# F&H PLAY

**DATA PROCESSING POLICY AND INFORMATION**

valid from

17.04.2023

TABLE OF CONTENTS



Please note that this is a translation of the table of contents. If you need a translation of specific sections or the entire content, please provide the relevant text, and I'll be happy to assist you further.

1. PREAMBLE, PURPOSE OF THE POLICY

1.1. WISH4TV Limited Liability Company (registered office: 8200 Veszprém, Kossuth utca 6; company registration number: 19-09-523144; tax identification number: 32016145-2-19; hereinafter referred to as the "Company") has established the FH Play online and separate application-based streaming service system (hereinafter referred to as "FH Play") to provide thematic, fishing-hunting media content provided by a separate service provider to its subscribers. The FH Play service can be accessed by subscribers through the application (hereinafter referred to as the "Application") developed by the Company and on the website operated by the Company, www.fhplay.com (hereinafter referred to as the "Website").

1.2. In the course of its activities, the Company may process information that qualifies as "personal data" under Article 4(1) of the EU General Data Protection Regulation (GDPR) concerning its clients, users of the Website and Application, recipients of marketing messages, and other individuals. This data processing policy and information (hereinafter referred to as the "Policy") provides information on the processing of such personal data, as well as the rights and remedies available to individuals regarding data processing. This Policy, unless otherwise defined, interprets capitalized terms in accordance with the applicable general terms and conditions (hereinafter referred to as the "GTC") of the Company. The Company, as the data controller, acknowledges the content of this Policy as binding on itself and undertakes to ensure that all data processing activities related to its operations comply with the provisions of this Policy and the applicable Hungarian and European Union laws.

1.3. The Application and the Website are owned by the Company or operated indirectly by the Company.

1.4. The purpose of this Policy is to ensure that:

(a) the processing of personal data and potentially sensitive data necessary for using the FH Play services, as well as the services provided through the Application and the Website,

(b) the promotion of the Application and the Website, and

(c) other activities of the Company,

are carried out in compliance with the relevant Hungarian and European Union data protection laws. It also aims to ensure that, before starting any data processing, the Company provides clear and detailed information regarding all aspects of the data processing, including but not limited to the purpose and legal basis of the processing, the individuals authorized to process and access the data, the duration of the data processing, and the rights and remedies available to the data subjects.

1.5. Furthermore, the purpose of this Policy is to ensure that in all areas of services provided by the Company, for all individuals, regardless of gender, nationality, or place of residence, their rights and fundamental freedoms, particularly the right to privacy, are respected during the automated processing of their personal data (data protection). The Company handles recorded personal data confidentially, in compliance with data protection laws, and

1.6. During the processing of personal data, the Company is obliged to adhere to the following principles defined in the applicable legislation (Article 5(1) of the GDPR):

(a) lawfulness, fairness, and transparency;

(b) purpose limitation;

(c) data minimization;

(d) accuracy;

(e) storage limitation;

(f) integrity and confidentiality;

(g) accountability.

1.7. The following relevant laws are applicable to data processing, which may change from time to time. In case of changes in the legislation, the relevant part of the policy should consider the required modifications imposed by the applicable law, and the Data Controller will take the necessary measures to amend the policy as soon as possible.

• Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 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).

• Act V of 2013 on the Civil Code ("Civil Code"),

• Act I of 2012 on the Labour Code ("Labour Code"),

• Act CXII of 2011 on Informational Self-Determination and Freedom of Information ("Infotv."),

• Act CXXXIII of 2005 on the Rules of Personal and Property Protection and Private Investigation ("Szvtv."),

• Act C of 2000 on Accounting,

• Act XX of 1996 on Identification Modes Replacing Personal Identification Mark and the Use of Identifying Codes ("Szaztv."),

• Act CXVII of 1995 on Personal Income Tax,

• Act XCIII of 1993 on Occupational Safety and Health.

1.8. In the development of the provisions of this Policy, the Company has taken into particular consideration the GDPR, Act CXII of 2011 on Informational Self-Determination and Freedom of Information ("Infotv."), Act V of 2013 on the Civil Code ("Civil Code"), as well as the provisions of Act XLVIII of 2008 on the Basic Conditions and Certain Restrictions of Commercial Advertising ("Grtv.").

2. INTERPRETATION AND DEFINITIONS OF THE POLICY

2.1. This Policy shall be interpreted in accordance with the rules of the Hungarian language, while considering the general principles of Hungarian civil law. When interpreting the Policy, terms written in capital letters shall have the meaning defined in the GTC, unless otherwise specified in this Policy.

