P r i v a c y P o l i c y

Effective as of: 31 January 2021 until withdrawal

I. Data controller and the subject matter of the present Privacy Policy:

NEXT1 Szolgáltató Korlátolt Felelősségű Társaság

Registered seat:	H-1149 Budapest, Nagy Lajos király útja 214. 7. em. 1.
Company registration number:	Cg.01-09-303166
EUID:	HUOCCSZ.06-09-021287
Tax number:	24937599-2-42
Statistical number:	24937599-7311-113-01.
EU VAT number	HU24937599.
Website:	www.beatalent.app
Email address:	hello@beatalent.app
Represented by:	Bácsfalvi, Tamás managing director, individually

as data controller (hereinafter: "**Data Controller**") adapts the present privacy policy (hereinafter "**Privacy Policy**") with the following material, temporal and personal scope – scope of application –:

The present Privacy Policy applies to all data processing activities related to the use of "*Be a Talent*" mobile application operated by the Data Controller	
Material scope: ***–organisational, economic, social and other conditions of the Data Controller covered by the present Privacy Policy–***	
Name	**Name**
Business activities related to contracts in the scope of the main and secondary activities of the Data Controller	
Registration of the Data Controller, maintenance of client databases	
Preparation, accounting and auditing electronic and paper-based invoicing	
Accounting obligations related to contracts in the scope of the main and secondary activities of the Data Controller	
Registration of receivables related to contracts in the scope of the main and secondary activities of the Data Controller	
Personal scope	
Data subjects (whose personal data is processed by the Data Controller pursuant to the present Privacy Policy): *– natural person identified or directly or indirectly identifiable on the basis of any given personal data–*	All players, supporters, voters and other users of the Data Controller's „Be a Talent" mobile application and services. Data Subjects are the natural persons indicated in individual contracts and natura persons concerned by the Data Controller's data processing activities related to the performance of the contracts – including also, beyond clients, third persons, transaction witnesses, other data subjects –
	All natural persons whose personal data is processed by the Data Controller on the basis of the present Privacy Policy and all further data protection provisions covered by it.
Data Controller and persons under its control:	Members, employees of the Data Controller, or any person who has been involved in any activity of the Data Controller covered by the present Privacy Policy
Data processor(s)	See the Chapter on such special subject matter in the present Privacy Policy

II. Special provisions

1. The present Privacy Policy shall apply to all other internal policies, standard form contract terms and conditions and full business practice of the Data Controller. If any of the said policies of the Data Controller includes any provision violating this Privacy Policy, the provision of the Privacy Policy shall prevail.

III. Purpose of this Privacy Policy

1. The purpose of this Privacy Policy is to ensure that the Data Controller's data processing respects the natural persons' privacy; to determine the scope of the Data Subjects' data processed by the Data Controller, the manner, purpose and legal basis of processing, ensure the application of the constitutional principles of data

protection and the conditions of data security, hinder any unauthorized access to the Data Subjects' data, and the modification, unauthorized disclose or use of data.

2. Moreover, to provide full, prior information to the Data Subjects in relation to the processing activities of the Data Controller processing their data.

IV. Data protection laws

1. Laws of particular relevance are particularly, but not exclusively, the following:

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) (hereinafter: "GDPR")
Fundamental law of Hungary
Act CXII of 2011 on informational self-determination and freedom of information (hereinafter: "Privacy Act")
Act V of 2013 on the Civil Code (hereinafter: „Civil Code")
Act LIV of 2008 on the protection of business secrets
Act XC of 2017 on criminal proceedings
Act CXXX of 2016 on the Code of Civil Procedure ("Code of Civil Procedure")
Act CL of 2017 on the rules of taxation (hereinafter: "Tax Act")
Act C of 2000. on accounting (hereinafter: "Accounting Act")
Act LIII of 2017 on the prevention and combating of money laundering and terrorist financing (as regards client identification, reporting and registering provided by the act, hereinafter: „Money Laundering Act.")
Act LXVI of 1995 on public documents, public records and the protection of private archives (hereinafter: "Archive Act")
Act XLVIII of 2008 on the basic requirements and certain restrictions of commercial advertising activities
The relevant laws are available here: http://net.jogtar.hu/

