Privacy Notice and Terms of Use

on the processing of personal data of
users of the www.humaniahrsgroup.hu website,
companies interested in using the services of Humánia HRS Group Zrt. and
representatives of companies offering services to Humánia HRS Group Zrt.

(hereafter referred to as the "Notice")

Privacy notice

Humánia HRS Group Zrt. (hereinafter referred to as the "**Data Controller**") informs by means of this Privacy Notice all natural persons who

- visit the website of the Data Controller www.humaniahrsgroup.hu (users), or
- like or follow Facebook and other social networking sites, or
- wish to contact the Data Controller on their own behalf or on behalf of an organisation they represent in order to:
  - use or receive information about the services of the Data Controller (client contacts), or
  - offer services or goods to the Data Controller (supplier contact persons),

(hereinafter referred to as Data Subjects) on the processing of their personal data provided by the Data Subjects during the contact, on the identity and data of the Data Controller, on the principles and practices followed in the processing of personal data, on the transfer of data, on the organisational and technical measures taken to protect personal data, and on the ways and means of exercising the rights of Data Subjects.

This Notice applies to the following personal data by Data Subjects:

- sent on www.humanishrsgroup.hu,
- in a message or post on Facebook and other social media sites of the Data Controller,
- sent to the Data Controller by electronic mail or by any other means or application capable of transmitting electronic data, and
- provided to the Data Controller's staff by telephone or in person.

Please note that by providing your personal data as listed above after reading this Privacy Notice, you consent to the processing of your personal data in accordance with the provisions of this Privacy Notice by any means or channel!

Identification and contact details of the Data Controller

Data Controller:	**Humánia HRS Group Zrt.**
Headquarters:	1097 Budapest, Albert F. út 3/B.
Registration number:	01-10-047232
Adószáma:	23693375-2-43
Registration number:	NAIH-78844/2014
Webpage:	www.humaniahrsgroup.hu
Customer service phone number:	+36 (1) 248-2010
Customer service e-mail address:	info@humaniahrsgroup.hu

The Data Controller's primary objective and commitment is to protect the personal data provided by natural persons who contact the Data Controller through any channel.

Contact details of the Data Protection Officers

Name	**Henrietta Gyurkóczi and Bálint Farkas**
Phone:	+3612482010
e-mail:	adatvedelem@humaniahrsgroup.hu
Postal address:	1097 Budapest, Albert F. út 3/B.

I. General provisions, information

A. Terminology

The terms used in the Privacy Notice shall be interpreted in accordance with the definitions laid down in Regulation 2016/679 of the European Parliament and of the Council (hereinafter: GDPR) and Act CXII of 2011 on the Right to Informational Self-Determination and Freedom of Information (hereinafter: Info.tv.).

data subject: a natural person identified or identifiable on the basis of any information;

Identifiable natural person: a natural person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the natural person;

personal data: any information relating to the data subject

Consent: a freely given, explicit and properly informed indication of the data subject's wishes by which he or she signifies, by a statement or by other means which unambiguously express his or her wishes, his or her agreement to the processing of personal data relating to him or her.

data controller: a natural or legal person or an unincorporated body which, alone or jointly with others, determines the purposes for which the data are to be processed, takes and implements the decisions concerning the processing (including the means used) or implements them with the processor, within the limits set by law or by a legally binding act of the European Union

'*processing*' means any operation or set of operations which is performed upon data, regardless of the procedure used, such as collection, recording, recording, organisation, storage, alteration, use, retrieval, disclosure, transmission, alignment or combination, blocking, erasure or destruction, prevention of further use, taking of photographs, sound recordings or images and recording of physical characteristics which can be used to identify a person

transfer: making data available to a specified third party

disclosure: making the data available to anyone;

erasure: making data unrecognisable in such a way that it is no longer possible to recover it;

restriction of processing: blocking of stored data by marking it for the purpose of restricting its further processing

processing: the set of processing operations carried out by a processor acting on behalf of or under the instructions of the controller;

data processor: a natural or legal person or an unincorporated body which processes personal data on behalf of or under the authority of the controller, within the limits and under the conditions laid down by law or by a legally binding act of the European Union.