2.2. In accordance with the provisions of the Act CXII of 2011 on Informational Self-Determination and Freedom of Information ("Infotv.") and the GDPR, unless the context otherwise indicates in this Policy, the meaning of terms used in lowercase in the Policy is as follows:

data processing: any operation or set of operations performed on personal data or data sets, whether automated or non-automated, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination, or otherwise making available, alignment or combination, restriction, erasure, or destruction;

**data processor**: a natural or legal person, public authority, agency, or any other body that processes personal data on behalf of the data controller;

**data controller**: a natural or legal person, public authority, agency, or any other body that determines the purposes and means of the processing of personal data;

**data erasure:** making data unrecognizable in such a way that their restoration is no longer possible;

**data blocking:** identifying data with a special mark for the purpose of permanently or temporarily restricting their processing; instead of erasing the data, the data controller blocks the data if their permanent erasure would violate the legitimate interests of the data subject; the blocked data may only be processed as long as the purpose of data processing exists, which excludes the erasure of personal or special data;

**data transfer:** making data accessible to a specified third party;

**data destruction**: complete physical destruction of the data carrier containing the data;

**data protection incident**: a breach of security resulting in the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored, or otherwise processed.

r**ename/alias**: the processing of personal data in such a way that it can no longer be attributed to a specific natural person without the use of additional information, provided that such additional information is kept separately and technical and organizational measures are in place to ensure that the personal data cannot be linked to identified or identifiable natural persons.

**user**: any person who uses the services provided by the Company, uses the Application or the Website, or any specific natural person identified or identifiable - directly or indirectly - based on personal data.

**Supervisory Authority**: the supervisory authority responsible for the protection of personal data and freedom of information, which is the National Data Protection and Freedom of Information Authority (registered office: 1125 Budapest, Szilágyi Erzsébet fasor 22/. mailing address: 1387 Budapest Pf 40.).

**commercial Ad**: any communication, information, or display aimed at promoting the sale or other utilization of a tradable movable property - including money, securities, and financial instruments, as well as natural resources that can be utilized as property - (hereinafter collectively referred to as "product"), service, real estate, or a property right of economic value (hereinafter collectively referred to as "goods"), or aimed at promoting the name, designation, or activities of a business or increasing the recognition of goods or trademarks associated with it.

**Third Party**: any natural or legal person or organization without legal personality who is not the data subject, data controller, or data processor.

**approval/consent**: the voluntary, specific, and informed expression of the data subject's will, based on appropriate information, by which the data subject signifies their agreement to the processing of personal data relating to them, either by a statement or by a clear affirmative action indicating consent.

**special data**: personal data revealing racial or ethnic origin, membership of national minority, political opinion or affiliation, religious or philosophical beliefs, trade union membership, personal data concerning sex life, health data, data relating to pathological addictions, and criminal personal data.

**disclosure**: making data accessible to anyone.

**personal data**: any information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, identification number, location data, online identifier, or factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of the natural person.

**personal identification data**: the data subject's surname and given name(s), maiden name, gender, place and date of birth, mother's maiden name, residence, domicile, or social security identification number (hereinafter collectively referred to as "TAJ number"), or any combination of these or any of these if suitable or capable of identifying the data subject.

**objection/protestation**: the statement by the data subject by which they object to the processing of their personal data and request the termination of the data processing and the erasure of the processed data.

2.3 Unless otherwise specified in the text:

(a) any reference to a legal provision in this Policy includes the potentially modified, expanded, or consolidated form of the relevant legal provision that may have occurred in the meantime;

(b) headings and paragraph numbers in this Policy are solely for reference purposes and should be taken into account only in conjunction with the interpretation of the text of the Policy;

(c) any reference to a person in this Policy includes any individual, company, association, government, state or governmental institution, or authority;

(d) no provision of this Policy shall be construed as excluding liability or remedies for fraudulent or deceitful statements or conduct.

3. DATA CONTROLLER'S DETAILS AND CONTACT INFORMATION

3.1 Data controller's name: WISH4TV Korlátolt Felelősségű Társaság

3.2 Data controller's registered office: 8200 Veszprém, Kossuth utca 6.

3.3 Data controller's postal address: 8200 Veszprém, Kossuth utca 6.

3.4 Data controller's registration number: 19-09-523144

3.5 Data controller's tax identification number: 32016145-2-19

3.6 The data controller's email address is privacy@fhplay.com. The data subject acknowledges that the Company only accepts questions and complaints related to data processing and this Policy at the specified email address.

4. PRINCIPLES OF PERSONAL DATA PROCESSING

4.1 The data controller processes personal data in accordance with the principles of good faith, fairness, transparency, and the provisions of applicable laws and this Policy.

4.2 The Company may process personal data solely for the purposes of data processing defined in this Policy. Based on the consent of the data subject, the data controller may also process personal data for purposes other than those specified in this Policy.

4.3 The data controller processes personal data only for the purposes defined in this Policy and the relevant laws. The scope of processed personal data shall be proportionate to the purpose of data processing and shall not exceed it.

4.4 In cases where the data controller intends to use the personal data for a purpose other than the original purpose of data collection, the data subject shall be informed thereof and the data subject's prior express consent shall be obtained, or the data subject shall be given the opportunity to prohibit such use.

4.5 The data controller does not verify the accuracy of the provided personal data. The person providing the personal data shall be solely responsible for its accuracy.

4.6 Personal data of individuals who have not reached the age of 16 may only be processed with the consent of a parent or legal guardian exercising parental responsibility. The data controller is unable to verify the authorization or the content of the statement of the consenting person. Therefore, the data subject or the parent/legal guardian providing consent guarantees compliance with the relevant legal requirements. In the absence of a consent statement, the data controller shall not process or collect personal data concerning individuals under the age of 16.

