Controller shall not process the provided personal data for unfair purposes or any additional purposes not specified herein; in the course of its data processing (controlling) activities it constantly acts according to this policy and the applicable legislation.
  - iii. In case the legal basis for data processing is consent of the data subject, the existence of the right to withdraw consent at any time shall not affect the lawfulness of processing based on consent before its withdrawal.
  - iv. In case the legal basis for data processing is legitimate interest of the Controller, before commencing processing the Controller shall carry out an assessment of interests.
37. **Purpose limitation:** personal data may be processed by the Controller only for purposes specified in the Information document and the relevant legislation, including the Money Laundering Act, the Gambling Act, the SZTFH Decree and the Game Organisation Decree.
- a) The purpose of data processing on behalf of the Online Casino shall - from time to time - be the continuous provision of compliance with regulations, as well as the satisfactory compliance with the requests of the relevant authorities based on their authority set forth in law.
  - b) The purpose of data processing in other cases shall be ensuring the use of the Service, improving user experience, providing contractual service and the payment of prizes.
  - c) In order to ensure the transparency of the specific purposes of data processing, the Controller herein provides information regarding the purposes, duration and legal basis for processing different personal data. These requirements shall be applied by the Controller as binding.
38. **Storage limitation:** personal data of the Player shall be stored in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. The Controller shall take the processing periods prescribed by law as basis and shall in any case retain the data for the required mandatory period, and for certain processing operations may specify a longer processing period. Personal data processed exclusively according to Article 6 (1) item a) of the GDPR, based on the explicit and voluntary consent of the Player shall be processed by the Controller until the Player requests erasure or revokes consent. Personal data processed according to the Money Laundering Act, unless otherwise regulated by law or this Information document, shall be preserved by the Controller for 8 years after the termination of the business relationship with the Player, in each case (pursuant to Section 56-57 of the Money Laundering Act). The Controller shall process the data controlled in the course of the ban records specified in Section 1 (5c) of the Gambling Act and also herein, for 6 years after the ban is ordered.
- a) Regarding the Controller and the Player, the finalisation of the Player's registration at the Controller, as the organiser of the Online Casino (LVC Diamond Kft.) shall constitute establishing business relationship (Money Laundering Act Section 3 item 35 point b); Section 6 (1) point a)).
  - b) The business relationship of the Controller and the Player is terminated when the Player initiates the termination of his contract established through registration for participating in online casino games, and as the result thereof, the Player's account is terminated. In case

the Player intends to re-register, he can do so pursuant to the provisions of the EULA of the Controller, with the renewed recording of his personal data.

- c) Pursuant to the provisions of Section 56-57 of the Money Laundering Act, upon the request of the Gambling Authority, the authority operating as the financial information unit, the investigating authority, the office of the state attorney and the court, the Controller shall preserve data for the term specified in the request, but no more than 10 years (Money Laundering Act Section 58 (1)).

The 8-year data preservation period specified in the Money Laundering Act may be extended based on the request of an authority, in case the data, document specified therein is necessary for conducting ongoing or future authority proceedings. Following the final decision or the failure of initiating the planned proceedings the Controller shall remove the personal data from its records (Money Laundering Act Section 58 (2)-(3)).

- d) Unless otherwise regulated by law or this Information document, the Controller shall preserve all personal data based on the Gambling Act, the SZTFH Decree or the Game Organisation Decree for 6 years after processing the data (Gambling Act Section 1 (7a)). If the Controller specifies a different period, then it shall be indicated in this Information document and the obligation for a minimum term of 6 years shall also be taken into account.

39. **Data minimisation:** the personal data processed by the Controller shall be adequate, relevant to the purposes for which they are processed; the Controller shall only process personal data that are absolutely necessary. It is the objective of the Controller to only request consent of the Player for processing personal data that are absolutely necessary for providing the Services at the highest possible level (GDPR Article 6 (1) item a)). At all times, these are personal data that are actually required for the use of the Service. The recording and processing of any additionally processed personal data is required by law or performance of the contract.

40. **Accuracy:** in order to provide Services at the highest possible level, and also to comply with legislative obligations, it is the objective of the Controller to ensure that the recorded personal data are continuously kept updated (Money Laundering Act Section 12 (1)), and the Controller takes all reasonable efforts to ensure that at all times. The Player shall also support the accuracy of the data, and thus during the existence of the business relationship he shall inform the Controller within five business days after receiving information about any changes to the data provided during the customer due diligence according to the Money Laundering Act.

41. **Principle of data protection (integrity and confidentiality);** the Controller lays special emphasis on protecting the personal data provided and the private sphere of the Player. The Controller shall ensure the security of personal data at all times, and make arrangements for and carry out data processing operations in a way so as to ensure full respect for the right to privacy of data subjects in due compliance with regulations on data protection and confidentiality. In order to ensure the high level protection of data, the Controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures for ensuring the protection of the rights of the Players (GDPR Article 28 (1)). Personal data shall be protected by the Controller through suitable measures against unauthorized access, alteration, transmission, public disclosure, deletion or destruction, as well as damage and accidental loss, and to ensure that stored data cannot be corrupted and rendered inaccessible due to any changes in or modification of the applied technique (including password protection, encryption methods, restoration from backup, in case of data loss).

## **PURPOSES OF PROCESSING**

The ranges of cases (purposes of data processing) applied in practice to process the personal data of the Player are summarised below.

## 42. Processing type: Preliminary registration

- a) Purpose of processing: the prospective Player can opt for preliminary registration preceding the finalisation of his registration. Upon the preliminary registration, in the course of the registration process required for the use of the service, the Controller creates a technical user account for the person performing the registration. Until the registration is finalised, the registrant has restricted access: he can log in to the user account, browse the contents of the website and access free demo games, but cannot participate in real cash games. During preliminary registration, the Controller does not carry out client due diligence fully, this will happen during registration.
- b) Range of processed personal data: e-mail address, password, selected username, date of birth, statement on politically exposed status, statement of the registrant about being at least 18 years old, playing in his own name and providing the data for registration on his own behalf.
- c) The legal basis for processing is the performance of the contract concluded by accepting the EULA in the preliminary registration process, by the Player and the Controller [GDPR Article 6 (1) point b)].
- d) Processing period: if the registrant finalises the registration, processing of the data is performed according to the rules applicable to registration; if no finalised registration takes place, the Controller will process data for 8 years following the last login.

## 43. Processing type: Registration

- a) Purpose of data processing: the Controller registers the Player in order to carry out client due diligence measures specified in the act on the prevention and combating of money laundering and terrorist financing, and to provide player protection.
- b) Range of processed personal data and legal basis for data processing: we provide a summary of the personal data required to be provided during registration below, and also present legislation applicable to processing:

	Name of personal data	Legal basis for data processing: compliance with legal obligation [GDPR Article 6 (1) point c)]
1.	surname and forename	Money Laundering Act Section 7 (2) point aa); Gambling Act Section 29/H (1) point a)
2.	birth surname and forename	Money Laundering Act Section 7 (3) point ab); Gambling Act Section 29/H (1) point a)
3.	place and date of birth	Money Laundering Act Section 7 (2) point ad); Section 17 (1); Gambling Act Section 29/H (1) point e)
4.	mother's name	Money Laundering Act Section 7 (2) point ae); Section 17 (1); Gambling Act Section 29/H (1) point a)



5.	address (or place of abode, if the address is not in Hungary)	Money Laundering Act Section 7 (2) point af); Gambling Act Section 29/H (1) point b)
6.	nationality	Money Laundering Act Section 7 (2) point ac); Gambling Act Section 29/H (1) point c)
7.	type and number of the personal identification document	Money Laundering Act Section 7 (2) point ag); Gambling Act Section 29/H (1) point d)
8.	photo of the Player in case of data query from a public register	Money Laundering Act Section 7 (1)
9.	in case of Hungarian nationals: <ul style="list-style-type: none"> <li>- personal identification document + official certificate of the permanent address, only the side without personal identification (address card) (the latter only if the home address is located in Hungary).</li> <li>- driver's licence card + address card (the latter only if the home address is located in Hungary) or</li> <li>- passport + official certificate of the permanent address, only the side without personal identification (address card) (the latter only if the home address is located in Hungary);</li> <li>- for Hungarian nationals providing a foreign address, we request a document certifying the foreign address to be uploaded as well.</li> </ul>	Money Laundering Act Section 7 (3) point aa)
10.	in case of foreign nationals: <ul style="list-style-type: none"> <li>- official certificate of having a home address in Hungary (only the side without personal identification if an address card is presented), if the home address is located in Hungary</li> </ul>	Money Laundering Act Section 7 (3) point ab); Gambling Act Section 29/H (1) point b)
11.	in case of foreign nationals: <ul style="list-style-type: none"> <li>- passport or personal identification document, provided that it embodies an authorisation to reside in Hungary, document evidencing the right of residence or a valid residence permit</li> </ul>	Money Laundering Act Section 7 (3) point ab)
12.	copy of the document including the data specified in Section 7 (2)-(3) of the Money Laundering Act and the document specified in Section 7 (4) of the Money Laundering Act	Money Laundering Act 17. §
13.	digital copy of the personal identification document	Money Laundering Act Section 7 (8) and (8a)
14.	expiry of the personal identification document	Money Laundering Act Section 7 (5)
15.	in case of business relationship, the type, subject and duration of the agreement (EULA)	Money Laundering Act Section 10 (1) point a)