third party: any natural or legal person or unincorporated body other than the data subject, the controller, the processor or the persons who, under the direct authority of the controller or processor, are carrying out operations relating to the processing of personal data

data breach: a breach of data security that results in the accidental or unlawful destruction, loss, alteration, unauthorised disclosure or transmission of, or access to, personal data transmitted, stored or otherwise processed;

profiling: any processing of personal data by automated means intended to evaluate, analyse or predict personal aspects relating to the data subject, in particular his or her performance at work, economic situation, state of health, personal preferences or interests, reliability, behaviour, location or movements;

recipient: the natural or legal person or unincorporated body to whom or which personal data are disclosed by the controller or processor;

pseudonymisation: the processing of personal data in a way which makes it impossible to determine, without further information, to which data subject the personal data relate and which ensures, by technical and organisational measures, that the personal data cannot be linked to an identified or identifiable natural person

B. Principles of data management

The Data Controller has drafted this Policy with the following principles in mind and with a view to ensuring maximum compliance with them, bearing in mind that Humania is responsible for compliance with the following principles and for demonstrating compliance (accountability).

Personal data

1) must be lawful, fair and transparent for the data subject ("lawfulness, fairness and transparency");
2) collected only for specified, explicit and legitimate purposes and not processed in a way incompatible with those purposes ("purpose limitation");
3) be adequate and relevant for the purposes for which the data are processed and limited to what is necessary ("data minimisation");
4) be accurate and, where necessary, kept up to date; all reasonable steps must be taken to ensure that personal data which are inaccurate for the purposes for which they are processed are erased or rectified without undue delay ("accuracy");
5) be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed ("limited storage");
6) be carried out in such a way as to ensure adequate security of personal data, including protection against unauthorised or unlawful processing, accidental loss, destruction or damage ("integrity and confidentiality"), by implementing appropriate technical or organisational measures.

C. Purposes of the processing of the Data Subject's personal data

1) The Data Controller may contact the Data Subject to present the services within the scope of its activities or send him/her a personal or system message (offer) about the services;
2) to prepare the contract for the use of the services provided by the Data Controller and to enable the necessary contacts between the parties in the process of performance of the service in order to exercise the rights and fulfil the obligations of the contract (principal contact);
3) in the process of preparing the contract for the provision of services or the purchase of goods by the Data Controller, and in the process of receiving the service or goods, to enable the parties to communicate with each other as necessary to exercise their rights and obligations under the contract (supplier communication).
4) Following the conclusion of a contract with a client or supplier, the additional purposes of data processing are.
   a) the Data Controller to comply with its legal obligations in relation to the legal relationship, or the legitimacy of the cooperation and settlements of the Parties can be verified by the Data Controller to the competent authorities entitled to do so, and the personal data is an integral part of a document necessary for this purpose;
   b) to ensure the possibility of contact in the processes and procedures relating to possible warranty, guarantee and compensation claims arising from the cooperation with the principal and the supplier after the termination of the contract.
5) The Data Controller regularly collects information on the detailed opinion of the customer's contacts about the service and performance of the Data Controller (satisfaction measurement). The Data Controller may also need the personal data of the contacts for the purpose of this measurement.

D. Legal basis for processing personal data

1) For the purposes of Chapter *C,* points 1) and 5), the legal basis for processing is the data subject's consent [Article 6(1)(a) GPPR].
2) For the purposes of Chapter *C*, points 2 and 3, the processing is necessary for the establishment or performance of a contract between the principal or supplier and the Controller [Article 6(1)(b) GDPR],
3) For the purposes of Chapter *C.*4(a), processing is necessary for compliance with legal obligations [Article 6(1)(c) GPPR].
4) For the purposes of Chapter *C.*4(b), processing is necessary for the purposes of the legitimate interests pursued by the Controller or a third party [Article 6(1)(f) GDPR].