4.7 The data controller shall not disclose the personal data it processes to third parties, except for the data processors specified in this Policy and in certain referred cases. An exception to this provision is the use of data in statistically aggregated form that does not contain any data capable of identifying the data subject in any form. Such use does not qualify as data processing or data transfer.

4.8 In certain cases, such as official court or police requests, legal proceedings related to copyright, property rights or other infringements, or a risk to the interests of the data controller or the provision of services by the Company, the data subject's accessible personal data may be made available to third parties.

4.9 The data controller shall inform the data subject and those to whom the personal data has previously been transmitted for the purpose of data processing about the rectification, restriction, or erasure of personal data. This notification can be omitted if it does not infringe upon the legitimate interests of the data subject considering the purpose of data processing.

4.10 The data controller ensures the security of personal data by implementing technical and organizational measures and establishing procedural rules to protect the collected, stored, and processed data, prevent its accidental loss, unlawful destruction, unauthorized access, or unauthorized use.

5.1 The personal data provided during the order of FH Play service (contractual agreement) are as follows:

5.1.1 The legal basis for data processing and the scope of processed data:

The Company obtains and processes the following personal data based on the voluntary consent of the data subjects in accordance with Section 5(1)(a) of the Information Act and Article 6(1)(a) and (b) of the GDPR for the purpose of fulfilling the contract to be concluded with the data subject and taking necessary steps for the preparation of the contract:

(a) Surname and first name;

(b) Address;

(c) Email.

5.1.2 Purpose of data processing:

The above-mentioned personal data is processed by the Company for the following purposes:

(i) Efficient, secure, and personalized services provided by FH Play to subscribers;

(ii) Identification of data subjects, distinguishing them from other data subjects, and communication with the data subjects;

(iii) Fulfillment and execution of the contract related to the FH Play service;

(iv) Assertion of claims in case of contract termination;

(v) Sending system messages related to the services;

(vi) Compliance with legally required data processing and data reporting;

(vii) Statistical data collection, including data collection necessary for market analysis;

(viii) Ensuring payments related to the services provided by the Company;

(ix) Resolution of disputes arising from the use of FH Play;

(x) Providing information from the Company;

(xi) Resolution of operational issues;

(xii) Acquisition of information for research purposes.

Consent can be given by providing the necessary personal data and ticking the appropriate "checkbox."

(vi) sending newsletters and other marketing advertisements; (vii) collecting data for statistical purposes; (viii) storing and processing data for research purposes, based on the voluntary consent of the data subjects, in accordance with Section 5(1)(a) of the Information Act and Article 6(1)(a) of the GDPR, the Company handles the following personal data:

(a) first and last name;

(b) email address;

(c) residential/address for billing;

(d) phone number.

5.3.3 The consent is given by the data subject during the registration process by checking the appropriate "checkbox" provided for giving consent, and by voluntarily providing the requested information.

5.3.4 Data retention period

The processing of personal data provided during the registration process begins with the registration and continues until its deletion. The user may request the deletion of their registration, deletion of their personal data, or modification of their data at any time by emailing (privacy@fhplay.com). After receiving the request, the Company permanently deletes the user's personal data from its system, and recovery of the data becomes impossible. The deadline for data deletion is 5 (five) business days following the receipt of the deletion request. These provisions do not affect the fulfillment of legal retention obligations, as well as the processing of data based on additional consents given during registration on the website or in any other way (e.g., newsletter subscription).

5.3.5 The Company requests that the data subject only register if they have no objections or reservations regarding the aforementioned provisions.

5.4 Data processing related to advertising activities

5.4.1 Pursuant to Section 6(1) of the Advertising Act, direct marketing to a natural person as a recipient of advertising may only be conducted by the Company's direct contact method (particularly through electronic mail or equivalent individual communication tools, excluding postal advertising) if the recipient of the advertising has given clear and explicit prior consent. The Company maintains a register of individuals who have provided the consent declaration, in accordance with the provisions of the relevant laws (Advertising Act, Direct Marketing Act, E-commerce Act, etc.). The data recorded in this register, pertaining to the recipient of the advertising, may only be processed in accordance with the consent declaration, until its withdrawal, and may only be disclosed to third parties with the explicit consent of the data subject or as required by law.

5.4.2 The data subject may authorize the Company and give consent for the Company to inform them about its services for marketing purposes via direct mail or other communication tools (telephone, email, SMS, etc.), and to process their data for this purpose. The data subject is entitled to request from the Company, at any time and without restrictions or justifications, that no direct marketing materials be sent to them and that their data not be used for such purposes.

The relevant consent declaration can be freely withdrawn by the data subject at any time. The data subject can communicate their request in this regard through the contact details specified in the Company's current Policy, as well as through other means indicated in the communications. In such cases, the Company will no longer contact the customer for advertising purposes.

5.5 Data Processing on the Company's Website

5.5.1 The Company's operated website (Honlap) can identify visitors' computers through a system employed by the Company called "cookies." In order to view all content on the website, users need to enable cookies. Accordingly, when certain parts of the website are accessed, cookies may be placed on the user's computer, which are necessary for the functioning of certain features of the website/FH Play. Cookies are small text files stored by the computer and the browser, and the user does not receive any further notifications from the Company regarding their storage. Cookies cannot be used to identify the user personally and only live during the session. By placing cookies, the Company aims to provide visitors with relevant information more effectively. The above information is used by the Company solely for the technical operation of the website, targeted newsletter and marketing purposes, as well as for statistical purposes.