16.	The Player must provide a written statement to the Controller regarding whether pursuant to the laws of his country of residence he qualifies as a politically exposed person, close relative of a politically exposed person or a close associate of a politically exposed person. If the Player qualifies as a politically exposed person, his statement shall include the specification of which point in Section 4 (2)-(4) of the Money Laundering Act applies to him.	Money Laundering Act Section 9/A (1)
17.	If the Player qualifies as a politically exposed person, close relative of a politically exposed person or a close associate of a politically exposed person, his statement must include the information on the source of funds and the source of assets.	Money Laundering Act Section 9/A (2)
18.	Risk level classification of the Player (low, average, high)	Money Laundering Act Section 6/A and 10 (1) point b)
19.	e-mail address	SZTFH Decree Section 19 point a)
20.	username (unique)	SZTFH Decree Section 19 point b)
21.	existence and period of self-exclusion	SZTFH Decree Section 19 point c)
22.	subject and duration of the self-restriction measure	SZTFH Decree Section 19 point d)
23.	password related to the username (can be modified)	SZTFH Decree Section 20 (2)
24.	IP address of the Player's computer	Gambling Act Section 29/M
25.	data relevant to the time, duration and location of using the Service	E-Commerce Act Section 13/A (2)

During registration, the Controller is obliged to record the following personal data **regarding the type and performance of the Service provided:**

	Name of personal data	Legal basis for data processing: compliance with legal obligation [GDPR Article 6 (1) point c)]
1.	address, surname and given name, birth name, mother's name, place and date of birth	E-Commerce Act Section 13/A (1)-(2)
2.	player account and the entire data traffic thereof	Gambling Act Section 29/H (5), SZTFH Decree Section 24
3.	circumstances of performance (place, time, method)	Money Laundering Act Section 10 (1) point c)
4.	information on the purpose and planned type of business relationship	Money Laundering Act Section 10 (1) point d)

The data listed in this section (item 42) are hereinafter collectively referred to as: **data provided during registration.**

c) Duration of data processing:

The Controller retains the data provided during registration for the period set out in the applicable legislation, as follows:

- retention period of data processed under the Money Laundering Act is 8 years from the termination of the business relationship,
- retention period of data generated in relation to gambling organisation, under the Gambling Act or the SZTFH Decree is 6 years from generation of the data,
- The following data are processed by the Controller for 8 years following the termination of business relationship: e-mail address, username, password, player account and data traffic, data relevant to the time, duration and location of using the service, IP address, existence and period of self-exclusion, subject and duration of the self-restriction measure.

**44. Processing type: Player protection register**

- a) Purpose of data processing: the Controller shall verify whether the Player is under any restriction based on the data of the player protection register, before the registration of the Player and upon each online login instance following registration. The Controller shall inform the Player about denying registration based on the player protection register in e-mail.
- b) Range of processed personal data: surname and forename, birth surname and forename, mother's name, place and date of birth, type and number of personal identification document, home address. The Controller may access the player protection register for the sole purpose of fulfilling its verification obligation, using an electronic excerpt. The excerpt contains a non-reversible alphanumeric code generated from personal data. The Supervisory Authority of Regulatory Affairs (SZTFH) provides the Controller with the procedure for generating the alphanumeric code in an electronic form. Using the query, the Controller can compare the alphanumeric code generated from the personal data of the Player with the alphanumeric code included in the excerpt. If the two codes match, the Controller denies the registration of the Player, or provides no opportunity to play for the registered Player.
- c) Legal basis for data processing: compliance with a legal obligation [GDPR Article 6 (1) point c)]. Compliance with the legal obligation is required pursuant to Section 1 (6) of the Gambling Act and Sections 7, 8, 20 of the Game Organisation Decree.
- d) Processing period: time of verification and the notice sent to the Player is stored by the Controller for 5 years.

**45. Processing type: Phone communication**

- a) Purpose of data processing: ensuring communication with clients, communication with the Player. If the Player wishes to communicate via phone (as well), he can provide his mobile phone number for this purpose during registration.
- b) Range of processed data: mobile phone number of the Player.
- c) Legal basis for data processing: Consent of the data subject pursuant to Article 6 (1) point a) of the GDPR, the Player can disclose his phone number at his own discretion, if he wishes to.
- d) Processing period: until consent is withdrawn, but no later than the termination of the client relationship.

**46. Processing type: Enhanced customer due diligence, Foreign Player, client relationship**

- a) The purpose of data processing - in accordance with the provisions of the Money Laundering Act (Sections 7, 10, 17, 9/A), the Gambling Act (Section 29/H) and the Game Organisation Decree is to carry out high-level client due diligence measures in the cases set forth in Section 6 (1) of the Money Laundering Act (Money Laundering Act Section 17-17), to provide player protection (Gambling Act Section 29/H), to record the data specified in Section 13/a of the E-Commerce Act. The legal basis for each purpose is specified in the legislation indicated in brackets.
- b) In the case of foreign national Players – pursuant to Section 7 (3) item (ab) of the Money Laundering Act – the Controller is obliged to record the following personal data: passport or personal identification document, in case it authorises residence in Hungary, the document certifying residence in Hungary or the document authorising residence, official certificate of the permanent address in Hungary (the side of the address card not carrying the personal identification number), in case the address is located in Hungary. The legal basis for this processing is compliance with a legal obligation to which the Controller is subject, according to GDPR Article 6 (1) point c).
- c) In the course of registration, the Player enters his e-mail address. The Controller informs the data subjects pursuant to Article 13 (3) of the GDPR that it also processes the disclosed e-mail address for the purpose of providing customer services, in order to ensure that the Service can be provided to data subject at the highest level of standard. Processing period: till the termination of the contract. Legal basis for data processing: legitimate interest of the Controller [GDPR Article 6 (1) point f)]. (It is in the legitimate interest of the Controller to provide its service at the highest possible level, to communicate with Players live and to be able to inform the Players about the service. The Controller has carried out the purpose test in a separate document.)
- d) The Controller shall ensure that, with regard to the audited means of electronic communications as defined in the Money Laundering Act, the Controller shall, upon the Player's request, allow the Player to store data relating to his identification, authentication and declaration for a period appropriate to the purpose of data processing and to display the stored data in unchanged form and content. The Player shall send an e-mail with such subject to the [ugyfelszolgalat@vegas.hu](mailto:ugyfelszolgalat@vegas.hu) address to request information on the data recorded by the Controller about the Player in this regard.

**47. Processing type: Special data processing related to finalising the registration and the (simplified) client due diligence required thereto according to section 5.1.2 of the EULA**

- A. In case during the registration, according to the provisions of the EULA, the verification of personal identification is performed using the entry card issued to the Player by the live casino operated by the Controller, then in addition to the data provided during registration, the number of the entry card issued to the Player by the live casino operated by the Controller is also recorded. This data processing is optional, based on the Player's decision, its legal basis is conducting the steps of concluding the contract, requested by the Player (GDPR Article 6 (1) point b)). The Controller processes the card number (in the records of the online casino) till the termination of the contract.
- B. If the Player wishes to carry out a verification of identity by means of data query from a public register during registration, according to the provisions of the EULA, the Player must take a picture of the document to be used for identification purposes and then take a photo of himself using the software that executes identification electronically. The identification software then uses artificial intelligence to compare and analyse the Player's image and the image in the document used for identification purposes. The software is able to compare the face

with the image on the document and verify that the data match based on the unique characteristics. If identification is successful, the Data Controller shall, pursuant to Section 7 (7) of the Money Laundering Act and Section 29/H (2) of the Gambling Act, request data in electronic form from the register of personal data and addresses of citizens in order to verify the identity of the Player, to establish the correspondence of the data with the registration data and the validity of the identity document. Considering the fact that the above data are from data query from the relevant public register, in the verification check the Organiser considers these data approved (until any circumstances of reasonable doubt arise). Data obtained through data query from the public register remain in Hungary or an EEA member state.

The Player has multiple ways available to carry out the verification of identity, and he is free to choose the suitable option. If the Player does not give consent to the processing under this section or revokes such consent in the process, he is free to choose another means of identification.