V. Definitions:

1. Data subject: any natural person identified or directly or indirectly identifiable on the basis of any given personal data;
2. Consent: any freely given, specific, informed indication of the Data Subjects' wishes, by which he or she signifies clear agreement to the processing, fully or covering certain processing activities only, of the personal data related to him or her;
3. Personal data: any Data relatable to the Data Subject – particularly his or her name, identity number, and any information on one or more of his or her physical, physiological, mental, economic, cultural or social identity, and any conclusion that can be drawn therefrom as regards the data subject;
4. Data Controller: the natural or legal person, or a body lacking the status of a legal person who, individually or jointly with others, determines the purpose of the data processing, makes the decisions as regards data processing (including the means applied), and implements such decisions or has them implemented by the data processor;
5. Data processing: any operation or operations carried out on the data, regardless of the process applied, particularly collecting, recording, organising, storing, modifying, using, retrieving, transferring, disclosing, harmonising or connecting, locking, erasing and destroying data, as well as hindering any further use of the data, making photographs, sound or video recordings of the data, and recording the physical features appropriate for identification of a person (e.g. fingerprints or palm print, DNA sample, iris image);
6. Data Transfer: making the data available to a determined third person, particularly the data processor or co-controller in line with the separate agreements concluded regarding the data processor's activity and mandate given in such regard;
7. Activities of the data processor: data processing operations, carrying out technical tasks, regardless of the method and means applied for the operations and place of application.
8. Disclosure: making the data available to anyone
9. Erasure of data: making the data unrecognisable so that the recovery thereof is no longer possible;
10. Automatic processing: the following operations provided that they are carried out by automated means fully or partially: data storage, logical or arithmetic operations carried out with data, modification, erasure, retrieval and distribution of data.
11. Document of lasting value: any document significant from an economic, social, legal, home defence, national security, scientific, cultural, technical or any other aspect, necessary for studying, learning, understanding

historical past, for carrying out public tasks in an uninterrupted manner or enforcing civil rights, which includes data that cannot be learned or cannot be fully learned from any other sources.

12. Otherwise, the terms used in the present Privacy Policy shall be construed in line with the relevant Standard Terms and Conditions of the Data Controller – if applicable –, and in accordance with the definitions included in section 3 of the Privacy Act and Article 4 of the GDPR, noting that in the case of any derogation, the definitions of the GDPR shall prevail.

VI. Data processing based on consent and mandatory data processing

1. The Data Controller caries out data processing activities only in the following cases:
   - based on the Data Subject's consent; or
   - the processing is necessary for the performance of a contract or if it is prescribed by an act or local government decree – on the basis of authorization provided by ab act, in the scope determine therein (hereinafter: mandatory data processing);
     or
   - it is justified by the Data Controller's legitimate interest, in compliance with the principles of proportionality and necessity.
2. In accordance with the aforesaid, the Data Controller processes the Data Subjects' data, as included in the present Privacy Policy, primarily in relation to the conclusion of a contract by and between the parties and/or to the performance of such contract, on the basis of free, informed and express consent of the Data Subject, and with reference to a mandate and in proportion thereto, secondarily, in order to fulfil legal obligations and pursue legitimate interests of the Data Controller and third persons – *provided that it is absolutely necessary, and that pursuing such interest is proportionate to the protection of personal data* – , in line with the relevant provisions of the GDPR, as detailed below.
3. The Data Controller emphasises separately to the Data Subjects that the consent to voluntary data processing may be withdrawn freely at any time, yet data processing may nonetheless be continued if it has any further legal basis and the processing of the concerned data is absolutely necessary for achieving the intended purpose.