5.5.2 The user acknowledges that by using the website, they expressly consent to the use of cookies for marketing purposes (remarketing) by the Company, which enables the Company to deliver personalized advertisements to website visitors through the internet. The user can disable the use of these cookies in their browser settings on the Google Ad Settings page.

5.5.3 During browsing on the website, technical information may be recorded (e.g., in the form of log files containing the user's IP address, timestamp, and the URL of the visited page). The system continuously logs this data but does not link it to the data provided during registration or usage. Only the Company has access to the data obtained in this way. The above information is used by the Company solely for the technical operation of the website, as well as for statistical purposes.

5.5.4 Automatically and technically recorded data during the operation of the website may be stored in the system for a justifiable duration from their generation to ensure the functioning of the system. The data controller ensures that these automatically recorded data cannot be linked to other personal data, except as required by law. If the user revokes their consent to the processing of personal data or unsubscribes from the service, the technical data will no longer be personally identifiable, except for investigative authorities and their experts.

5.5.5 The Company uses the following categories of cookies on the website:

The following categories of cookies are used on the website:

(a) Essential Cookies:

These cookies are essential for the proper functioning of the Company's services and cannot be disabled from the Company's systems. The system typically sets these cookies when services are requested (e.g., when the data subject sets privacy settings, logs in, accesses content, or performs searches). The browser can be configured to block these cookies or display warnings related to them, but certain parts of the website may not function properly in such cases.

(b) Performance Measurement Cookies:

These cookies allow the Company to measure and improve the performance of the website by analyzing visits and the source of incoming traffic. They help the Company determine the most popular and least popular pages and observe how visitors navigate the website. It is important to note that even if the data subject has set the category to inactive, the Company can still collect and use data with the sole purpose of ensuring uninterrupted service.

(c) Targeting and Advertising Cookies:

These cookies can be set by the Company and/or its advertising partners through the website. They can be used for profiling the data subject's areas of interest to display relevant advertisements to the data subject on this and other websites. They cannot store freely identifiable personal data but operate based on the unique identification of the data subject's browser and internet device. The data subject can enable or disable these cookies at any time.

5.5.6 The Company requests that the data subject only enable the use of cookies and use the website if they have no objections or reservations regarding the above provisions.

5.5.7 By accepting the Policy, the data subject acknowledges that they will not share any content or send any messages through the website that:

(a) violates the honor or dignity of others,

(b) insults others based on their belonging or perceived belonging to a national, ethnic, racial, or religious group,

(c) maliciously or defamatorily disparages any service, economic company, with the intent to discredit or harm its reputation.

The Company promptly deletes such personal data and urges the data subject to comply with the above requirements. If the data subject exhibits behavior that violates the above provisions again after being warned, the Company reserves the right to delete them without further notice.

6. GENERAL PROVISIONS OF DATA PROCESSING

6.1 The Company informs the data subject that no processing of special categories of data takes place.

6.2 It is the data subject's voluntary decision whether to provide the personal data specified in Chapter 5 of the Policy to the Company. However, certain services of the Company cannot be used without recording specific personal data. If the data subject has provided the data of a third party and thereby caused any harm, the Company is entitled to take legal action against the data subject. To claim compensation from the Company, the provided personal data is not verified. The accuracy and truthfulness of the provided data are solely the responsibility of the individual providing them. When providing an email address and mobile phone number, any party involved also assumes responsibility to ensure that only they utilize the service from the provided email address and mobile phone number.

"6.3 The Company may request the recording of other personal data from the data subject, indicating the purpose of the data processing before each data request. The recording of personal data is always voluntary, and its omission does not affect the previous services provided by the Company.

6.4 If the Company processes personal or special data about the data subject based on a legal provision, it shall inform the data subject appropriately, indicating the purpose and duration of the data processing, with reference to the relevant legal provision, before carrying out such data processing. Before requesting any personal data, the Company shall inform the data subject adequately that providing the respective data is voluntary and based on the data subject's consent, or mandatory and based on legal authorization.

6.5 The Company may use the personal data of the data subject for statistical purposes by anonymizing them and depriving them of the possibility of being linked to the data subject. The Company undertakes that after the statistical processing, it will not be possible to re-identify individual data subjects.

6.6 For the purpose of security data verification, the Company may verify the provided personal data, request the data subject's identification document, and make a copy of it to verify the authenticity of the personal data. The data subject may provide the copy of their identification document personally, by scanning and sending it via email or by post, subject to separate data processing consent, to the Company. The personal data collected during security data verification may be temporarily stored in the Company's protected information system. The Company provides separate information to the data subject regarding the purpose and further conditions of data processing carried out through security data verification when requesting the data. The Company may be approached by a court, public prosecutor's office, investigative authority, or administrative authority for the purpose of providing information, disclosing or transferring personal data, or making documents available. The Company, fulfilling the lawful request of authorities – provided that the authority specifies the exact purpose and scope of the data – shall only disclose personal data to the extent necessary to achieve the purpose of the request.