- a) Purpose of data processing: identity verification of the Player through data query from a public register
- b) Range of processed personal data: name, birth name, nationality, number of the personal identification document, issue date, place and expiry, date and place of birth, photo of the identity document, mother's name, home address, Player's photo image and sex.
- c) Legal basis for data processing:
  - 1. Explicit consent of the data subject for the Player's photo image and sex, pursuant to GDPR Article 6 (1) point a) and Article 9 (1) point a).
  - 2. Compliance with the legal obligation pursuant to Article 6 (1) point c) of the GDPR with regard to name, birth name, nationality, number of the personal identification document, issue date, place and expiry, date and place of birth, mother's name, home address. The legal obligation is set out in Section 7 (1) and (7) of the Money Laundering Act and Section 29/H (2) of the Gambling Act.
- d) Duration of data processing:
  - 1. until consent is withdrawn, but no later than the successful matching of the Player's photo image with the photo in the document to be used for identification purposes, with regard to data processed based on consent,
  - 2. for data processed to comply with the legal obligation, 8 years from the termination of the business relationship.

UAB "iDenfy" is the processor of the Controller for the verification of personal identification.

The processing of data is subject to automated decision-making and profiling.

- i. purpose: matching of the characteristics and security features of the document with the requirements applicable to the document and matching of the facial features of the photo image in the document with the facial features of the image captured by the audited electronic communication device for the purpose of verification of identity;
- ii. range of data used: photo image, photograph on identity document;



- iii. legal effect on the Player as result: successful completion of the verification check / in the event of unsuccessful identification, the Player can contact the customer service of the online casino.
- iv. UAB “iDenfy” processes the data disclosed during data query from the public register for the verification of personal identification for up to 5 days.

#### 48. Processing type: Initiating the payment of winnings

- a) Purpose of data processing: payment of winnings to the Player. The Player can initiate payment of prizes in his player account, by providing his own bank account number as set out in the EULA.
- b) Range of processed personal data:
  - amount of payment withdrawal initiated by the Player,
  - bank account provided by the Player,
  - fact, date and time of initiating the payment.
- c) Legal basis for data processing: Performance of contract [GDPR Article 6 (1) item b)].
- d) Duration of data processing: 8 years after the termination of the business relationship.  
Data transfer: the Controller transfers the Player's full name, the amount of money and currency to be paid and the bank account number to the bank managing the account in order to process the payment.

#### 49. Processing type: Source of funds and assets

- a) Purpose of data processing: client due diligence, collection and assessment of information related to the source of funds and assets used for gambling.
- b) Range of processed personal data: the declaration on the source of funds and assets includes the following data: name, birth name, mother's name, place and date of birth, address / place of abode, nationality, type and number of identification document, and also the statement on the source of funds used for gambling.
- c) Data subjects: any Player who qualifies as a politically exposed person, close relative of a politically exposed person or close associate of a politically exposed person; who is requested to provide such statement based on a risk sensitivity factor by the Controller; also who qualifies as a client from high-risk third countries with strategic deficiencies.
- d) Legal basis for data processing: compliance with a legal obligation - GDPR Article 6 (1) point c). The legal obligation is set out in Section 9/A, 10, 16/A of the Money Laundering Act.
- e) Duration of data processing: 8 years after the termination of the business relationship (pursuant to Section 56 (2) of the Money Laundering Act).

#### 50. Processing type: Suspected money laundering and terrorist financing

- a) Purpose of data processing: compliance with reporting obligation.
- b) Range of processed personal data: name, birth name, mother's name, place and date of birth, nationality, address, identification document type, number and expiry date. (Based on Section 30 (2) item a) of the Money Laundering Act, in its report the Controller shall include the data pursuant to Sections 7 to 14/A of the act and the circumstances used as the basis of the report.)
- c) Legal basis for data processing: compliance with a legal obligation - GDPR Article 6 (1) point c). The legal obligation is set out in Section 30 (1) points a) to b) of the Money Laundering Act.
- d) Duration of data processing: 8 years after the termination of the business relationship (pursuant to Section 56 (2) of the Money Laundering Act).

**51. Processing type: Controlling and reporting restrictive financial and pecuniary measures provided by the EU / UN Security Council**

- a) Pursuant to Section 3 (6) of Act LII of 2017, the service provider must have a screening system in place which is able to ensure the prompt implementation of EU acts and UN Security Council resolutions ordering financial and asset-related restrictive measures. Purpose of data processing: identification of persons under financial and asset-related restrictive measures.
- b) Legal basis for data processing: compliance with a legal obligation [GDPR Article 6 (1) point c)]. The legal obligation is set out in Section 3 (6) of Act LII of 2017.
- c) Duration of data processing: 8 years after the termination of the business relationship.
- d) Data transfer: Pursuant to Section 4 (1) of Act LII of 2017, the Controller shall report to the National Tax and Customs Administration all data, facts, circumstances suggesting that the subject of the financial and pecuniary restrictive measure has funds or financial assets in the territory of Hungary that are subject to the financial and pecuniary measure.

**52. Processing type: record of the Player's balance/account (hereinafter: player account)**

- a) The purpose of data processing is to create and maintain a player balance for the Player at the start of the Player's registration for the purpose of keeping a verifiable record of the events of the player balance.
- b) Range of processed personal data:
  - i. Recording of the fact, details and date of crediting the winnings;
  - ii. Player's current balance at a specific time;
  - iii. Data included in the Player's payout request;
  - iv. In case of the suspension of the player account: the fact, time, reason of suspension; the fact, time of revoking suspension (SZTFH Decree Section 26 (3));
  - v. Tax identifier number for prizes from foreign jackpot systems (Gambling Act Section 29/Q).
- c) Legal basis for data processing: performing the legal obligation pursuant to Article 6 (1) point c) of the GDPR. The legal obligation is set out in Section 29/H (5) of the Gambling Act and Sections 23, 24, 25, 26 of the SZTFH Decree.
- d) Personal data according to this section are processed by the Controller for 8 years after the termination of the business relationship.

**53. Processing type: Records on the validity of the official identification document**

- a) The purpose of data processing - in accordance with the provisions of the Money Laundering Act (Sections 7, 10, 17), the Gambling Act (Section 29/H) and the Game Organisation Decree - is to carry out high-level client due diligence measures (Money Laundering Act Section 16-17), to provide player protection (Gambling Act Section 29/H) and to satisfy the principle of data quality (Money Laundering Act Section 11).
- b) Scope (and legal basis) of the processed personal data:
  - i. digital copy of the personal identification document (Money Laundering Act Section 7 (8))
  - ii. expiry of the document certifying personal identity (Money Laundering Act Section 7 (5))
- c) The Controller processes these personal data in order to perform legal obligations, based on the legal basis of legal obligations set forth in the legislation specified in point b) (GDPR Article 6 (1) point c)).

**54. Processing type: Keeping of server log/backup server log**

- a) The purpose of data processing is to ensure the logging process of the Online Casino server so that the chronological order of events and their recording can be accurately determined at all times.
- b) Scope (and legal basis) of the processed personal data:
  - i. Baseline settings and changes applied to the use of the Service;
  - ii. all the essential information related to the games played by the Player, including deposits, bet and prize data, bonus games, the winning combination, prize payment, financial transactions ;
  - iii. data necessary for the unique identification of the Player, including IP address, MAC address, port number;
  - iv. the Player's logins and logouts to and from the Online Casino and all successful and unsuccessful connection attempts and events;
  - v. The log shall include the name of the events, the date and time (with precision down to the second) and all other information clearly identifying the event.
- c) Legal basis of processing: performing the legal obligation pursuant to Article 6 (1) point c) of the GDPR. The legal obligation of the controller is set out in Annex 2 of the SZTFH Decree item A) point 6, as well as item B) points 7, 8 and 9.
- d) Duration of data processing: The Organiser shall retain the processed personal data for 6 years from the generation of the data.
- e) Data transfer: the Processor, as the operator of the technical IT system for online casino gaming, must provide the Gambling Authority with access to the logs in accordance with Annex 2, item B), point 9 of the SZTFH Decree.

## 55. Processing type: processing related to chat services, records of ban from chat services

Purpose of processing	Legal basis for data processing	Processed personal data	Duration of data processing
Customer service administration, collection of information and problem-solving using chat service (including objections to changes of the EULA).	performance of contract (GDPR Article 6 (1) item b)).	i. Name; ii. Username; iii. IP address; iv. E-mail address; v. Chat transcript.	5 years following recording the personal data
Gathering of information using chatbot service	Legitimate interest of the Controller (GDPR Article 6 (1) point f)).	i. Name; ii. Username; iii. IP address; iv. E-mail address; v. Chat transcript.	5 years following recording the personal data
Enforcing ban from the chat service, as set out in the EULA.	Legitimate interest of the Controller (GDPR Article 6 (1) point f)).	i. Name; ii. Username; iii. IP address; iv. E-mail address; v. Recording conduct of the Player violating provisions of the EULA;	5 years following recording the personal data

Provision of chat communication during live games broadcast from the online studio.	performance of contract (GDPR Article 6 (1) item b)).	i. Name; ii. Username; iii. IP address; iv. E-mail address; v. Chat transcript.	5 years following recording the personal data
Enforcing ban from chat communication service in live games broadcast from the online studio.	Legitimate interest of the Controller (GDPR Article 6 (1) point f)).	i. Name; ii. Username; iii. IP address; iv. E-mail address; v. Recording conduct of the Player violating provisions of the EULA; vi. Chat transcript.	5 years following recording the personal data

## 56. Processing type: Records on handling complaints

- a) Purposes of data processing: Management of complaints arising in relation to services provided by the Controller.