VII. Purposes and legal basis of data processing, the scope of personal data and further significant information

1. The Data Controller represents that it only processes personal data in order to exercise rights or fulfil obligations. The Data Controller does not use any personal data for private purposes, its processing activities comply at all times with the principle of purpose limitation – if the purpose if the data processing no longer exists or the processing of the given data is otherwise unlawful, the data shall be erased.
2. The Data Controller may process the Data Subjects' personal data for the following purposes, in the following scope and proportion:

Purpose of data processing:	**Electronic *conclusion of contract*, use of service, provision of service, sending push messages in the application in such regard to the user *(e.g. STC, Privacy Policy has been amended)*, invoicing and contact**
Processes, operations:	***See the provisions of: Player STC (Link: ……) and Sponsor STC (Link: ……), and Contest Rules (Link: ……)***
Expected time of data processing:	In the case of data processed on the basis of *electronic conclusion of contract, use of service, provision of service* ***and push messages related thereto***, the processed data are stored in our active data base for **7 days** after the deletion of the user account upon request. Freely provided data, contents, so-called Challenge videos shall be stored until the deletion of registration. Such data are available to the data subject and the data controller only. The uploaded contents may be deleted separately, there are no duplicates, thus, the recovery thereof is not possible. *Contact data* shall be stored for **30 days** of the deletion of the user account upon request
Personal data - scope, types categories -	*First name, surname, date of births, sex (optional), email address (contact), password (stored in anonymously after identification), address, image and sound recording of the Data Subject, mobile phone number (contact), social media accounts, android or iOS user account, bank card/credit card data: bank card number,* ***data that can be provided optionally: further data uploaded to the application by the user voluntarily***
Place of data	Logically separated on the Data Controller's server

processing:	
Legal basis for the processing:	Performance of a contract in line with Point b) of Article 6(1) of the GDPR Furthermore, data processing pursuant to paragraphs (1)-(9) of section 13/A of Act CVIII of 2001 on electronic commerce and information society services.

Purpose of data processing:	**Complaint management**
Processes, operations:	We hereby inform you that certain data concerning complaints shall be processed also on the grounds of law. Complaints may be received by the Data Controller's customer service via email or phone. The Data Controller has a multi-level complaint management system. If we receive a complaint via phone, the User, by calling the customer service regarding any issue (lodging a complaint, requesting information, etc.), voluntarily consents to the recording of the phone call conducted with the customer service by the Service Provider, after providing the User with complete information. Prior to the conversation, the Service Provider informs the User or other data subject initiating the call about the fact that his or her phone call will be recorded. By providing this short information block, the Service Provider offers the User an opportunity to give consent to the recording or to reject it. If the User does not wish his or her call to be recorded, he or she may terminate the phone call and contact the Service Provider in writing. All further provisions on complaint management are included in the standard terms and conditions and privacy policy of using the service (hereinafter: STC), under the heading complaint management, customer service.
Expected time of data processing:	**5 years** of lodging the complaint. Pursuant to paragraph (7) of section 17/A in Act CLV of 1997 on customer protection, the minutes taken of the complaint and a copy of the response given thereto shall be retained for five years, and shall be presented to the authorities upon request.
Personal data - scope, types categories -	User ID, first name, surname, address, invoicing address email address, mobile phone number, platform of service: Android, IOS, web**, the content of the minutes taken of the complaint pursuant** to paragraph (5) of section **17/A in the Customer Protection Act.**
Place of data processing:	Logically separated on the Data Controller's server
Legal basis for the processing:	Compliance with a legal obligation in line with Point c) of Article 6(1) of the GDPR Paragraphs (4)-(5) of section 17/A of Act CLV of 1997 on consumer protection (hereinafter: Consumer Protection Act)

Purpose of data processing:	**Direct marketing**
Processes, operations:	Newsletters, commercials, advertising materials, direct marketing or other marketing content sent directly to the User if he or she gave express consent thereto upon registration.
Expected time of data processing:	The data shall be erased **within 15 days** of the withdrawal of the consent
Personal data - scope, types categories -	First name, surname, date of birth, sex, address, email address, mobile phone number
Place of data processing:	Logically separated on the Data Controller's server
Legal basis for the processing:	The Data Subject's consent in line with Point a) of Article 6(1) of the GDPR The consent to the data processing is given voluntarily, which shall include express and clear approval and shall be based on appropriate information.