II. Processing of personal data

A. Scope of personal data processed

The Data Controller processes the following personal data of Data Subjects

1) on the basis of pre-contractual consent:
   a) Name
   b) office telephone number
   c) your office e-mail address
   d) Name of company on whose behalf you are contacting/maintaining contact
   e) the data provided by the Data Subject in the text of communications sent by the Data Subject to the Controller on the basis of the Data Subject's free choice to communicate the data

   Please note that the provision of personal data is a condition for the Data Subject to obtain information about the services of the Data Controller beyond what is available to anyone on the platforms available to them, and for the Data Controller to enter into a contract with them or the organisation they represent. In the absence of the provision of personal data, the Data Controller shall not provide any further information about its services or enter into any contract.

2) after the conclusion of the contract on the basis of law, performance of the contract or the interest of the Data Controller:
   a) Name
   b) office telephone number
   c) your office e-mail address
   d) the name of the organisation on whose behalf the contact is made
   e) location of activity
   f) schedule
   g) the scope of its decision-making powers

3) after the conclusion of the contract, on the basis of consent (for a purpose other than the original purpose of the data collection - satisfaction measurement):
   a) Name
   b) office telephone number
   c) your office e-mail address
   d) the name of the organisation on whose behalf the contact is made

B. Profiling and automated decision-making

The Data Controller does not perform profiling and automated decision-making.

C. Duration of storage of personal data, planned date of deletion

1) From *A.* subsection 1) , if, following an exchange of information during the contact, it becomes clear that a contractual relationship will not be established between the Data Controller and the Data Subject or an organisation represented by the Data Subject, two months after this becomes clear, unless the possibility of concluding a contract at a later date has not been excluded by the parties; in this case, two years after the data were provided or within 25 days of receipt of the Data Subject's request for their deletion.

2) For data processed for the purposes of subsection *A.* 3) in accordance with point 4) or within 25 days of receipt of the Data Subject's request for erasure ;

3) The personal data processed for the purpose of *A.* subsection 2) , which serve to support an accounting document, and other personal data forming an integral part of documents containing such data, shall be processed eight years after the last day of the year in which the data were generated;

4) Any other personal data after three years from the last day of the year in which the contract is terminated; in this respect, the date of termination of the contract is also the date on which the Data Controller becomes aware of the termination of the legal relationship or the right of representation between the Data Subject and the principal or supplier represented by him or her.

D. Persons entitled to process personal data

1) Data processed in relation to the Data Subject may only be accessed and processed by the Data Controller and the employees of the Data Processors specified in the internal rules of the Data Processors included in this Notice, subject to the limitations and confidentiality obligations set out in the internal rules of the Data Processors and the Data Controller.

2) For more information about the persons entitled to access and process your data, please send a request to info@humaniahrsgroup.hu.

E. Other treatment rules

1) The Data Controller is also entitled to use electronic communications generated in the course of data processing in accordance with the purpose of data processing, as set out in this Notice.

2) The Data Controller may move the Data Subject's data between independently operating datasets, provided that the Data Controller processes the Data Subject's data for the purposes set out in this Statement.

3) The Data Subject is solely responsible for the truthfulness and accuracy of the personal data.

4) The Data Controller is not in a position to verify the eligibility of the person giving consent, so the Data Subject warrants that the consent is in accordance with the law.

5) The Data Subject warrants that the consent of the Data Subject has been obtained lawfully for the processing of personal data provided and made available in the course of the Service about third natural persons.

6) Unless otherwise provided by law, the Data Controller may process the personal data collected for the purposes of complying with a legal or contractual obligation to which it is subject or for the purposes of pursuing its own legitimate interests or the legitimate interests of a third party, where such interests are proportionate to the restriction of the right to the protection of personal data, without further specific consent and even after the withdrawal of the Data Subject's consent.

F. Data security

1) The Data Controller shall implement appropriate technical and organisational measures to ensure a level of data security appropriate to the scale of the risk, taking into account the state of science and technology and the cost of implementation, the nature, scope, context and purposes of the processing and the varying degrees of probability and severity of the risk to the rights of natural persons.