Range of processed personal data:

- i. Name, home address of the Player submitting the complaint;
- ii. Place, time, way of submitting the complaint;
- iii. Detailed description of the complaint, list of attached documents;
- iv. Unique ID of the complaint submitted by the Player;
- v. Result of investigation following the complaint, response to the complaint.

- b) Legal basis for data processing: Compliance with legal obligation pursuant to Article 6 (1) point c) of the GDPR. The legal obligation is set out in Section 17/A of the Consumer Protection Act.

The personal data processed with regard to the complaint shall be preserved by the Controller with the records taken on the complaint and a copy of the reply for three years, and these shall be presented to the controlling authorities upon request, in accordance with the provisions of Section 17/A (7) of the Consumer Protection Act. If requested, the Controller shall present the stored complaint to the Consumer Protection Authority.

## 57. Processing type: Implementing and recording self-restriction measures

- a) The purpose of data processing is to ensure the following self-restriction measures relevant to player protection:

- the possibility of self-exclusion for the period determined by the Player;
- defining the maximum daily, weekly, monthly loss;
- setting a deposit limit for each occasion;
- defining daily, weekly, monthly wagering limits;
- setting allowed time spent in the game.

- b) Range of processed personal data:

- i. existence, subject of self-restriction measures;
- ii. number of self-exclusions;
- iii. duration of self-exclusion;
- iv. cancellation of self-exclusion measures (for each data type: E-Commerce Act Section 13/A (1)-(3); SZTFH Decree Section 19 point c); Game Organisation Decree Section 13 (2));
- v. name;
- vi. username;

- vii. date of birth;
- viii. mother's name;
- ix. address;
- x. identification document number;
- xi. specific category of measure: maximised single or aggregated deposit payment, maximised loss, bets/total bets, maximised duration spent playing (SZTFH Decree Section 19 point d)).
- c) The legal basis of processing is performing the legal obligation pursuant to Article 6 (1) point c) of the GDPR. The legal obligation is set out in Section 29/I of the Gambling Act and Sections 11 to 13 of the Game Organisation Decree.
- d) Duration of processing: processing performed to ensure the self-restriction measure is aligned with the duration of the self-restriction measure, otherwise the Controller processes data for 8 years after the termination of the business relationship.
- e) Data transfer: pursuant to Section 13 (2) of the Game Organisation Decree, the Controller keeps monthly records of self-restriction measures, the numbers and durations thereof and the cancellation of self-restriction measures. The Controller provides remote access to its records for the Gambling Authority by no later than the 20th day after the subject month.

## 58. Processing type: Prize certificate

- a) The purpose of data processing is - upon the request of the Player entitled to winnings - the issue of the certificate on the prize, the HUF value and the legal title thereof, about prizes exceeding the actual value of 2 million HUF (or the same value denominated in another currency) (Gambling Act Section 1 (8)).
- b) Range of processed personal data:
  - i. Identification data of the Player;
  - ii. Data included in the Player's payout request;
  - iii. Location and date of winning and receiving the prizes;
  - iv. Amount of personal income tax deducted from the winnings.
- c) The legal basis of processing is performing the legal obligation pursuant to Article 6 (1) point c) of the GDPR. The legal obligation is set out in Section 1 (8) of the Gambling Act.
- d) The copy of the prize certificate intended for the Controller shall be processed by the Controller for 8 years pursuant to Section 169 (1) of Act C of 2000 on accounting.

## 59. Processing type: Ban records

- a) The purpose of data processing is the effective implementation of denying logging in to the online casino website and participating in gambling (Service) to the Player (hereinafter: ban) who committed a material violation of the EULA.
- b) Range of processed personal data:
  - i. Player's data pursuant to Section 29/H (1) of the Gambling Act: surname and given name, birth surname and given name, mother's name; address, or in the lack thereof: place of abode; nationality; identification document type, number; place and date of birth;
  - ii. In case of foreign national Players: place of abode in Hungary; nationality; type and number of the personal identification document; place and date of birth (Gambling Act Section 1 (5c));
  - iii. Fact, reason of the ban, time of ordering the ban (Gambling Act Section 1 (5c));
  - iv. Ad hoc nature of the ban, or the definite term of up to 5 years (Gambling Act Section 1 (5c)).

In order to ensure that the Player is notified about the ban:

  - v. E-mail address;
  - vi. Fact and date/time of the ban;
  - vii. scope and justification of the ban.



- c) Duration of data processing: The Controller can process the data of the ban records for 6 years after ordering the ban, and shall remove them after the 6-year duration expires (Gambling Act Section 1 (5c)).
- d) The Controller can transfer the data of the ban records to the Controller and other gaming casinos operated by the Controller (as an organiser of gambling), and the ban relevant to the Player can also be applied in these casinos (Game Organisation Decree Section 25 (2)).
- e) The legal basis of processing is performing the legal obligation pursuant to Article 6 (1) point c) of the GDPR. The legal obligation is set out in Section 1 (5c) of the Gambling Act and Section 25 (9) of the Game Organisation Decree.

## 60. Processing type: Disclosure of the username for promotional purposes

- a) Purpose of data processing: The Controller discloses the usernames of Players using its online service with third parties and publishes them on its own interfaces and the interfaces of third parties, for the purposes of recording and publishing promotion offers, bonus rankings and winners, for the publication of occasional and regular winners/winnings with a marketing purpose, as well as for the interests of display and broadcast of certain online games available under the service (including but not limited to the Youtube.com and Twitch.tv platforms).
- b) Range of processed personal data: under processing for this purpose, the Controller only processes and discloses the username of the Player. According to section 5.1.1 of the EULA the Player shall select a username that does not contain any reference to personal data of the Player.
- c) Legal basis for data processing: legitimate interest of the Controller [GDPR Article 6 (1) point f)]. (It is the legitimate interest of the Controller to promote its service (including through promotions) and to make its service convenient, live and transparent for Players. The Controller has carried out the purpose test in a separate document.)
- d) The duration of this processing ends upon objection of the Player, but no later than until the purpose is achieved or the publication page is operational.

**The Player may object to the publication of the username for promotional purposes at any time, free of charge, by contacting the Controller. In the event of an objection, the controller shall no longer process the relevant personal data in order to achieve the purpose of the processing. The objection may be communicated by the data subject via multiple channels, including:**

- via e-mail sent to the [ugyfelszolgalat@vegas.hu](mailto:ugyfelszolgalat@vegas.hu) e-mail address;
- via postal mail sent to the registered office of the Controller;
- via the chat window accessible on [www.vegas.hu](http://www.vegas.hu).

With regard to this purpose of processing, the Controller involves processors (under a separate legal relationship) that act with the purpose of providing the online (web) broadcast, in addition to processing the personal data specified in the scope of this purpose. The persons/entities acting as such processors may be subject to change depending on the web interface and the game type, and therefore their fixed identification is impeded, in accordance with the WP260 guidelines. In order to ensure a high degree of conformity with Article 14 of the GDPR, the Controller identifies the affected processors according to their activity, and provides the opportunity for the data subjects to separately request information on the matter.

## 61. Processing type: Sending of newsletter containing general and personalised marketing offers

- a) The purpose of the data processing is to provide general and personalised information, including news about current events, bonuses and promotions of the Controller's online and

offline casino and betting services, to those Players who have given their prior and explicit consent. The Player can determine the channels through which communication is made (e-mail, SMS, app push notification, web push notification).

- b) Processed personal data: name, e-mail address and/or phone number.
- c) Legal basis for data processing: the legal basis for sending marketing offers is the voluntary, explicit and informed consent of the Player, pursuant to Article 6 (1) point a) of the GDPR, in accordance with Section 6 (1) of the Business Advertising Act. Processing period: processing is performed until consent is withdrawn (unsubscribe), till a request for self-exclusion is made or, in the lack of the former, until the customer relationship is terminated or self-exclusion expires.
- d) In the framework of sending offers of marketing purposes, the Controller may also advertise services not offered for persons under the age of 18 (pursuant to Section 1 (5b) of the Gambling Act) or which may involve the restriction pursuant to Section 8 (1) of the Business Advertising Act. Only such persons can subscribe to the marketing offers who have provided statement on being at least 18 years old.
- e) The Player may revoke consent at any time, without any limitation or necessary justification, free of charge:
  - via e-mail sent to the [ugyfelszolgalat@vegas.hu](mailto:ugyfelszolgalat@vegas.hu) e-mail address;
  - via postal mail sent to the registered office of the Controller;
  - via the chat window accessible on [www.vegas.hu](http://www.vegas.hu);
  - on the [www.vegas.hu](http://www.vegas.hu) website, after logging in and updating the personal preferences.
  - In case of unsubscribing, requests are processed by the Controller in a couple of days following receipt, and action is taken to terminate sending marketing-purpose offers to the unsubscribing Player as soon as possible. The Player can unsubscribe with instant effect when changing the relevant personal preferences in the player profile.