**6.7 In the case of data processing based on consent, the data subject has the right to withdraw their consent at any time, which, however, does not affect the lawfulness of the data processing**

**prior to the withdrawal. Data processing may continue even after the withdrawal of consent if there is another legal basis for the data processing.**

6.8 If a court or authority orders the erasure of personal data with legal force, the data controller shall carry out the erasure. Instead of erasure, the data controller, with the data subject's information, may restrict the use of personal data if requested by the data subject or if it can be presumed based on the available information that the erasure would prejudice the legitimate interests of the data subject. The data controller shall not erase personal data as long as the purpose of the data processing that excluded the erasure is still valid."

**7. ACCESS TO PROCESSED DATA, DATA PROCESSING, AND DATA TRANSFER**

7.1 Access to processed data

Personal data is primarily accessed by the Company and its internal employees, who are authorized to access the data. The data is not disclosed to third parties, and it is used or can only be used for the purposes defined in the Policy.

7.2 Data processing

7.2.1 The rights and obligations related to the processing of personal data by the data processor are determined by the GDPR and other specific laws, within the framework set by the Company as the data controller. The Company, as the data controller, is responsible for the legality of the instructions provided. The data processor cannot make substantive decisions regarding the data processing and can only handle the personal data according to the instructions of the Company as the data controller. The data processor cannot carry out data processing for its own purposes and is obligated to store and preserve the personal data according to the instructions of the Company as the data controller.

7.2.2 The data controller monitors the work of data processors. During research activities, the Company may engage additional data processors for data processing, analysis, and evaluation. The engagement of additional data processors by data processors is only permitted with the consent of the data controller.

7.2.3 The data controller is authorized and obliged to transmit any personal data available to them and lawfully stored by them to the competent authorities, if they are obligated to do so by law or an enforceable official obligation. The data controller shall not be held responsible for such data transfer and its consequences. The release of personal data to third parties or authorities is only possible based on an official decision or with the prior explicit consent of the data subject, unless otherwise provided by law.

7.2.4 Transferring data to the data processors specified in this Policy can be done without the separate consent of the data subject. The Company engages the following data processors' services: [Specify the data processors' services].

| Dta Processor Name and address | Data Process tasks | List of Personal data |
|---|---|---|

| | | |
|---|---|---|
| | | |
| ECO-KVART Kft.1123 Budapest, Kék Golyó utca 2. a ép. I. em. 2 | könyvelés | családi és utónév;<br>e-mail cím;<br>lakcím/szállítási cím;<br>telefonszám. |
| Screenist Solutions Kft. 7843 Tésenfa, Kossuth Lajos utca 85 | rendszer gazda | családi és utónév;<br>e-mail cím;<br>lakcím/szállítási cím;<br>telefonszám. |
| Microsoft Corporation | cloud szolgáltatás | családi és utónév;<br>e-mail cím;<br>lakcím/szállítási cím;<br>telefonszám. |
| | | |
| | | |

7.3 Data transfer

7.3.1 The data controller is authorized to transfer the personal data designated in the explicit consent of the data subject, to the third party specified in the consent, for the purpose and duration indicated in the consent. The data processing provisions of the third party shall apply to the transferred data.

7.3.2 The data controller maintains a record of data transfers for the purpose of verifying the legality of data transfers and ensuring the information of the data subject.

7.3.3 The Company shall only transfer personal data to a third country (non-EEA country) if the data subject has expressly consented to it or if the conditions prescribed by law for data processing are fulfilled, and if the third country ensures an adequate level of protection for the personal data.

7.3.4 Data transfer to a third party without the explicit consent of the data subject can only occur based on a legal provision.

8. DATA SECURITY

8.1 Principles of implementing data security

8.1.1 The Company shall only process personal data in accordance with the activities specified in this policy and the purpose of data processing.

8.1.2 The Company ensures the security of the data and undertakes to implement all necessary technical and organizational measures to enforce data security laws, data protection, and confidentiality regulations, as well as to establish procedural rules necessary for the enforcement of the aforementioned laws.

8.1.3 The technical and organizational measures to be implemented by the Company aim to:

(a) ensure the continuous confidentiality, integrity, availability, and resilience of the systems and services used for processing personal data,

(b) enable timely restoration of access to and availability of personal data in the event of a physical or technical incident,

(c) apply procedures for regularly testing, assessing, and evaluating the effectiveness of the technical and organizational measures implemented to ensure data processing security.

8.1.4 When determining the appropriate level of security, particular consideration should be given to the risks arising from data processing, including accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or unauthorized access to transmitted, stored, or otherwise processed personal data.

8.1.5 The Company protects the data through appropriate measures against unauthorized access, alteration, transmission, disclosure, deletion, or destruction, as well as against accidental destruction, loss, or unavailability due to changes in the applied technology.

8.1.6 The Company keeps records of the processed data in accordance with applicable laws, ensuring that only those employees and other persons acting within the scope of the Company's interests can access the data when necessary for the performance of their duties and tasks.

8.1.7 During each data processing activity, the Company stores the personal data provided separately, and according to the above provision, only employees and data processors with appropriate access rights can access the segregated data sets.

8.1.8 The managers and employees of the Company do not transfer personal data to third parties and take necessary measures to prevent unauthorized access.