2) The Data Controller is constantly developing, in line with the requirements of the times and market expectations, the possibilities for its potential employees, staff and partners to access and manage information about its services and the benefits they offer to users, the possibility to contact them and the processes related to the use of the service in an increasingly online environment. In order to meet this challenge, the Data Controller continuously develops and operates websites, mobile applications, social media platforms and other digital access points where users can voluntarily provide data (external data management systems).

3) The Data Controller strives to achieve the highest possible level of digitisation in both corporate governance and internal operational processes. The nature of the services provided by the Data Controller involves the processing of a large amount of personal data , which is greatly facilitated by digital data management facilities. As a result, the Data Controller uses and develops computer programs and interfaces that process personal data (internal data management systems).

4) The Data Controller shall, when procuring and developing its systems, continuously ensure that the system in question ensures.
   a) deny access to the system by unauthorised persons,
   b) prevent the unauthorised reading, copying, modification or removal of data media,
   c) preventing the unauthorised input of personal data into the processing system and the unauthorised access, modification or deletion of personal data stored in the processing system,
   d) preventing the use of data processing systems by unauthorised persons through data transmission equipment,
   e) that persons authorised to use the system have access only to the personal data specified in the access authorisation,
   f) to be able to verify and establish to which recipients the personal data have been or may be transmitted or made available by means of a data transmission installation,
   g) to be able to verify and establish a posteriori which personal data were entered into the system by whom, at what time,
   h) prevent the unauthorised disclosure, copying, modification or deletion of personal data during their transmission,
   i) to ensure that the data management system can be restored in the event of a malfunction; and
   j) that the data management system is operational, that any errors in its operation are reported and that the personal data stored cannot be altered by the system's malfunction.

5) The information technology systems and networks of the Data Controller and the data processors involved in the processing are protected against computer fraud, espionage, sabotage, vandalism, fire and flood, computer viruses and computer intrusions. The Data Controller and the data processors involved in data processing ensure security through server-level and application-level protection procedures.

6) Additional measures necessary for data security, which also define the responsible staff members, are set out in the Data Controller's Privacy Policy.

7) We inform the data subjects that electronic messages transmitted over the Internet, regardless of the protocol (e-mail, web, ftp, etc.), are vulnerable to network threats that could lead to fraudulent activity, contract disputes, or the disclosure or modification of information. The Data Controller shall take all reasonable precautions to counter such threats.

8) In accordance with the instructions of the Controller or the Data Controller, the Processor shall monitor the IT systems used in order to record any security discrepancies and provide evidence of any security incidents. The monitoring of systems shall also allow the effectiveness of the precautions taken to be checked.

9) The Data Controller shall keep a record of any data breaches, indicating the facts relating to the data breach, its effects and the measures taken to remedy it.

10) The Data Controller shall notify the National Authority for Data Protection and Freedom of Information of any potential data breach without delay and, if possible, no later than 72 hours after the data breach has come to its attention, unless the data breach is unlikely to pose a risk to the rights of natural persons .

G. Specific rules for the processing of personal data that may be provided on the www.humaniahrsgroup.hu website

1) The Data Controller shall store the date of completion of the contact form and the version of the Information Document in force at the time of completion in an identifiable and traceable manner.

2) The following cookies are used for the proper functioning of the Website:

a) The authentication session cookie (PHP session cookie) is necessary for the basic operation of the website, it provides the identified browser-server connection during the use of the website, thus allowing the User to use convenience features such as the return of the form page with warning messages if the form is incomplete, and the return of the form page with warning messages to fill in the fields already filled in. The validity period of this cookie is limited to the User's current visit, and this type of cookie is automatically deleted from the User's computer at the end of the session or when the browser is closed.

b) The website uses cookies to ensure that a cookie warning message does not reappear in a browser if the User has accepted the use of cookies and clicked OK. This cookie stores information about whether the User has accepted the use of cookies in the browser.