## 62. **Processing type:** remarketing enquiries

- a) Purpose of data processing: remarketing enquiries enable Vegas.hu to display advertisements for its services to the Player when visiting a website on the list managed by Ads Interactive FZCO and Adform A/S, provided that the Player consents to the marketing communications upon registration.
- b) Processed personal data: e-mail address, IP address, cookies.
- c) Processing period: until consent of the data subject is withdrawn or registration is cancelled.
- d) Data transfer: with regard to the data processed during remarketing, the involved service provider (Ads Interactive FZCO and Adform A/S) is considered a data processor.

## 63. **Profiling for the assessment of personal characteristics**

- a) Purpose of data processing: in the course of profiling, the Controller analyses the Player's purchase and game data, trains Player groups (segments) for the purpose of developing and displaying, in case of consent with marketing content, personalised offers to the Players after classification into groups, and also to improve its business processes based on these information.
- b) Range of processed personal data: the personal data provided by the Player during registration, online reference number, previous games, transactions, data from previous games and data generated during the use of Vegas.hu.
- c) Legal basis for data processing, i.e. profiling: legitimate interest of the Controller [GDPR Article 6 (1) point f)]. It is the legitimate interest of the Controller to increase its profitability and, in this context, to promote its services and encourage Players to continue to use the services it provides. The Controller has carried out the purpose test in a separate document.) The Player may object to profiling at any time, free of charge, by way of **contacting the Controller. In the event of an objection, the controller shall no longer process the**

**relevant personal data for the purpose of profiling. The objection may be communicated by the data subject via multiple channels, including:**

- via e-mail sent to the [ugyfelszolgalat@vegas.hu](mailto:ugyfelszolgalat@vegas.hu) e-mail address;
  - via postal mail sent to the registered office of the Controller;
  - via the chat window accessible on [www.vegas.hu](http://www.vegas.hu).
- d) Duration of processing: profiling is performed till the objection of the data subject, or (in the lack thereof) the termination of the client relationship.
- e) During the registration of the Player, the controller assigns the Player an online reference number containing no personal data, accessible in his user account after registration.. When the Controller carries out analyses for the purpose of improving its service, it uses the online reference number to ensure that the analysed data cannot be linked to a specific person, but only the activity of users organised in segments and their usage of the service can be analysed.
- f) Processor: The service providers used in the processing of data during profiling and in sending marketing offers to the target group specified in connection with the processed data (Simplify Technologies AB and Flows Ltd.) are considered data processors.

#### **64. Processing type: Processing relevant to the use of social media websites**

The Controller operates its Facebook page to publish news relevant to its operation, information, current campaigns and games.

- a) Purpose of data processing: providing information to Players on the Controller's Facebook page, promoting the activities of the Controller.
- b) Range of processed data: name, comment, review.
- c) Legal basis for data processing: consent of the data subject [GDPR Article 6 (1) point a)]. (Withdrawal of consent shall not affect the lawfulness of processing carried out on the basis of consent prior to its withdrawal.)
- d) Data subjects: fans (people who like the page), followers, commenters who have a Facebook profile.
- e) Duration of data processing: until deletion upon the request of the data subject, but no later than the termination of the social media page.
- f) Facebook page of the Controller: <https://www.facebook.com/vegaskaszino>

For the use of the Facebook page the Data Subject must have his own account on the social media website. Operators of social media websites perform processing as independent controllers, according to the terms set out in their own privacy information documents. The controller for Facebook is a Meta Platforms Ireland Ltd. (4 Grand Canal Square, Grand Canal Harbour, D2 Dublin Ireland). By using Facebook, the data subject declares to have read and accepted the proprietary conditions of use and privacy information document of Facebook. <https://www.facebook.com/policy.php>

Facebook receives the information that the data subject wishes to post on the social media page of the online casino, with the data subject's IP address. Rights related to the data (name, photo, comment, rating) that the Data Subject wishes to post, rights can be directly exercised vis-à-vis Facebook, or the Data Subject can contact the Controller.

The Controller can initiate the deletion of data that violate the reputation or rights of the Controller or any third party.

The processing of data for statistical purposes during the use of Meta products is carried out between the Controller and Meta Platforms Ireland Ltd. (4 Grand Canal Square, Grand Canal Harbour, D2 Dublin Ireland) as joint processing. Detailed information on site analytics is available under the following link: [https://www.facebook.com/legal/terms/page\\_controller\\_addendum](https://www.facebook.com/legal/terms/page_controller_addendum)

On 10 July 2023, the European Commission adopted its adequacy decision on the EU-US Data Protection Framework ("DPF"). The Decision concludes that the United States provides an adequate level of protection for personal data transferred from the EU to US entities participating in the DPF and therefore personal data can be transferred from the EU to US entities participating in the DPF without the application of additional data protection safeguards. Meta is considered a DPF participating organisation.

## 65. **Processing type: Security check of documents used for registration**

The Controller is entitled to carry out the following processing and take the following measures, as set out in the EULA, in order to detect and prevent registration with falsified data; prevent the misuse of bonuses resulting from registration with false data::

65/ If doubts arise about the authenticity of the document, for security reasons the Controller shall compare the photo of the foreign document in a format unknown to the Data Controller, uploaded during registration, with ID photo images in a similar format uploaded to publicly available databases.

Range of processed data: photo of the document used for registration and personal data specified on the document.

Data subjects: person initiating registration.

Legal basis for data processing: legitimate interest of the Controller [GDPR Article 6 (1) point f)]. (It is the legitimate interest [business and economic interest] of the Controller to ensure the security of the service, the fairness of online games and protection of the Players. The Controller has carried out the purpose test in a separate document.)

Duration of data processing: search results are not stored, thus the duration of processing is limited to the day of conducting the check.

Processor: Google Ireland Limited (registration number: 368047; Gordon House, Barrow Street Dublin 4 Ireland). Privacy policy of this processor: <https://policies.google.com/privacy?hl=en-US>

65/B For security reasons, the Controller is entitled to request from the person initiating registration or the Player a photograph showing the Player's face and the identification document held next to his face.

Range of processed personal data: photo.

Data subjects: person initiating registration, Player.

Legal basis for data processing: legitimate interest of the Controller [GDPR Article 6 (1) point f)]. (It is the legitimate interest (business and economic interest) of the Controller to ensure the security of the service, the fairness of online games and protection of the Players. The Controller has carried out the purpose test in a separate document.)

Duration of data processing: Successful objection of the Player, but no later than 8 days after the submission of the photo.

## 66. **Processing type: Client satisfaction survey**

- a) Purpose of data processing: the Controller may contact registered Players for the purpose of a client satisfaction survey in order to gain a better overview of the use of its services and the opinions of its customers, and to improve the quality and use of its services.

These contact efforts are made by e-mail. If the data subject does not wish to take part in the survey, he may disregard the request and can object to the processing at any time, free of charge. In the event of an objection, the Controller shall no longer process the relevant personal data.

- b) Range of processed data: name, e-mail address, answer to the questions. The answers received may be evaluated as statistical data or in a personalised form.

- c) Legal basis: legitimate interest of the Controller [GDPR Article 6 (1) point f)]. (The legitimate interest of the Controller is to maintain its services and to increase the quality and use of its services, which is a business and economic interest. The Controller has carried out the purpose test in a separate document.)
  - d) Processing period: until objected by the data subject, in the lack thereof, till the completion of the processing purpose, but for no more than 1 year.
- 67. Processing type: Data processed for the sending of system messages**
- a) Purpose of data processing: the Controller sends e-mail notification to the Player to finalise already commenced registration. The Controller sends notification to the Players via e-mail, app push message, web push message, in-app message and other similar electronic means of any downtime, malfunction, repair, interruption or other non-promotional circumstances related to the operation of the technical/IT system of the online casino game.
  - b) Range of processed personal data: Player's name and e-mail address.
  - c) Legal basis: Legitimate interest [GDPR Article 6 (1) point f)]. The Controller has carried out the purpose test in a separate document.
  - d) Duration of data processing: 5 years after sending the message (general civil law limitation period).
- 68. Processing type: Recording calls received at the central phone line:**
- a) Purpose of processing: Preventing unlawful actions and ensuring lawful operation.
  - b) Range of processed personal data: Time of call (day, hour, minute); caller number, extension called; voices of the participants in the conversation, any personal data/information spoken during the conversation.
  - c) Legal basis: legitimate interest of the Controller [GDPR Article 6 (1) point f)]. The Controller has carried out the purpose test in a separate document.
  - d) Processing period: 7 calendar days after the recording was made. If the data subject objects to the processing of his personal data and there are no overriding legitimate grounds, the Controller will delete the personal data.
  - e) If any other authority - including the Police - sends request to the Controller, the requested information will be disclosed by the Controller based on legislative obligation. In certain cases, the Controller may initiate the proceedings of relevant authorities.
- 69. Processing type: Ensuring the fairness of the games**
- a) Purpose of processing: Preventing, identifying and combating fraud and abuses.
  - b) Range of processed personal data: Player's name, username, game ID, all the essential information related to the games played by the Player, including deposits, bet and prize data, bonus games, the winning combination, prize payment, financial transactions. Sanctions applied in relation to identified fraud and abuse.
  - c) Legal basis: legitimate interest of the Controller [GDPR Article 6 (1) point f)].
  - d) (It is in the legitimate interest of the Controller to prevent fraudulent abuse attempts that cause financial damage. Furthermore, it is in the Controller's legitimate interest to ensure the fairness of the game, safe operation and the trust of other Players in the game.)
  - e) The Player can object processing at any time, free of charges.
  - f) Duration of data processing: Screening and identification of fraud and abuse continues until the termination of the contract with the Player. In the case of sanctions for identified fraud and abuse, 5 years from the date of identification.
  - g) If the identified fraud or abuse also constitutes an offence under Act C of 2012 on the Criminal Code, the Controller may file an official report and forward data necessary for the investigation to the competent investigative authority pursuant to section 69 herein.