Purpose of data processing:	**Data processing concerning notifications**

Processes, operations:	Should any dispute arise in relation to the contract, retaining the data indicated in points a)-b) is crucial regarding the issue of provability, whether in a court procedure or otherwise. Having regard to that the rules of civil procedure expressly prescribe the burden of proof [paragraph (2) of section 4 in the Code of Civil Procedure], the possibility of proof does not violate any provision of law, on the contrary, it is expressly required by law.
Expected time of data processing:	If, based on the investigation, the notification is not substantiated or no further measure is required, the data concerning the notification shall be erased **within 60 days of the closure of the investigation**. If any measure is taken as a result of the investigation – including the initiation of a legal procedure against the notifying person or the taking of any disciplinary measure –, the data concerning the notification may be processed in the employer's notification system until no longer than the **final closure of the procedures** initiated on the basis of the notification.
Personal data - scope, types categories -	All personal data determined at the above data processing purposes.
Place of data processing:	It is not logically separated on the servers of the Data Controller.
Legal basis for the processing:	In line with Point f) of Article 6(1) of the GDPR (necessary for pursuing the legitimate interest of the Company). Legitimate interest are the Company's assets, business secrets, intellectual property and business reputation, as well as the prevention and investigation of anomalies hindering a working environment based on mutual respect, free of fear or retaliation, and the accountability of the persons responsible.

Purpose of data processing:	**Compliance with the requests of authorities**
Processes, operations:	It is the legitimate interest of the authority performing a public task or any other authority who sends a request to our company to be able to conduct the procedure before it and investigate the concerned case. On the other hand, it is the legitimate interest of our company to be able to fulfil the request sent by the authority and provide the authority with the necessary data. In the case of the data processing carried out for such purpose, the data shall be processed for a period necessary for pursuing the legitimate interest of the authority performing a public task or any other authority, i.e. until the final closure of the authority's procedure. The Company can provide information regarding the requesting authority, while the requesting authority can provide information regarding the data processing carried out by it.
Expected time of data processing:	Data shall be processed for a period necessary for pursuing the legitimate interest of the authority performing a public task or any other authority, i.e. until the final closure of the authority's procedure. The Company can provide information regarding the requesting authority, while the requesting authority can provide information regarding the data processing carried out by it.
Personal data - scope, types categories -	The data indicated in the authority's request from among the data included in the present Privacy Policy.
Place of data processing:	Logically separated on the Data Controller's server
Legal basis for the processing:	In line with Point f) of Article 6(1) of the GDPR (necessary for pursuing the legitimate interest of the Company and the authority as a third person). legitimate interest: it is the legitimate interest of our company to be able to fulfil the request sent by the authority in due time. It is the legitimate interest of the authority performing a public task or any other authority who sends a request to our company to be able to conduct the procedure before it and investigate the concerned case. The Company shall provide the data subject with the interest assessment test upon request.

VIII. Summary of the legal basis (bases) of data processing

1. Pursuant to points

a) – „*the data subject has given consent to the processing of his or her personal data for one or more specific purposes*" – ,	**Y**/N
b) – „*processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract*" – ,	**Y**/N
c) – „*processing is necessary for compliance with a legal obligation to which the controller is subject*" –	**Y**/N
d) – „*processing is necessary in order to protect the vital interests of the data subject or of another natural person*" –	Y/**N**
e) – „*processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller*" –	Y/**N**
f) – „*processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child*" –	**Y**/N

of Article 6(1) of Chapter II in the GDPR

2. and, in the case of the special categories of data, points

a) – „*the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 of article 9 in chapter II*[1] *may not be lifted by the data subject" – ,*	Y/**N**
b) – *„processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject*" – ,	Y/**N**
c) – *„processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent*" –	Y/**N**
d) – *„processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects" –*	Y/**N**
e) – „*processing relates to personal data which are manifestly made public by the data subject*" –	Y/**N**
f) – *„processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity*" –	Y/**N**
g) – *processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject; –*	Y/**N**
h) – *processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3*[2]*; –*	Y/**N**

[1] (1) Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

[2] „Personal data referred to in paragraph 1 may be processed for the purposes referred to in point (h) of paragraph 2 when those data are processed by or under the responsibility of a professional subject to the obligation of professional secrecy under Union or Member State law or rules established by national competent bodies or by another person also subject to an obligation of secrecy under Union or Member State law or rules established by national competent bodies."

i) – *processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy; –*	Y/**N**
j) – *processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1)*[3] *based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data; –*	Y/**N**

of Article 6(1) of Chapter II in the GDPR, processes personal data lawfully.