Please note that without these cookies we cannot guarantee you the use of our website!

c) You can refuse the use of browser cookies by selecting the appropriate settings on your browser(s), which can be found in the links below.

- For Mozilla Firefox browser:
  https://support.mozilla.org/hu/kb/sutik-engedelyezese-es-tiltasa-amit-weboldak-haszn
- For the Google Chrome browser application:
  https://support.google.com/accounts/answer/61416?hl=hu
- For Safari browser applications:
  https://support.apple.com/hu-hu/guide/safari/sfri11471/mac

H. Web analytics and ad-serving external companies

1) The Data Controller uses external web analytics and ad serving companies for the operation of the Website, which perform their activities independently of the Data Controller.

2) The Data Controller uses Google Analytics and Google Adwords. Google uses cookies and web beacons (web beacons) to collect information and to help analyse the use of the Website. The information stored by the cookie (including the User's IP address) is stored on Google's own servers. Google may transfer the

information collected to third parties where required to do so by law, or where such third parties process the information on Google's behalf. As part of the Google Adwords remarketing service, Google places visitor-tracking cookies on Users' devices that monitor visitors' online behaviour and allow Google to serve them advertising on other websites based on their behaviour and interests. The tracking cookie also allows Google to identify the User on other websites. Google's "Privacy Policy" can be found at https://policies.google.com/privacy?hl=hu&gl=hu. Google's website contains further useful information about Google's data practices and how to disable cookies and personalise your advertising. It is not possible to opt-out of web beacons.

3) The Data Controller uses the services of Adverticum Zrt. as an advertising server. Further information about these services and Adverticum's data management can be found at https://adverticum.net/.

III. Transfers, recipients of personal data, external controllers

A. Transmission of data to the Fürge Student School Cooperative

1) The Data Controller is entitled to transfer the personal data detailed in point II.*A*.1) of this Notice to the Fierce Student School Cooperative.

2) Definition and contact details of the Fiery Student School Co-operative

Data Controller:	**Fürge Student School Co-operative**
Headquarters:	9700 Szombathely, Belsikátor 3.
Tax number:	11011011-2-18
Processing registration number:	NAIH-78837/2014
Webpage:	www.furgediak.hu
Customer service phone number:	+36 (1) 248-2010
Customer service e-mail address:	info@furgediak.hu

3) The purpose of the transfer is to contact the Data Subject to present the student employment service.

4) The legal basis for the transfer is the Data Subject's consent by accepting the terms of this notice.

B. Transmission of data to processors

1) The Data Controller processes the majority of personal data in digital form within its own organisation, using data processors. The Controller may transfer the Data Subject's personal data to a processor. Processors shall carry out the processing on behalf of the Controller and on the basis of the Controller's instructions.

2) The legal basis for the data transfer is the data processing contract between the Data Processor and the Data Controller in accordance with the GDPR and the Info.

3) Processors used for the processing of Data Subjects' data:

Name of data processor	**Infocomplex Ltd.**
Title:	7632 Pécs, Béke u. 1.
Phone number:	+36 (72) 555-777
Availability:	support@infocomplex.hu
Scope of data processing:	We store and transfer the processed personal data between our internal (own) departments and IT systems within the framework of IT asset management and system operation using the devices operated by Infocomplex Ltd. and the data security and other IT solutions and services provided by Infocomplex Ltd.

Name of data processor	**Netpositive Ltd.**
Address:	1031 Budapest, Záhony utca 7. I.
Phone number:	+36 (1) 266-9043
Availability:	info@netpositive.hu
Scope of data processing:	The Data Controller provides the possibility for the data subjects to provide personal data on the humaniahrsgroup.hu website within the framework of website operation, on the devices operated by Netpositive Ltd., using the data security and other IT solutions and services provided by them.

C. Transmission of data by courts and authorities

Court, public prosecutor's office, investigating authority, criminal investigation authority, administrative authority, the National Authority for Data Protection and Freedom of Information, or other bodies authorised by law may request the Data Controller to provide information, data, or documents. The Data Controller shall provide the requesting body with the personal data necessary to achieve the purpose of the request, provided that the precise purpose and the scope of the data have been specified.