## 70. Processing type: Provision of promotional services

- a) Purpose of processing: Organising and conducting promotions within the framework of promotional service, verifying compliance with the conditions, payment of prizes.
- b) Range of processed personal data: name, vegas.hu player ID, e-mail address, data enabling verification of compliance with the conditions of the promotion, data relating to financial transactions for the payment of the prize.
- c) Legal basis: Performance of contract [GDPR Article 6 (1) item b)]. The Player may set up to participate in the promotions offered by the Controller in the framework of promotional services in his user account, which generates a contract to which the Player is party. The Player can change this setting at any time, and thus the promotional service will be terminated with immediate effect.
- d) Duration of data processing: 5 years after the termination of the promotional service.

## 71. Processing type: processing saved bank card data

- a) Purpose of data processing: in order to provide a more comfortable experience of depositing money to the account, the Player can save bank card data in cases of the SimplePay and K&H financial service providers. This ensures that the Player does not have to repeatedly enter its bank card details upon the next deposit to the account.
- b) Range of processed personal data: Player's name, first 6 and last 4 digits of the bank card number.
- c) Legal basis: Bank card details can be saved by clicking on the "consent" field by the Player. This consent can be revoked by the Player at any time, by removing the relevant field in the Player profile or submitting such explicit request to the [kifizetes@vegas.hu](mailto:kifizetes@vegas.hu) e-mail address.
- d) Processing period: until the Player's consent is revoked, or otherwise until the contract with the Player is terminated.

## DATA TRANSFER

The Controller may only transfer the personal data of the Player to third parties in the cases specified below.

## 72. Bank card deposit to the player account using the OTP SimplePay application

- a) Purpose of processing: The purpose of Processing is to ensure the payment to the Player's account by means of a payment transaction through the OTP Simple Pay system.
- b) Range of processed personal data: surname, first name, country, phone number, e-mail address, IP address of the Player used to carry out the transaction, transaction data (amount of the transaction, date of execution, address data (country, city, street))
- c) Legal basis: Performance of contract [GDPR Article 6 (1) item b)].
- d) Processing period: 8 years pursuant to Section 169 (1) of Act C of 2000 on accounting.
- e) Processor: During the payment process, the Player is redirected to the secure payment site of OTPSimplePay ("OTP SimplePay") operated by SimplePay Zártkörűen Működő Részvénytársaság ("SimplePay Zrt."), where the payment will be made. Upon redirection, the Controller transfers the following data to SimplePay Zrt. as the data processor in order to process the payment: (i) surname; (ii) first name; (iii) country; (iv) phone number; (v) e-mail address.

Contact details of SimplePay Zrt.: registered office: 1138 Budapest, Váci út 135-139. B. ép. 5. em.; registration number: 01-09-174466; e-mail address: [ugyfelszolgalat@otpmobil.com](mailto:ugyfelszolgalat@otpmobil.com);

website address: [www.otpmobil.hu](http://www.otpmobil.hu). The OTP SimplePay privacy policy is available at: <https://simplepay.hu/adatkezelesi-tajekoztatok/>

- f) When the Player enters the OTP SimplePay application, SimplePay Zrt. shall be considered an independent controller with regard to the personal data provided in the app for payments by card. During payment by bank card, LVC Diamond Játékkaszinó Üzemeltető Korlátolt Felelősségű Társaság does not perform any data processing, data collection or other processing activities, and does not have access to these personal data. After successful payment, the OTP SimplePay application redirects the Player to the Controller's website and informs the Controller about the transaction data (amount of the transaction, date of execution, address (country, city, street)).
73. **Data transfer based on official request:** Pursuant to Sections 261 to 265 of Act XC of 2017 on criminal procedure (Criminal Procedure Code) the court, the state attorney and the investigating authority, or the body conducting preliminary proceedings may contact any legal person (controller) to request data. Under this request, the transfer of data, transfer of electronic data/documents, provision of information can be requested. In case of requests to be fulfilled in an electronic form, the deadline of at least 1 day but no more than 30 days, in case of requests fulfilled in any other way, the deadline of at least 8 days but not more than 30 days can be specified. The entity contacted in the course of a data request - unless otherwise regulated in law - shall comply with the request within the specified deadline, or give information about any impediment to fulfilling such requests without delay.  
If any other authority - including the National Tax and Customs Administration - sends request to the Controller, the requested information will be disclosed based on legislative obligation. In certain cases, the Controller may initiate the proceedings of relevant authorities.
74. **Data transfer to the affected authorities:** pursuant to the money laundering prevention policy of the Controller, in case of circumstances suggesting money laundering, it shall inform the relevant authorities in each case, including the National Tax and Customs Administration Hungarian Financial Intelligence Unit or the Gambling Authority. Pursuant to Section 1/A (1) of the Gambling Act, the Controller is required to provide access for the Gambling Authority to the records of the processed personal data, in order to perform the tasks specified in Act XXXII of 2021 on the Supervisory Authority of Regulated Activities. Pursuant to Section 17/A (7) of the Consumer Protection Act, the handled complaint shall be presented to the Consumer Protection Authority by the Controller, upon request.
75. **Data transfer for confirming financial transactions:** In order to control the validity of financial transactions, and to identify any possible financial abuses, the Controller is authorised to transfer data to K&H Bank Zrt. (registered office: 1095 Budapest, Lechner Ödön fasor 9.) and K&H Pénzforgalmi Szolgáltató Kft. (registered office: 1095 Budapest, Lechner Ödön fasor 9.) (hereinafter: K&H) based on legitimate interest of the Controller [GDPR Article 6 (1) point f)], pursuant to the provisions of the agreement concluded with K&H.  
Upon request submitted in writing, the Controller discloses with K&H the data certifying the identity of the Player, as well as data that certify the completion of the specific transaction subject to the report/complaint (payment transaction receipt). Scope of personal data transferred in this regard: name; address; number of official document suitable to confirm personal identity (personal identification document, driver's licence or passport) and the official certificate of the permanent address (address card), userID.
76. **Data transfer to - service provider - partners of the Controller, as data processors:**