8.1.9 Access to personal data is granted to employees and data processors of the Company who have undertaken to comply with data security rules by signing a confidentiality agreement in relation to the processed personal data categories.

8.1.10 The Company considers the current state of technology and multiple possible measures when determining and implementing security measures for data protection.

In the case of a data management solution, a higher level of protection of personal data is chosen, except if it would represent disproportionate difficulty.

8.2 Protection of the Company's IT records

8.2.1 The Company takes the necessary measures to ensure data security in its IT records as follows:

8.2.2 It provides constant protection against computer viruses for the data files it manages (using real-time antivirus software).

8.2.3 It ensures the physical protection of the hardware components of the IT system, including protection against elemental damage.

8.2.4 It ensures protection against unauthorized access to the IT system, both in terms of software and hardware devices.

8.2.5 It takes all measures necessary for the restoration of data files, performs regular backups, and ensures the separate and secure handling of backup copies.

9. RIGHTS OF THE DATA SUBJECT

9.1 Information and right of access to personal data

9.2 At the time of acquiring personal data, the Controller provides the data subject with the following information:

(a) The identity and contact details of the data controller and, if applicable, the data controller's representative.

(b) Contact details of the data protection officer, if applicable.

(c) The intended purpose of the planned processing of personal data, as well as the legal basis for the data processing.

(d) In the case of data processing based on Article 6(1)(f) of the GDPR (legitimate interests of the data controller or a third party), the legitimate interests pursued by the data controller or the third party.

(e) If applicable, the recipients or categories of recipients of the personal data, including particularly recipients in third countries or international organizations.

(f) If applicable, whether the data controller intends to transfer personal data to a third country or international organization, and the existence or absence of an adequacy decision by the Commission or, in the case of data transfers referred to in Articles 46, 47, or 49(1) second subparagraph of the GDPR, the indication of suitable safeguards and the means to obtain a copy of them or where they have been made available.

9.3 In addition to the information mentioned in the previous paragraph, at the time of acquiring personal data, the data controller informs the data subject of the following supplementary information, in order to ensure fair and transparent data processing:

(a) The duration of the storage of personal data, or if this is not possible, the criteria for determining that period.

(b) The data subject's right to request access to, rectification, erasure, or restriction of processing of their personal data, and the right to object to such processing, as well as the right to data portability.

(c) The right to withdraw consent at any time in cases where the processing is based on consent, without affecting the lawfulness of processing based on consent before its withdrawal.

(d) The right to lodge a complaint with a supervisory authority.

(e) Whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and the possible consequences of failure to provide such data.

9.3.2 The data subject has the right to obtain from the data controller confirmation as to whether or not personal data concerning them is being processed, and if so, access to the personal data and the following information:

(a) The purposes of the data processing.

(b) The categories of personal data concerned.

(c) The recipients or categories of recipients to whom the personal data have been or will be disclosed, including recipients in third countries or international organizations.

(d) If applicable, the envisaged duration of the storage of personal data or, if not possible, the criteria used to determine that period.

(e) The

data subject's right to request rectification, erasure, or restriction of processing of their personal data, and to object to such processing.

(f) The right to lodge a complaint with a supervisory authority.

(g) Where the personal data were not collected from the data subject, any available information as to their source.

(h) The existence of automated decision-making, including profiling, and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

9.3.3 If personal data is transferred to a third country or international organization, the data subject has the right to be informed about the appropriate safeguards pursuant to Article 46 of the GDPR.

9.3.4 The data controller shall provide a copy of the personal data undergoing processing to the data subject upon request. The data controller may charge a reasonable fee based on administrative costs for any further copies requested by the data subject. If the request is submitted electronically, the information shall be provided in a widely used electronic format, unless otherwise requested by the data subject.

9.3.5 The right mentioned in point 9.3.3 shall not adversely affect the rights and freedoms of others.

9.4 Right to rectification

9.4.1 The data subject has the right to request the data controller to rectify any inaccurate personal data concerning them without undue delay. Taking into account the purposes of the processing, the data subject is entitled to request the completion of incomplete personal data, including by means of providing a supplementary statement.

9.5 Right to erasure ("right to be forgotten")

9.5.1 The data subject has the right to request the data controller to erase personal data concerning them without undue delay, and the data controller is obliged to erase such personal data without undue delay if one of the following grounds applies:

(a) The personal data is no longer necessary for 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 the processing, and there are no overriding legitimate grounds for the processing or the data subject objects to the processing.

(d) The personal data has been unlawfully processed.

(e) The personal data must be erased for compliance with a legal obligation in Union or Member State law to which the data controller is subject.

(f) The personal data has been collected in relation to the offer of information society services.

9.5.2 If the data controller has made the personal data public and is obligated to erase it according to the above, taking into account available technology and the cost of implementation, the data controller shall take reasonable steps, including technical measures, to inform other data controllers processing the personal data that the data subject has requested the erasure of any links to, or copy or replication of, such personal data.

9.5.3 The right to erasure shall not apply to the extent that processing is necessary:

(i) for exercising the right of freedom of expression and information;

(ii) for compliance with a legal obligation which requires processing by Union or Member State law to which the data 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 data controller;

(iii) for reasons of public interest in the area of public health;

(iv) for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes, insofar as the right to erasure is likely to render impossible or seriously impair the achievement of the objectives of that processing; or

(v) for the establishment, exercise, or defense of legal claims.