D. Personal data processed by external controllers and processed by the Controller

1) The operator of external services (e.g. Facebook) that allow the sharing of content made available and shared on various social networking sites in the context of the Data Controller's activities is considered the data controller of personal data, and its own terms of use and privacy policy apply to its activities. For services embedded in the services but maintained by an external service provider, the operator of that service is also the data controller.

2) The Data Controller Humánia HRS Group Zrt. In case of installation and/or use of applications available on the Facebook page, the Data Controller will provide the personal data specified in the information made available by Facebook Inc. during installation and/or use to the Data Controller on the basis of the Data Subject's voluntary consent and in compliance with the **Facebook Inc.** Where a Facebook application refers to this Notice, the Notice shall govern the Data Controller's processing accordingly, otherwise processing within the Facebook service (e.g. deleting an application, posting a comment, etc.) shall be governed by the Facebook Privacy Policy.

3) You can delete applications by going to the Facebook user settings and going to the application menu (http://www.facebook.com/settings?tab=applications). The deletion of a Facebook application by the Data Controller does not result in the withdrawal of the consent given when using the wwww.humaniahrsgroup.hu website.

IV. Rights of data subjects

A. *Scope of the Data Subject's rights*

1) The data subject has the right to.
   a) at his or her request, to be informed by the Controller of the personal data relating to him or her processed by the Controller and of the information relating to the processing of such data
   b) at the request of the Data Controller, to correct or complete inaccurate or incomplete personal data relating to him or her,
   c) at the request of the Data Controller, the Data Controller shall restrict the processing,
   d) at his or her request, the Controller to delete personal data concerning him or her,
   e) upon request, receive personal data concerning him or her in a structured, commonly used, machine-readable format or have such data transmitted by the Controller to another controller,
   f) object at any time, on grounds relating to his or her particular situation, to the processing of his or her personal data based on the legitimate interests of the Controller.

B. *Enforcing the rights of the data subject*

1) The person concerned

   - any information previously provided by you through any channel (website, Facebook or other social media application, email or other electronic mail application, telephone, postal mail or otherwise); and
   - from other data sources processed by the Data Controller

   personal data concerning

   - for information,
   - to clarify,
   - to complement,
   - to delete,
   - a restriction or
   - for portability

   your request and your objection to the processing of your personal data

   - by sending an e-mail to info@humaniahrsgroup.hu, or
   - by post to the postal address at 1097 Budapest, Albert F. út 3/B., or
   - in person at any office of the Controller

   you may notify the Data Controller.

2) Where there are reasonable grounds to believe that the person making the request or objection is not the Data Subject, the Data Controller shall comply with the request after obtaining credible proof of the identity of the person making the request. The Data Controller shall consider such proof to be credible if the Data Subject has made the request or objection
   a) sends to the Controller from an electronic mail address previously provided to the Controller; or
   b) by post, accompanied by a copy of a photocopy of a photocopy of a public document, or
   c) in person at an office of the Data Controller, and provide proof of identity by means of a photo identification document (the addresses of our offices can be found on our website www.humaniahrsgroup.hu).

3) If the Data Subject does not provide sufficient proof of his or her identity, the Data Controller shall not comply with the request or objection. The Data Controller shall notify the Data Subject of the non-fulfilment of the request or objection, the reason for the non-fulfilment and the credible means of proof of identity in the same way as the Data Subject submits his or her request or objection.

4) The Data Controller will delete the data if.
   a) the personal data are no longer necessary for the purposes for which they were collected or processed;
   b) the data subject withdraws his or her consent and there is no other legal basis for the processing;
   c) the data subject objects to the processing and there are no overriding legitimate grounds for the processing,
   d) unlawfully processed the personal data;
   e) the personal data must be erased in order to comply with a legal obligation applicable to the Data Controller;
   f) personal data are collected in connection with the provision of information society services.