IX. Principles of data processing

1. Personal data may only be acquired and processed in a fair and lawful manner.
2. Personal data may only be stored for a determined and lawful purpose, and shall not be used in any other manner.
3. The scope of the processed data shall be proportionate to the purpose of their storage, shall be suitable for the purpose of storage and shall not exceed such purpose.
4. Appropriate safety measures shall be taken to protect personal data stored in automated data bases, i.e. in order to hinder accidental or unlawful destruction, unauthorized access, modification or distribution.

X. Data transfer

1. The Data Controller shall be entitled and obliged to transfer to the competent authorities all data available to it and stored lawfully by it, where such transfer is prescribed by law or a final decision of the authority. The Data Controller shall bear no liability for such data transfer or the consequences thereof.
2. The Data Controller transfers data exclusively to its co-controllers and/or data processors with whom the Data Controller has concluded a separate agreement and who are bound by the provisions of such agreement with regard to the Data Controller; accordingly
3. The Data Controller provides data to third persons exclusively to fulfil the purposes determined in the present Privacy Policy and to the extent necessary thereto. Such transfer shall not put the Data Subject into a less favourable situation than that determined by the provisions on data processing and data protection prescribed in the effective Privacy Policy.
4. The Data Controller shall not transfer the personal data of the Data Subject to third countries or international organisations (i.e. outside Europe, to a non-EEA state), unless if the Data Subject gives express consent thereto, in which case the data transfer shall comply with the terms determined in the written statement of the parties and the proper safeguards determined in the GDPR shall be ensured.
5. The above restriction shall not apply to cases covered by Article 45 of the GDPR, i.e. if the data are transferred to a state and/or international organisation regarding which the European Committee has issued a so-called "adequacy decision", where no separate permission is necessary for the data transfer. At adopting the present document, adequacy decision is in effect regarding the following countries: Andorra, Argentina, Faroe Islands, Guernsey, Israel, Jersey, Canada, Isle of Man, Switzerland, Uruguay, Japan, New Zealand – *in the cases of the USA and South Korea, the procedure for the issuance of an adequacy decision is pending*. The situation of the United Kingdom as regards data protection is currently uncertain, however, no data is transferred thereto by the Data Controller.

XI. Security of data processing

1. Fulfilling the requirements prescribed in Article 32 of the GDPR, and considering such requirements as obligations, the Data Controller takes all measures to ensure the security of the Data Subjects' data, moreover, it shall implement appropriate technical and organisational measures, develop the procedural rules necessary for abiding by the provisions of the GDPR and other laws on data protection and confidentiality.
2. The Data Controller processes data primarily by automated process, secondarily on a paper basis. Where data are processed in an automated manner, any processing operation that require human involvement may only

[3] „Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, shall be subject to appropriate safeguards, in accordance with this Regulation, for the rights and freedoms of the data subject. Those safeguards shall ensure that technical and organisational measures are in place in particular in order to ensure respect for the principle of data minimisation."

occur exceptionally and when justified. The activity of the Data Controller and the processors engaged by it fulfils the requirements concerning organisational security, employees, external personnel and environment, classification and control of devices, communication and operation management, access control, uninterrupted operation control, system development and maintenance.