- a) **Game management:** Finnplay Technologies Oy; [Miestentie 9, 02150 Espoo, Finland] – It accesses the data stored in the Controller’s system for providing the IT background of certain games and management as well;
- b) **Gaming service providers:**
- i. Greentube GmbH (Wiedener Hauptstrasse 94, 1050, Wien, Austria);
  - ii. Play ’n Go Malta Ltd. (Vincenti Buildings, 28/19 (Suite 1026) Strait Street, Valletta VLT 1432, Malta);
  - iii. HABANERO Systems Ltd. (Level 5 Quantum House, 75 Abate Rigord Street, Ta’Xbiex, XBX 1120, Malta);
  - iv. Evolution Malta Limited (Level 1, Spinola Park, Mikiel Ang Borg Street, St Julians SPK 1000, Malta);
  - v. Amusnet Gaming Ltd. (EET) (Villa Ichang, Triq Mons. Alfredo Mifsud, Fl.1, Ta’Xbiex XBX 1063, Malta);
  - vi. Edict Malta Limited (No.2, Geraldu Farrugia Street, Zebbug, ZBG, 4351, Malta);
  - vii. Ezugi N.V. Van Engelenweg 23, Curacao, Netherlands- data centre located at: the branch sites of S.C. GTS Telecom, S.R.L., Bucharest, Romania;
  - viii. N-Serve Ltd. (Triq it-Torri Wejter, Birkirkara, BKR 4730, Malta);
  - ix. Arrise Solutions (Malta) Limited (Falcon House Block E, Main Street, Sliema SLM1455, Malta);
  - x. Sub Tech Ltd. (Suite 7, Valletta Buildings, South Street, Valletta, VLT 1103, Malta);
  - xi. Yggdrasil Gaming Limited (Level 2, Tagliaferro Business Centre, High Street, c/w Gaiety Lane, Sliema SLM 1551, Malta)
  - xii. Relax Gaming Ltd. (Block 6, Floor 4, Paceville Avenue Street, St Julian’s, STJ 3109, Malta)
  - xiii. ISB Ena Limited (27 Gregory Afxentiou Street, Lanarca, Cyprus)
  - xiv. Evoplay Development Ltd. (28 Oktovriou & Aimiliou Chourmouziou, Lophitis Business Centre I, 4th Floor, Flat/Office No. 403, 3035, Limassol, Cyprus)
  - xv. Playson Limited (Valletta Buildings, Second Floor, Suite 7, South Street, Valetta, Malta);
  - xvi. EGT Digital Ltd. (Rich Hill Business Center, 6 Panorama Sofia St., Sofia Park, Sofia 1766, Bulgaria);
  - xvii. Thunderkick Malta Ltd. (The Bastions, Office no. 2, Emvin Cremona Street, Floriana FRN 1281, Malta);
  - xviii. Galois Srl (Via dei Prati Fiscal 199, 00141 Roma, Italy)
- the above companies operate certain games available on the online casino website, and therefore as data processors, these companies process certain personal data of the Data Subjects using the specified games;
- c) **Chat service:** LiveChat Inc. [One International Place Suite 1400 Boston, MA 02110-261, United States of America] – it operates the chat service available on the online casino website as a third party agent, and therefore this company qualifies as a data processor regarding the information transferred as regards the chat service.
- The Controller informs data subjects that the processing of personal data in relation to the chat service involves the transfer of personal data to a third country (the United States), which is however not considered risky, taking into account that the processor applies binding corporate rules under Article 47 of the GDPR (<https://www.livechat.com/legal/data-processing-addendum/>).
- d) **Segmentation of personal data in connection with profiling and personalisation and sending of marketing offers:**
- Symplify Technologies AB (registration number: 556589-7294, registered office: Drottninggatan 55, 111 21 Sweden, Stockholm; phone: +46 8 505 721 00; email: [info@symplify.com](mailto:info@symplify.com); privacy policy: <https://symplify.com/privacy-policy/>).

- Flows Ltd (registration number: 13303855, registered office: C/O Rw Blears Llp, Suite 32 Brookside Business Park, Cold Meece, Stone, England; privacy policy: <https://flows.world/privacy-policy/>).

e) **Remarketing-purpose enquiries:**

- Ads Interactive FZCO (Building A2 Silicon Oasis DDP, Dubai UAE);  
- Adform A/S (Silkegade 3B, ST. & 1., 1113 Copenhagen, Denmark);  
- a Meta Platforms Ireland Ltd. (4 Grand Canal Square, Grand Canal Harbour, D2 Dublin Ireland).

f) **Data collection with statistical purpose:** Google Analytics - Google Ireland Limited (registration number: 368047; Gordon House, Barrow Street Dublin 4, Ireland; <https://policies.google.com/terms?hl=hu>).

g) **Hosting service provider:** Shock Media B.V. (Twentepoort Oost 18, 7609 RG Almelo, The Netherlands).

h) Identification using an audited communication device: the identification is carried out electronically by iDenfy (UAB "iDenfy", registered office: Baršausko street 59, 51423 Kaunas, Lithuania; phone: +370 640 84466; email: [dpo@idenfy.com](mailto:dpo@idenfy.com); website: [www.idenfy.com](http://www.idenfy.com)).

i) **Compiling forms necessary for customer satisfaction feedback (item 66) and promotional services (item 70) data processing purposes, and statistical evaluation of the data provided:** Survio s.r.o. (registered office: Hlinky 995/70, 603 00 Brno, Czech Republic, contact address: Hlinky 78a, Brno, 603 00, Czech Republic; privacy policy: <https://www.survio.com/hu/szemelyes-adatok-vedelme>

j) **Measurement and assessment of actions on the website in order to improve user experience** (e.g. mouse clicks, mouse movements, keystrokes, scrolling activities and pages visited): Microsoft Clarity - Microsoft Ireland Operations Ltd., One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, Ireland

The Controller also transfers personal data to the United Kingdom, in which case we inform you that the European Commission has issued an adequacy decision in relation to the United Kingdom (COMMISSION IMPLEMENTING DECISION of 28.6.2021 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by the United Kingdom). The adequacy decisions have confirmed that personal data are also adequately protected in these countries.

## 77. Cloudflare content provider network

In order to enhance security and optimise the display speed of the [www.vegas.hu](http://www.vegas.hu) website, the Controller uses the Cloudflare content provider network ("CDN"). A CDN helps website content - especially large media files such as graphics and text - to be made available faster through a geographically distributed network of servers, and includes security features (such as DDoS protection) to protect the website.

Legal basis for using the CDN: legitimate interest of the Controller [GDPR Article 6 (1) point f)]. It is in the legitimate interest of the Controller to provide its online services in a secure and efficient manner. The Controller has carried out the purpose test in a separate document.

The data transmitted through the CDN network are those which the Player provides to the Controller when using the website. Data are transmitted in encrypted form.

Processor of the Controller during the use of the CDN is Deimos Cloud (pty) Ltd. (registered office: 50 Canterbury street, Cape Town 8001). The Controller has concluded a data processing agreement in accordance with the GDPR. Data processing takes place mainly in the European Union. In the course of providing the service, data may be transferred to a third country only if it has been established, pursuant to Article 45 of the GDPR, that the level of data protection

in that country is equivalent to the level of data protection in the EU or if the recipient of the data ensures an adequate level of data protection by other means provided for by the GDPR. Processing period: till achievement of the purpose of processing, but not longer than 1 year. The Player can object processing at any time, free of charges.

The privacy policy of the processor is available at: <https://www.deimos.io/privacy-policy>

#### 78. **Transfers to law office:**

In specific cases, including requests and complaints from the data subjects, the Controller cooperates with the Lajer Ügyvédi Társulás (Lajer Attorneys Partnership, 1024 Budapest, Lövház utca 30.) as the data protection officer of the Controller. The law office processes the disclosed personal data in accordance with the applicable legislation.

#### 79. **Cookies and data collection for statistical purposes**

An HTTP cookie (or simply: cookie) is an information package sent by the server to the browser and then returned by the browser to the server with each request submitted to the server. Cookies are generated by the web server using the browser on the user's computer where they are stored in a dedicated folder. The cookie is a small-size text file which is saved on the computer of the User when he visits a website. Cookies can have multiple functions, including (but not limited to) collecting information, saving user preferences, enabling the website owner to better understand user habits, and certain cookies are necessary for the operation and operability of the website.

The application of cookies (allow/block) can be set up in the browser by the User according to the following process:

- Android: Via Google Chrome
- Microsoft Edge: <https://support.microsoft.com/hu-hu/help/10607/microsoft-edge-view-delete-browser-history>
- Firefox: <https://support.mozilla.org/hu/kb/weboldalak-altal-elhelyezett-sutik-torlese-szamito>
- Google Chrome: <https://support.google.com/chrome/answer/95647?hl=hu&co=GENIE.Platform=Desktop>
- iOS: <https://www.apple.com/legal/privacy/en-ww/cookies/>
- Opera: <https://help.opera.com/en/latest/web-preferences/#cookies>
- Safari: <https://support.apple.com/hu-hu/guide/safari/sfri11471/mac>
- Samsung Internet: <https://www.samsung.com/uk/support/mobile-devices/what-are-cookies-and-how-do-i-enable-or-disable-them-on-my-samsung-galaxy-device/>

For more information about the cookies used by the online casino website, please refer to the cookie policy on the online casino website under "Cookie settings".

#### **RIGHTS RELATED TO DATA PROCESSING**

The following is a summary of the Player's rights vis-à-vis the Controller in relation to the processing of his personal data.

80. **Right of information and access by the data subject (GDPR Article 15):** regarding the data subject rights of the Player relevant to data protection, he can contact the Controller via the contacts designated in this Information document and the Vegas.hu website. The Player shall have the right to obtain from the Controller confirmation as to whether or not personal data concerning him are being processed, and, where that is the case, access to the personal data with the following scope.



The range of information related to data processing provided in the course of such access by the Controller shall include the following:

- a) source of processed personal data;
- b) purpose and legal basis for data processing;
- c) range of processed personal data;
- d) in the case of transferring the personal data, the range of recipients of data transfer (including third-country recipients and international organisations);
- e) duration of the retention of the processed personal data, criteria for specifying this time-period;
- f) rights of the data subject under the Freedom of Information Act and the GDPR, and the means of enforcing such rights;
- g) fact of applying automated decision-making and profiling (if applicable),
- h) the circumstances of personal data breaches occurring in relation to the processing of the personal data of the data subject, the impacts thereof and the measures taken to handle such breaches,
- i) right to submit complaints to the supervisory authority.

81. **Right to rectification (GDPR Article 16):** during the existence of the business relationship, the Player shall be based on Section 12 (3) of the Money Laundering Act - inform the Controller (via the customer service of the online casino) about any changes affecting his data provided during registration or subsequently updated, within 5 business days after receiving information thereof. In case the Player fails to report any changes to his personal data without delay, the Player shall be liable for any consequences thereof. In case the submitted personal data is deemed inaccurate, and the correct personal data is at the

Controller's disposal, the Controller shall rectify the personal data in question automatically.