5) The Data Controller shall not delete the personal data of the Data Subject even at the request of the Data Subject, if the processing is
   a) for the purposes of complying with a legal obligation applicable to the Data Controller that requires the processing of personal data;
   b) for the presentation, exercise or defence of legal claims

   needed.

6) The Controller shall also erase the personal data of the Data Subject without the data subject's request to do so, if.
   a) the processing of personal data is unlawful or the purpose of the processing has ceased;
   b) the time limit for storing the data set by law or the Data Controller's Privacy Policy has expired;
   c) ordered by a court or the National Authority for Data Protection and Freedom of Information;
   d) if the processing is incomplete or inaccurate and this situation cannot be lawfully remedied, provided that erasure is not excluded by law.

7) The Data Controller shall restrict processing if.
   a) the Data Subject contests the accuracy of the personal data; in this case, the restriction applies for the period of time that allows the Controller to verify the accuracy of the personal data;
   b) the processing is unlawful and the Data Subject opposes the erasure of the data and requests instead the restriction of their use;
   c) the Controller no longer needs the personal data for the purposes of processing, but the Data Subject requires them for the establishment, exercise or defence of legal claims; or
   d) the Data Subject has objected to the processing; in this case, the restriction applies for the period until it is established whether the legitimate interests of the Controller override the legitimate interests of the Data Subject.

8) If the processing is restricted, the Data Controller shall process such personal data, except for storage, only with the consent of the Data Subject or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for important public interest.

9) At the request of the Data Subject, the Controller shall provide the personal data provided by the Data Subject to the Data Controller in a structured, commonly used, machine-readable format or transmit it to a controller designated by the Data Subject, if.
   a) the processing is based on consent or a contract, and
   b) the processing is carried out by automated means.

10) In case of an objection, the Data Controller shall examine whether the legal basis for the processing of the personal data concerned by the objection is the legitimate interest of the Data Controller, i.e. the processing is not necessary for compliance with a legal obligation or for the performance of a contract between the Data Subject and the Data Controller. If the legal basis for the processing is a legal obligation or the performance of a contract, or if the Controller demonstrates compelling legitimate grounds for the processing which override the rights of the Data Subject or for the establishment, exercise or defence of legal claims, the Controller shall reject the objection. Otherwise, the Data Controller shall delete the data concerned by the objection without delay.

11) By accepting the Privacy Notice, the Data Subject consents to the Data Controller responding to the Data Subject's request or objection by e-mail, if the Data Subject has provided an e-mail address, regardless of the channel through which the Data Subject has sent the request or objection to the Data Controller. In the absence of an e-mail address of the Data Subject, the Controller shall respond to the Data Subject's request for enforcement or objection in the same way as the submission of the request or in the same way as the submission of the Data Subject's request.

12) In case of a request for information by the Data Subject, the Data Controller shall provide information on the data relating to the Data Subject processed by the Data Controller or by a data processor on its behalf, their source, the purpose, legal basis and duration of the processing, the name and address of the data processor, the legal basis and recipient of the data transfer, and the data controller's activities related to the processing.

13) The Data Controller shall take the necessary measures and inform the Data Subject of the request or objection within a maximum of 25 days from the date of the request.

14) The procedures related to the Data Subject's enforcement request are free of charge and the Data Controller may not charge a fee or charge any fee for them, unless the Data Subject's request is for information on the data processed and the Data Subject requesting the information has already submitted a request for information to the Data Controller for the same data subject in the current year. In this case, the Controller may claim reimbursement of the costs incurred.

15) In the event of the death of the Data Subject, the next of kin of the Data Subject within the meaning of the Civil Code may exercise the rights to the Data Subject's personal data by presenting the death certificate in person or by sending a copy to the customer service address info@humaniahrsgroup.hu and by proving their relationship with the Data Subject.

16) In case of alleged violation of rights in connection with the processing of personal data, the Data Subject may turn to the competent court, in the capital city to the Metropolitan Court, or initiate an investigation at the National Authority for Data Protection and Freedom of Information (1055 Budapest, Falk Miksa street 9-11 ., ugyfelszolgalat@naih.hu , +36 (1) 391-1400, www.naih.hu).