3. The Data Controller shall protect the data particularly from unauthorised access, modification, transfer, disclosure, erasure and destruction, as well from accidental destruction or corruption.
4. The data recorded in an automated technical manner during the operation of the Data Controller's system(s) shall be stored in the system, as of the generation of such data, for a period justified with regard to the operation of the system(s) of the Data Controller. The Data Controller shall ensure that such automatically recorded data cannot be linked to other personal data – unless provided mandatorily by law. If the Data Subject withdraws his or her consent to data processing or objects to it, then the Data Subject shall not be identifiable from the technical data – not including the request of any investigation authority of their expert.
5. If that occurs, the employees carrying out data processing activities at the organizational units of the Data Controller shall keep the personal data they became aware of as business secrets. For such purpose, the employees who process personal data and have access thereto make a confidentiality statement. Furthermore, the employees of the Data Controller shall ensure, during their work at all times, that no unauthorized access occurs regarding the personal data. Personal data are stored and placed so that no unauthorized person may gain access to, modify or destroy it.
6. The head of the Data Controller with decision-making competence shall keep the characteristics of the Data Controller in mind when determining the organisation of data protection, the functions and powers regarding data protection and the activities related thereto, and when designating the person responsible for the supervision of data processing.
7. The Data Subject or the person acting in his or her behalf shall be liable, in each case, for the authenticity of the data obtained directly from the Data Subject or a person acting in his or her behalf. The Data Controller does not verify the personal data provided to it.

XII. Period of data processing

1. The periods of processing determined at the data processing purposes shall apply, yet
   - In principle, until the purpose of data processing is fulfilled,
   - In the case of data processing related to rights and obligations concerning a legal relationship, until those terminate.
   - Finally, until the withdrawal of the Data Subject's consent and/or the termination, elimination of the circumstances which render it necessary or the purpose to be achieved.
   - Otherwise, the Data Controller shall erase the data upon the Data Subject's request – *unless where such erasure would violate professional secrecy or Point f of Article 6(1) of the GDPR or other legal basis of mandatory data processing* –, except for the data as regards which further processing is necessary due to settlement debate or other legal dispute between the parties – *until such dispute is settled* – and/or a provision of law. In the scope of the latter, not exclusively, the Data Controller shall process
     - the data covered by paragraph (3) of section 78 of the Tax Act for 5 years
     - the data covered by paragraphs (1)-(2) of section 169 of the Accounting Act for 8 years,
     - or for a longer period of time if provided by law.
2. The Data Controller reserves the right to process the relevant data, to the extent necessary, for a period longer than the aforesaid, i.e. for the period available to enforce claims based on rights and obligations arising from the activity due to which the concerned data are processed.
3. The Data Controller warns the Data Subjects that documents covered by point j) of section 3 of Act LXVI of 1995 on public documents, public records and the protection of private archives, which are essential to enforce civil rights, and contain data is not or not fully available in any other document, as well as the information included therein shall be processed until transferred from the Data Controller's processing to the Data Subject or another data controller, or until erased, culled or destroyed. The Data Controller shall process such information for an unlimited period.
4. As regards the aforesaid, the Data Controller accepts resolution No. NAIH/2018/582/J of the Hungarian National Authority for Data Protection and Freedom of Information as governing.

XIII. Possible amendment of the Privacy Policy

1. The Data Controller reserves the rights to unilaterally amend the present Privacy Policy for the future. The new policy will be displayed in „Be a Talent" Application and/or informs the Data Subjects directly without delay.

XIV. Registration of data processing activities

Having regard to that the Data Controller employs fewer than two hundred and fifty employees, it keeps no separate record of the data processing
Pursuant to Recital (13), the GDPR includes a derogation for organisations with fewer than 250 employees with regard to record-keeping; thus, the Data Controller is not obliged to keep a separate record of the data processing.