9.5.4 The data controller shall inform the data subject of the refusal to erase personal data and provide the reasons for the refusal. Once the request for erasure has been fulfilled, the deleted data cannot be restored.

9.5.5 Newsletters sent by the data controller can be unsubscribed through the unsubscribe link provided. Upon unsubscribing, the data controller will delete the personal data of the data subject from the newsletter database.

9.6 Right to restriction of processing

9.6.1 The data subject has the right to request the data controller to restrict the processing of personal data if one of the following applies:

(a) The data subject contests the accuracy of the personal data, in which case the restriction shall be applied for a period enabling the data controller to verify the

accuracy of the personal data.

(b) The processing is unlawful, and the data subject opposes the erasure of the personal data and requests the restriction of its use instead.

(c) The data controller no longer needs the personal data for the purposes of the processing, but the data subject requires them for the establishment, exercise, or defense of legal claims.

(d) The data subject has objected to the processing, pending verification whether the legitimate grounds of the data controller override those of the data subject.

9.6.2 Where processing has been restricted under point 9.6.1, such personal data shall, with the exception of storage, only be processed with the data subject's consent or for the establishment, exercise, or defense of legal claims, or for the protection of the rights of another natural or legal person, or for reasons of important public interest of the Union or of a Member State.

9.6.3 The data controller shall inform the data subject in advance of the lifting of the restriction on processing imposed under point 9.6.1.

9.7 Right to data portability

9.7.1 The data subject has the right to receive the personal data concerning them, which they have provided to the data controller, in a structured, commonly used, and machine-readable format and has the right to transmit those data to another data controller, where the processing is based on consent or on a contract, and the processing is carried out by automated means.

9.8 The right to object

9.8.1 The data subject has the right to object at any time, for reasons related to their particular situation, to the processing of personal data based on Article 6(1)(e) or (f) of the GDPR, including profiling based on those provisions. In this case, the controller shall no longer process the personal data unless they demonstrate compelling legitimate grounds for the processing which override the interests, rights, and freedoms of the data subject or for the establishment, exercise, or defense of legal claims.

9.8.2 Where personal data are processed for direct marketing purposes, the data subject has the right to object at any time to the processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing.

9.8.3 Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.

9.8.4 The right referred to in points 9.8.1 and 9.8.2 shall be explicitly brought to the attention of the data subject and presented clearly and separately from any other information at the latest at the time of the first communication with the data subject.

9.8.5 In the context of the use of information society services and notwithstanding Directive 2002/58/EC, the data subject may exercise his or her right to object by automated means using technical specifications.

9.8.6 Where personal data are processed for scientific or historical research purposes or statistical purposes, the data subject shall have the right to object, on grounds relating to his or her particular situation, to the processing of personal data concerning him or her, unless the processing is necessary for the performance of a task carried out for reasons of public interest.

9.9 Obligation to notify in relation to rectification or erasure of personal data or restriction of processing

9.9.1 The controller shall communicate any rectification or erasure of personal data or restriction of processing to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. The controller shall inform the data subject about those recipients if the data subject requests it.

9.10 The data subject may exercise the aforementioned rights through the following contact details:

Name: WISH4TV Limited Liability Company

Email: privacy@fhplay.com

Address: 6 Kossuth Street, 8200 Veszprém, Hungary

10. DATA SUBJECT'S OBLIGATIONS

10.1 The data subject is obligated to provide accurate personal data and, if any data changes, to correct the personal data or request the correction from the Company.

10.2 The Company reserves the right to delete any data subject, without further notice, who abuses the personal data of any other person.

11. REGISTER OF DATA PROCESSING ACTIVITIES

11.1. The Company and its representative shall maintain an electronic register of data processing activities carried out under their responsibility, with the following content.

11.2. The register shall contain the following information:

(a) The name and contact details of the data controller, and, if applicable, the name and contact details of the joint controller, the representative of the data controller, and the data protection officer;

(b) The purposes of the data processing;

(c) Description of the categories of data subjects and the categories of personal data involved;

(d) Categories of recipients to whom the personal data have been or will be disclosed, including recipients in third countries or international organizations;

(e) Where applicable, information regarding the transfer of personal data to a third country or an international organization, including the identification of the third country or international organization and a description of the appropriate safeguards pursuant to Article 49(1) second subparagraph of the GDPR;

(f) Where possible, the envisaged time limits for erasure of the different categories of data;

(g) Where possible, a general description of the technical and organizational security measures referred to in Article 32(1) of the GDPR.

11.3. Upon request, the Company and its representative shall make the register available to the supervisory authority.

## 12. DATA BREACH

12.1. The data controller shall notify the competent National Data Protection and Freedom of Information Authority without undue delay, and where feasible, not later than 72 hours after becoming aware of a data breach, unless the data breach is unlikely to result in a risk to the rights and freedoms of natural persons. If the notification is not made within 72 hours, it shall be accompanied by reasons for the delay.

12.2. The notification referred to in point 12.1 shall at least:

(a) Describe the nature of the data breach, including, where possible, the categories and approximate number of data subjects concerned, and the categories and approximate number of personal data records concerned;

(b) Communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;

(c) Describe the likely consequences of the data breach;

(d) Describe the measures taken or proposed to be taken by the data controller to address the data breach, including, where appropriate, measures to mitigate any possible adverse effects.