82. **Right to erasure (GDPR Article 17):** the data subject shall have the right to obtain from the Controller the erasure of personal data concerning him without undue delay, and the Controller shall have the obligation to erase personal data relevant to the data subject without undue delay, when one of the following grounds applies:
- a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
  - b) the data subject withdraws consent on which the processing is based and there is no other legal ground for the processing;
  - c) the data subject objects to processing, there are no overriding legitimate grounds for the processing, or the data subject objects to the processing on the basis of Article 21 (2) of the GDPR;
  - d) the personal data have been unlawfully processed;
  - e) the personal data have to be erased for compliance with a legal obligation in EU or Member State law;
  - 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.

The Controller however is not required to erase the processed personal data in the case of the above circumstances, to the extent that processing is necessary:

- a) for exercising the right of freedom of expression and information;
- b) for compliance with a legal obligation which requires processing by EU or Member State law to which the Controller is subject, or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Controller;
- c) for reasons of public interest in the area of public health;

- d) for archiving or statistical purposes, as well as scientific or historical research purposes in so far as erasure is likely to render impossible or seriously impair the achievement of the objectives of that processing; or
  - e) for the establishment, exercise or defence of legal claims.
83. **Right to object (GDPR Article 21):** the Player shall have the right to object, on grounds relating to his particular situation, to processing of personal data concerning him according to this Information document, based on a legitimate interest. In such cases, the Controller shall no longer process the personal data unless the Controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the Data Subject or for the establishment, exercise or defence of legal claims.
84. **Right to restriction of processing (GDPR Article 18):** the Player shall have the right to obtain from the Controller restriction of processing where one of the following applies:
- a) the accuracy of the personal data is contested by the Player, for a period enabling the Controller to verify the accuracy of the personal data;
  - b) the processing is unlawful and the Player opposes the erasure of the personal data and requests the restriction of their use instead;
  - c) the Controller no longer needs the personal data for the purposes of the processing, but they are required by the Player for the establishment, exercise or defence of legal claims;
  - d) the Player has objected to processing, pending the verification whether the legitimate grounds of the Controller override those of the Player.

Where processing has been restricted as specified above, such personal data shall, with the exception of storage, only be processed with the Player's consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person, for reasons of important public interest. When the restriction of processing is lifted, the requesting Player shall be informed by the Controller in advance.

85. **Right to data portability (GDPR Article 20):** the Player shall have the right to receive the personal data concerning him, which he has provided to the Controller based on the Player's consent or in order to perform the contract, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided. This right can only be exercised regarding personal data processed based on the legal basis of consent or performing the contract, in case data processing is carried out in a digital form.
86. **The Controller shall comply with/respond to the exercise of the right to personal data processing without undue delay, but at the latest within one month of the submission of the request.** Taking into account the complexity of the request and the number of requests, this one-month time limit may be extended by a further two months by means of a reasoned communication to the Data Subject within one month of the submission/receipt of the request to the Controller.
87. If the Controller does not take action on the above request of the Player, the Controller shall inform the data subject without delay and no later than within 1 month of receipt of the request of the reasons for not taking action, as well as on the possibility of lodging a complaint with the Authority and seeking a judicial remedy.
88. The Controller only reviews and answers the e-mail sent by the Player regarding data processing, if it is sent from the e-mail address provided by the Player during registration or

subsequently updated (unless the Player claims in the message that his e-mail address is changed, or it enables the personal identity of the Player to be clearly ascertained).

## **RIGHT TO REMEDY**

89. **Initiating proceedings of the Authority:** The Player shall have the right to notify the Authority and request an investigation alleging an infringement relating to his personal data, or if there is imminent danger of such infringement. The Authority shall carry out the investigation free of charge; the costs thereof shall be advanced and borne by the Authority. Having submitted a notification to the Authority may not entail any discrimination against the notifier. The Authority may reveal the person of the notifier only if the inquiry cannot be carried out otherwise. If so requested by the notifier, the Authority shall not disclose his identity even if the inquiry cannot be carried out otherwise (Freedom of Information Act Section 52). Contact data of the Authority:  
Hungarian National Authority for Data Protection and Freedom of Information, Nemzeti Adatvédelmi és Információszabadság Hatóság (address: 1055 Budapest, Falk Miksa utca 9-11.; mailing address: 1363 Budapest, Pf. 9.; e-mail: [ugyfelszolgalat@naih.hu](mailto:ugyfelszolgalat@naih.hu); website: <http://naih.hu>; phone: +36 (1) 391-1400)
90. **Judicial enforcement of rights:** in the event of any infringement of his rights, the Player may turn to court action against the Controller. The action shall be adjudicated before the regional court. The action shall be heard by the competent tribunal according to the registered office of the Controller. If so requested by the Player, the action may be brought before the regional court in whose jurisdiction the Player's address or place of abode is located. Jurisdictions of the regional courts can be confirmed using the "Court finder" application on the [www.birosag.hu](http://www.birosag.hu) website. The court shall hear such cases in priority proceedings (Freedom of Information Act Section 23).
91. **Damages and restitution:** The Controller shall be liable for any damage incurred as a result of unlawful processing or by any breach of data security requirements:
- a) caused to the Player, or a third party, and it shall pay damages (compensation);
  - b) resulting in the violation of personal rights of the Player, in which case the Player may seek restitution from the Controller.

The Controller may be exempted from liability (regarding compensation or restitution) if it proves that the damage or the violation of the Player's personal rights was caused by unavoidable reasons, beyond the scope of data processing. No compensation or restitution shall be paid where the damage or the violation of personal rights was caused by intentional or seriously negligent conduct on the part of the Player (aggrieved party) (Freedom of Information Act Section 24).

## **DATA SECURITY**

92. The Controller ensures the security of data processing according to the provisions of the Information Security Policy and Strategy. It takes the technical and organisational measures necessary to ensure the confidentiality (e.g. unauthorised disclosure, access), integrity (alteration, change, deletion) and availability (accessibility, restorability) of the personal data.

The Controller - among other means - applies the following to satisfy the above criteria:

- ensures - by way of hardware and software tools - that unauthorised persons cannot access the equipment used for the processing data (hereinafter: processing system);
- stores the electronic data in a closed, password-protected IT system;

- ensures the appropriate security guarding of the buildings in which personal data are stored; separate measures are implemented for the storage of sensitive data (e.g. storage in locked cabinets);
- prevents the unauthorised entry of personal data into the processing system, any opportunity for the unauthorised disclosure, change or deletion of the personal data stored therein, as well as the use of the processing systems by unauthorised persons, via communications equipment;
- implements internal policies and instructions to ensure data confidentiality;
- only transfers personal data with the appropriate legal basis;
- only processes personal data for the necessary period;
- ensures the restorability of the processing system in the case of failure, ensures the restorability of the data files and their protection against viruses;
- prepares internal policies for preserving data security;
- ensure the regular review and - if necessary - improvement of the level of IT compliance;
- takes all reasonable measures to prevent personal data breaches.

## **MISCELLANY**

93. Pursuant to Section 29/T of the Gambling Act, in the case of gaming casinos and online casinos operated by the Controller, the Controller may apply a single access control and identification system.
94. The laws of Hungary and the GDPR shall apply to the Information document.
95. To issues not regulated herein, the EULA of the Online Casino and the provisions of the applicable laws of Hungary shall be applied. This Information document shall be interpreted in accordance with the EULA (in effect), as well as the applicable legislative provisions and authority licences.
96. The Controller reserves the right to amend the Information document unilaterally at any time. Reasons for amending the Information document may especially include following up on legislative amendments, and introducing measures ensuring the increased protection of the Player's rights and the security of the Service.
97. The Controller shall inform the Player about the amendments of the Information document, the entry into effect of the restated Information document (with amendments) and the accessibility thereof through system messages. The unabridged text of the Information document in effect is constantly and freely available on the online casino website.

## Information on the right to object pursuant to Article 21 of the GDPR

### Right to object

In each individual case, you have the right to object at any time to the processing of your personal data based on Article 6 (1) point f) of the GDPR (processing based on the balance of interests) - the same applies to profiling as defined in Article 4 (4) of the GDPR. If you exercise your right to object, we will no longer process your personal data unless there are legitimate grounds which override your interests, rights and freedoms or for the establishment, exercise or defence of legal claims.

**Objections should be addressed to:** LVC Diamond Játékkaszinó Üzemeltető Korlátolt Felelősségű Társaság, as the Controller, and you can communicate your objection without any format requirements:

- via e-mail sent to the [ugyfelszolgalat@vegas.hu](mailto:ugyfelszolgalat@vegas.hu) e-mail address;
- via postal mail sent to the registered office of the Controller;
- via the chat window accessible on [www.vegas.hu](http://www.vegas.hu).

Budapest, 15/05/2025