XV. Information, right to object, erasure of data, restriction of data processing

1. If the Data Controller have not obtained the personal data from the Data Subject, fulfilling its obligation prescribed by Article 14(3) of Chapter III of the GDPR – *unless Article 14(5) applies* –, shall inform the Data Subject by using one of his or her contact data – *if available, possibly via email* –, without delay, but not later than within a period of one month, on the following:
   - 1.1. the identity and the contact details of the controller and, where applicable, of the controller's representative, the contact details of the data protection officer, where applicable;
   - 1.2. the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
   - 1.3. the categories of personal data concerned;
   - 1.4. the recipients or categories of recipients of the personal data, if any;
   - 1.5. where applicable, that the controller intends to transfer personal data to a recipient in a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1) of the GDPR, reference to the appropriate or suitable safeguards and the means to obtain a copy of them or where they have been made available;
   - 1.6. the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
   - 1.7. where the processing is based on point (f) of Article 6(1) of the GDPR, the legitimate interests pursued by the controller or by a third party;
   - 1.8. the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject and to object to processing as well as the right to data portability;
   - 1.9. where processing is based on point (a) of Article 6(1) or point (a) of Article 9(2) of the GDPR, the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
   - 1.10. the right to lodge a complaint with a supervisory authority;
   - 1.11. from which source the personal data originate, and if applicable, whether it came from publicly accessible sources;
   - 1.12. the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) of the GDPR and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.
2. The Data Subject may request information regarding the processing of his or her personal data, may request the rectification or – with the exception of data processing prescribed by law – erasure of such data pursuant to the present Privacy Policy, particularly by using the above contact data.
3. As a response to the Data Subject's request submitted via email, the Data Controller shall provide information on the Data Subject's data processed by it, the purpose, legal basis and period of the processing, the name, address (registered seat) of the data processor and its activities carried out in relation to the processing, as well as on the recipients of the Data Subject's personal data and on the purpose such data transfer. The Data Controller shall, within the shortest possible time but no later than within fifteen (15) days, respond in writing, in plain language and free of charge, and provide the requested information. The Data Controller may charge a fee only in exceptional cases (no fee may be charged if the data subject has not yet lodged a request for information regarding the same field in the current year. Otherwise, costs may be charged on the data subject. The amount of such costs may be determined also in the contract concluded by and between the parties. The costs already paid by the Data Subject shall be repaid if the data have been processed unlawfully or if the request for information led to rectification.)

4. If the provision of information may not be lawfully rejected, the Data Controller shall provide information regarding the Data Subject's data processed by it or by a data processor engaged by the Data Controller, on the source of such data, the purpose and legal basis of the data processing, the name and address of the data processor and its activities carried out in relation to the processing, the circumstances and impacts of the personal data breach and the measures taken to avert it, and- if the Data Subject's data has been transferred – on the legal basis and recipient of the data transfer. Otherwise, the provision of information shall cover the information prescribed in Section 2 Articles 13-14 of the GDPR.
5. The Data Controller shall rectify incorrect personal data. The Data Controller shall erase the personal data if such data have been processed unlawfully, if the erasure was requested by the data subject – in such case no later than within five (5) days –, if he data are incomplete or false – and such incompleteness or falseness cannot be lawfully remedied – provided that the purpose of the data processing no longer exists, the storage period prescribed by law has lapsed, or the erasure of the data was ordered by court or by the Hungarian National Authority for Data Protection and Freedom of Information. The Data Controller shall notify the Data Subject and the those to whom the it has transferred the concerned data of the rectification or erasure. Notification may be dispensed with if that does not harm the legitimate interest of the Data Subject having regard to the purpose of processing.
6. If personal data is used unlawfully or in a deceptive way by the Data Subject, or the use of the personal data qualifies as a criminal act committed by the Data Subject, the Data Controller reserves the right to retain the data used in the said manner, in order to ensure proof in the possibly initiated criminal or other proceedings, until the closure of the proceedings. Mutatis mutandis, the same applies if the Data Subjects request the erasure of data in order to frustrate or at least hinder the enforceability of the Data Controller's legitimate claim.
7. The Data Subject may withdraw his or her voluntary consent at any time, and otherwise he or she may object to the processing of his or her personal data, particularly if
   7.1. if the processing or transfer of the personal data is necessary only for complying with a legal obligation to which the Data Controller is subject to or for the enforcement of the legitimate interest of the Data Controller, the recipient or a third person, unless the processing is mandatory;
   7.2. if the use or transfer of the personal data was caried out for the purpose of direct marketing, survey or scientific research; and
   7.3. in other cases prescribed by law.
8. The Data Subject's objection shall be investigated in the shortest possible time but no later than within fifteen (15) days, and Data Subject shall be informed about the decision rendered on whether or not his or her objection was substantiated. For the duration of the investigation, but for no longer than five (5) days, the Data Controller suspends the data processing. If the objection was substantiated, the head of the organisation unit shall proceed in line with the provisions of the GDPR.
9. If the Data Controller finds that the Data Subject's objection is substantiated, it shall terminate the processing – including any further data collection and transfer –, shall block the concerned data, and notify, of the objection and the measures taken as a result thereof, all of those to whom it has transferred the concerned data earlier and who are obliged to take measures in order to enforce the objection. If the Data Subject does not agree with the Data Controller's decision or of the Data Controller fails to meet the deadline, the Data Subject may initiate a court procedure within thirty (30) days of the communication of the decision or of the last day of the deadline.
10. The Data Controller shall be liable for the damages incurred by any other person due to the unlawful processing of the Data Subject's data or to the violation of technical data protection requirements. The Data Controller shall be relieved from liability it if is able to prove that the damage occurred due to an unavoidable cause that falls beyond the scope of the data processing. No compensation shall be provided for any damage insofar as it originates from an intentional or negligent conduct of the aggrieved party.
11. The provision of information to the data subjects may be dispensed with/rejected or restricted in line with Articles 13(4) and 14(5) of the GDPR – for the reasons and based on the justification provided therein – if
   11.1. the data subject already has the information;
   11.2. he provision of such information proves impossible or would involve a disproportionate effort, in particular for processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the conditions and safeguards referred to in Article 89(1) of the GDPR or in so far as the obligation referred to in Article 14(1) of the GDPR is likely to render impossible or seriously impair the achievement of the objectives of that processing. In such cases the controller shall take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available;
   11.3. obtaining or disclosure is expressly laid down by Union or Member State law to which the controller

