PRIVACY POLICY

This Privacy Policy describes the characteristics of data processing, in particular the collection, storage and use of data, on the following websites operated by Danubius IT Solutions Zrt.:
https://danubius.io/ | https://insurance.danubius.io/ | https://edtech.danubius.io/
(hereinafter collectively referred to as the "**Website(s)**"), operated by Danubius IT Solutions Zrt. (registered office: 2600 Vác, Hungary, Zichy utca 12; company registration number: 13-10-041091; tax number: 12413234-2-13, represented by Péter Balogh, Chief Executive Officer), hereinafter referred to as the "**Data Controller**".

This Privacy policy is effective from 20th January 2026. The Data Controller will make the current version of the Privacy policy available on its Websites.

The Privacy policy has been prepared on the basis of Regulation (EU) 2016/679 of the European Parliament and of the Council (hereinafter referred to as "GDPR"), subject to the provisions of Act CXII of 2011 on the Right to Informational Self-Determination and Freedom of Information (hereinafter referred to as "the Information Act"), and its definitions are in accordance with the definitions set out in Article 4 of the GDPR, and in certain points supplemented by the interpretative provisions of Article 3 of the Information Act. In matters not specified in this Privacy Policy, the GDPR and, in cases permitted by the GDPR, the rules of the Infotv. shall apply by way of assistance.

The Data Controller is entitled to prepare an extract of the contents of this Privacy Policy in relation to each processing operation and may also ensure that the data subjects sign this document to declare that they have read and acknowledge the contents of the extract in relation to the prior information relating to the processing of personal data. The Data Controller reserves the right to amend this Privacy Policy. If the modification affects the use of the personal data provided by the data subject, the changes will be communicated to the data subject in an appropriate form, such as an e-mail information letter. If the details of the processing are also changed as a result of the amendment of the Data Protection Policy, the Data Controller will seek the data subject's consent separately.

Please read the information below carefully and only use the services available on the Websites if you agree with the information below.

1. Principles of data processing

In providing its services, the Data Controller pays special attention to the protection of personal data, compliance with mandatory legal provisions, safe and fair processing. The Data Controller shall treat the personal data provided to it confidentially, as set out in the Privacy Policy.

As informational self-determination is a fundamental right of every natural person under the Fundamental Law, the Data Controller attaches the utmost importance to ensuring that its processing and its procedures for processing are carried out and practices are in accordance with the provisions of the applicable law and the following principles:

With regard to the principles of lawfulness, fairness and transparency, the Data Controller shall process personal data lawfully and fairly and in a transparent manner for the data subject in order to exercise a right or to fulfil an obligation. The use of personal data processed by the Controller for private purposes is strictly prohibited.

With regard to the purpose limitation principle, the Data Controller shall collect and process personal data only for specified, explicit and legitimate purposes, to the minimum extent and for the minimum time necessary to achieve those purposes, and shall not process them in a way incompatible with those purposes.

Accordingly, the Data Controller shall use the personal data of data subjects only for the purposes stated at the time of collection or for other appropriate purposes in accordance with the law.

The Data Controller shall pay particular attention to ensuring that its processing complies at all times with the purpose limitation principle and that the data are erased where the purpose for which they were processed has ceased to exist or the processing is otherwise unlawful. If the personal data are no longer needed, the Controller shall destroy them.

With regard to the principles of data quality (data minimisation and accuracy), the Data Controller shall process and collect only an adequate, relevant and necessary amount of personal data for the purposes for which it is processed. The Data Controller shall also take reasonable steps to ensure that personal data are accurate, complete and up to date and that personal data which are unnecessary for the purposes of the processing are deleted.

In accordance with the principle of 'limited retention', the Controller shall process personal data which allow the identification of data subjects only for the time necessary to achieve the purposes of the processing. The Data Controller shall ensure that the data are deleted after the purpose of the processing has changed or ceased to exist. The Data Controller shall store personal data for a longer period only if the personal data are processed for archiving purposes in the public interest, scientific and historical research purposes or statistical purposes. The Data Controller shall exercise particular care when disposing of data media containing personal data.

With regard to the principles of integrity and confidentiality, the Data Controller shall ensure the protection of personal data in a sealed, complete, continuous and risk-proportionate manner, and shall take organisational and technical measures to protect personal data in particular against unauthorised or unlawful processing, accidental loss, destruction or damage. In order to protect data against unauthorised use or disclosure, the Data Controller shall apply data security controls in its own activities.

The information security measures designed and implemented by the Controller shall ensure the confidentiality, integrity and availability of personal data. These measures are set out in the Controller's Information Security Policy.

Having regard to the principle of accountability, the Controller shall design and implement its data processing processes and set up its data management system in such a way that it is able to demonstrate compliance with the principles set out in this point at any time of processing, in particular when and in what form the personal data were collected and what information was provided to the data subject when the personal data were collected.