12.3. If it is not possible to provide all information at the same time, the information may be provided in phases without undue delay.

12.4. The data controller shall maintain a record of data breaches, including the facts relating to the personal data breach, its effects, and the remedial actions taken.

12.5. If the data breach is likely to result in a high risk to the rights and freedoms of natural persons, the data controller shall inform the data subject without undue delay.

12.6. The notification to the data subject referred to in point 12.5 shall be clear and easily understandable and shall include at least the information specified in points 12.2(b), 12.2(c), and 12.2(d).

12.7. The data subject shall not be informed if any of the following conditions are met:

(a) The data controller has implemented appropriate technical and organizational protection measures and those measures have been applied to the personal data affected by the data breach, in particular measures to render the personal data unintelligible to any unauthorized persons, such as encryption;

(b) The data controller has subsequently taken measures to ensure that the high risk to the rights and freedoms of data subjects referred to in point 12.5 is no longer likely to materialize;

(c) It would involve disproportionate effort to inform the data subject. In such a case, public communication or a similar

measure that ensures effective information to the data subjects shall be used.

12.8. Where the data controller has not already notified the data subject of the data breach, the supervisory authority, having considered whether the data breach is likely to result in a high risk, may require the data subject to be informed or may find that any of the conditions referred to in point 12.7 are met.

## 13. REMEDIES

13.1. If the data subject considers that the Company's data processing has infringed the Regulations or applicable legal provisions, the data subject shall have the right to lodge a complaint with the supervisory authority pursuant to Article 77 of the GDPR in order to terminate the alleged unlawful data processing.

13.2. The data subject may exercise their right to lodge a complaint at the following contact details:

National Data Protection and Freedom of Information Authority

Address: 1125 Budapest, Szilágyi Erzsébet fasor 22/c.

Phone: +36 (1) 391-1400;

Fax: +36 (1) 391-1410;

Website: http://www.naih.hu;

Email: ugyfelszolgalat@naih.hu

13.3. The supervisory authority to which the complaint has been submitted shall inform the data subject about the procedural developments and the outcome of the complaint, including the right of the data subject to seek judicial remedy under Article 78 of the GDPR.

13.4. In case of a breach of the rights set out in Section 9 of the Policy, the data subject may bring a lawsuit against the Company. The court shall proceed with the case in an expedited manner. The competent court shall be determined based on the data subject's place of residence or the Company's registered office, as decided by the data subject.

## 14. CONFIDENTIALITY OBLIGATION

14.1. Anyone who gains access to business secrets shall not use it to gain a direct or indirect advantage for themselves or another person, nor to cause harm to the Company.

14.2. Business secret refers to any fact, information, data, or compilation thereof related to the Company's activities that is not easily accessible to the public or persons engaged in economic activities, and the unauthorized acquisition, use, disclosure, or publication of which would harm or jeopardize the legitimate financial, economic, or market interests of the Company, provided that the Company is not at fault for maintaining the secrecy.

14.3. The same protection as business secrets shall apply to technical, economic, or organizational knowledge, experience, or compilations thereof (protected knowledge) that are recorded in an identifiable manner and represent economic value, if acquired, used, disclosed to others, or made public in a manner that violates the principles of good faith and fair dealing. This protection shall not apply to those who have gained access to protected knowledge:

(a) through independent development unrelated to the Company, or

(b) through examination and analysis of a lawfully obtained product or service that essentially replaces the protected knowledge.

14.4. Members, employees, including persons employed based on a mandate, organizations, and their employees associated with the Company, shall be obliged to maintain confidentiality regarding business secrets learned in connection with the Company's operations, without temporal limitations, even after the termination of their relationship (status). The obligation of confidentiality extends to the person or organization who has gained access to information qualifying as a business secret.

14.5. Prior to accessing the data, information, or documents, every natural person entering into a direct or indirect employment relationship with the Company shall be required to sign an appropriate confidentiality declaration.

14.6. The obligation of confidentiality shall be communicated regarding data processing, data protection, information security, and authorization management.

14.7. A person in an employment relationship with the Company, which aims to provide services, shall be obligated, in consultation with their immediate superior as necessary, to consider which data their obligation of confidentiality extends to, especially when communicating with third parties, but also in the daily communication between organizational units within the Company.

14.8. The obligation of confidentiality applies to all data not constituting part of the relevant employee's or third party's administrative or data reporting activities.

15. AMENDMENT, INTERPRETATION, AND EFFECTIVENESS OF THE POLICY

15.1. The Company reserves the right to unilaterally amend this Policy, with prior notification to the data subjects via email.

15.2. The Company declares that all amendments to the Policy will comply with the applicable data protection provisions in force at the time of the amendment.

15.3. The Company declares that the Policy shall be interpreted in accordance with Hungarian laws in force at the time of interpretation. In the event of any discrepancy between the Policy and the applicable laws, the latter shall prevail.

15.4. Matters not regulated by this Policy shall be governed by Hungarian law and the provisions of Hungarian legislation.

15.5. This Policy shall enter into effect on 20th of April, 2023