is subject and which provides appropriate measures to protect the data subject's legitimate interests; or

11.4. where the personal data must remain confidential subject to an obligation of professional secrecy regulated by Union or Member State law, including a statutory obligation of secrecy.

12. Furthermore, the Data Subject shall be entitled to gain access to his or her personal data and the following information:
    12.1. A copy of the personal data (fees may be charged for further copies.)
    12.2. Purposes of the data processing
    12.3. Data categories
    12.4. Data concerning automated decision-making and profiling
    12.5. At data reception, information concerning the source
    12.6. Recipients to whom the data has been or will be communicated
    12.7. Information, safeguards regarding data transfer to third countries
    12.8. Period and aspects of storage
    12.9. Rights of the Data Subject
    12.10. Right to turn to the authorities
13. Manner of exercising the right to access: Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.
14. The right to obtain a copy shall not adversely affect the rights and freedoms of others.
15. Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.
16. The Data Subject may not exercise his or her right to rectification and right to be forgotten if the data processing is necessary due to any of the following: freedom of expression, compliance with a legal obligation, exercise of official authority, public interest in the field of public health, recording out of public interest, scientific or historical research, pursuing the enforcement of legal claims.
17. The Data Controller restricts the processing at the Data Subjects request where one of the following applies:
    17.1. the accuracy of the personal data is contested by the data subject
    17.2. he processing is unlawful and the data subject opposes the erasure of the personal data
    17.3. the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims
    17.4. the Data Subject has objected to processing and the investigation is pending.

XVI. Notification obligation

1. The Data Controller shall inform all Data Subjects of the rectification, erasure or restriction to whom the data has been communicated, unless that is not possible or requires disproportionate effort.

XVII. Data portability

1. The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller:
    1.1. in a structured, commonly used and machine-readable format
    1.2. shall have the right to transfer it to another controller
    1.3. shall have the right to have the personal data transmitted directly from one controller to another
    1.4. where technically feasible

    unless: processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller

XVIII. Remedies

1. If the rights of the Data Subjects are violated, their rights against the Data Controller may be enforced before the court with competence and jurisdiction based on the relevant laws (in principle, the court with competence based on the Data Subject’s place of residence), or Data Subjects may turn to the Hungarian National Authority for Data Protection and Freedom of Information (postal address: H-1534 Budapest, Pf.: 834; address: H-1125 Budapest, Szilágyi Erzsébet fasor 22/c.) on the basis of the Privacy Act and other relevant laws. The court shall hear the case in priority proceedings.

I hereby accept the present Privacy Policy and put it into effect on the day indicated below.
Place and date: Budapest, 31 January 2021

NEXT1 Szolgáltató Korlátolt Felelősségű Társaság
represented by: Bácsfalvi, Tamás
managing director
Data Controller