V. Terms and conditions of use of the www.humaniahrsgroup.hu website (in this section: Policy)

A. *Content of the terms of use*

1) The present Terms of Use are published on the website **humaniahrsgroup.hu** (https://www.humaniahrsgroup.hu/) operated by Humánia HRS Group Zrt. (in this chapter: Service Provider) and on the website of Humánia HRS Group Zrt. (hereinafter collectively referred to as the "Service") on the website of the Humania Group HRG Group, Humania Group Group HRG Group, Inc.
2) A user is defined as a visitor to the Website or anyone who uses any of the services of www.humaniahrsgroup.hu, as well as a fan or follower of the Facebook page(s). If you start using any element of the Service, you accept the terms and conditions of this Policy.
3) Contracts resulting from the acceptance of the Rules are in Hungarian, do not constitute a written contract and are therefore not registered by the Service Provider and are not accessible afterwards.
4) The Service Provider is entitled to modify the Policy at any time. It will inform Users of the modification by means of a short notice on https://www.humaniahrsgroup.hu. By using any part of the Service after the amendment, the User accepts the amendment of the Rules.
5) Any website other than humaniahrsgroup.hu (Facebook.com, Google, etc.), whose service is linked to humaniahrsgroup.hu, is (also) subject to the terms and conditions published within the framework of that website.
6) The operation of the electronic channels and the contracts concluded between the Service Provider and the User shall be governed by the laws in force in Hungary, with the exception of conflict of law rules, and the jurisdiction of the Hungarian courts or the courts of the place of the Service Provider's registered office.

B. *Key features and elements of the Service*

1) The purpose of the Service is to display the Service Provider's services, to inform users and to receive applications from users.
2) The Service Provider reserves the right to modify or discontinue any content element of the electronic channels, to change their appearance, content, operation, to place content presenting its own services or other content on them at any time without prior warning or notice.

C. *Other provisions*

1) You may not use any system or solution that is intended to, enables or may result in the use of the Service in a manner not expressly permitted in these Terms or the downtime of servers used to operate the Service, or that in any way compromises the proper operation of the Service.
2) The Service and its content are protected by copyright. All copyrights and rights to protect the database producer belong to the Service Provider and may not be used or exploited in any form other than for reading, displaying on a screen and temporary reproduction necessary for the normal use of the Service, saving to a personal hard disk for non-commercial purposes and printing, without the prior written permission of the Service Provider.
3) The Service may be used only within the limits of the applicable legislation, without prejudice to the rights of the Service Provider and third parties, and in compliance with these Rules. If a User uses the Service in violation of the provisions of these Regulations or in breach of the law, or misuses the Service, the Service Provider shall be entitled to take the necessary legal action to hold the User liable. Such action may also be taken against the User if he misuses the data of another.

D. *Responsibility*

1) The Service Provider excludes all liability, i.e. does not assume any liability
   a) for the accuracy, reliability, error-free operation, completeness and fitness for purpose of the Service, including the software used to operate the Service and all content available through the Service;
   b) for errors caused by causes beyond its control and their consequences (technical malfunctions, outages, technical downtime of any origin, interruptions, destructive applications or programs installed by others, viruses, worms, macros or hacking activities, etc.);
   c) for any omissions in the data provided by the User during the use of the Website or for any consequences resulting from the incorrect data provided by the User;
   d) in respect of any material or non-material damage, injury or other consequences caused by the User, whether or not caused by the posted content or otherwise, or otherwise arising in connection with the User's conduct.

2) If, as a result of or in connection with the User's conduct, a third party, any authority or court brings any claim or proceeding against the Service Provider, the User shall take all measures required by the Service Provider and shall compensate the Service Provider for any damage, material damage and costs incurred by the Service Provider as a result of or in connection with any unlawful conduct of the User.

E. Scope of the Rules

The Service Provider reserves the right to terminate the Service in its entirety at any time, without prior notice or warning, in which case this Policy shall automatically terminate.