By means of this Data Processing Policy, the Data Controller shall provide the data subject with adequate information in accordance with Articles 13 and 14 of the GDPR.
The Data Controller, in its capacity as data controller, shall ensure that the data subject has access to the data processed by the Data Controller, unless an exception is provided by law, and may exercise his or her rights of access, rectification, restriction, erasure, portability and objection.

2. Concepts relating to data processing

The conceptual framework of the Privacy Policy corresponds to the definitions set out in Article 4 of the GDPR, supplemented at certain points by the interpretative provisions and definitions of Article 3 of the Data Protection Act. On this basis, therefore:

Data Processor: a natural or legal person or unincorporated organisation that processes data on the basis of a contract, including a contract concluded pursuant to a statutory provision, the Data Processors used by the Data Controller are listed in the Data Processor Register in Annex 1 to this Privacy Policy.

Data Processing: any operation or set of operations which is performed upon personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Data Controller: a legal person, as defined in this Privacy Policy, which autonomously determines the purposes for which the data are processed, takes and executes decisions regarding the processing of the data or has them executed by a processor.

Data Destruction: the complete physical destruction of a storage medium containing data.

Data erasure: rendering data unrecognisable in such a way that it is no longer possible to retrieve it.

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

Recipient: the natural or legal person, public authority, agency or any other body with whom or to which the personal data are disclosed, whether or not a third party. Public authorities which may have access to personal data in the context of an individual investigation in accordance with Union or Member State law are not recipients; the processing of such data by those public

authorities must comply with the applicable data protection rules in accordance with the purposes of the processing.

EEA Member State: a Member State of the European Union and another State party to the Agreement on the European Economic Area and a State whose nationals enjoy the same legal status as nationals of a State party to the Agreement on the European Economic Area under an international treaty between the European Union and its Member States and a State not party to the Agreement on the European Economic Area.

Data subject: any natural person who is or may be identified, directly or indirectly, on the basis of personal data.

Profiling: any form of automated processing of personal data whereby personal data are used to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict characteristics associated with that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

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, number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. Objection: a statement by the data subject objecting to the processing of his or her personal data and requesting the cessation of the processing or the erasure of the processed data.

3. Method and security of data processing

The Data Controller shall ensure the security of the data, and shall take the technical and organisational measures and establish the procedural rules necessary to enforce the data protection and confidentiality rules provided for in the GDPR and the Infotv. and other legislation. The Data Controller shall protect personal data against unauthorised access; alteration; disclosure; unauthorised disclosure; or accidental deletion, destruction; corruption; and inaccessibility resulting from changes in the technology used.

The Data Controller shall place particular emphasis on the protection of data files processed electronically in different registers so that data stored in different registers cannot be directly linked and attributed to the data subject, except where permitted by law.

4. Data processing in connection with the Data Controller's Website

4.1. Processing of data related to job applications

The Data Controller provides the opportunity to apply on its Website for each vacant position

Purpose of data processing	Receiving and assessing applications from jobseekers and filling the vacant position.
Scope of data processed	Name, e-mail address and any personal data provided by the data subject in his/her CV
Scope of data subjects	Persons who apply for a job advertisement published on the Data Controller's Website.
Legal basis for processing	The data subject's consent pursuant to Article 6(1)(a) of the GDPR.
Time limit for data storage	If the applicant has provided his/her personal data solely for the purpose of applying for a specific position, the Data Controller will process the data until the withdrawal of his/her consent or until the position is successfully filled, but not later than 90 days after the date of application for the position. If the applicant has given his/her consent to the Controller to process his/her personal data in connection with another position not filled by the Controller, the Controller shall process his/her data until the withdrawal of his/her consent, but for a maximum of 1 year from the date of application for the position.
Method of data processing	Electronically
Source of data	Data collected from the data subject.
Possible consequences of not providing data	The provision of the data is voluntary, if the data subject does not provide the Data Controller with the data, the data subject will not be able to apply for the position advertised on the Data Controller's Website.
Automated decision making and profiling	The Data Controller does not use automated decision-making or profiling.
Who can access the data?	The Data Controller's competent staff and any staff of the processors referred to in point 5 of this Privacy Policy.
Transfers to third countries or international organisations	No data will be transferred to third countries or international organisations.

4.2. Data processing in relation to the Facebook page

The Data Controller operates a Facebook page on the website https://www.facebook.com/, which can be accessed at the following link: https://www.facebook.com/danubiusinfo/

The Data Controller publishes information and informal news about its services and activities on its Facebook page. Visitors to the page have the opportunity to express their views on the services of the Data Controller. The Data Controller collects data and analyses the activity of visitors to its Facebook page through the Page Analysis function. With regard to the personal data collected through the Page Analytics on the Facebook Page, the Controller and Meta Platforms Ireland Ltd. are joint controllers pursuant to Article 26 of the GDPR, as the Controller and Meta Platforms Ireland Ltd. jointly determine the purposes and means of the processing.

For any other processing of personal data relating to the Facebook page and associated content where the purposes and means are not jointly determined, Meta Platforms Ireland Ltd. and the Controller, as the case may be, remain independent and separate controllers. The main obligations and responsibilities of the Data Controller and Meta Platforms Ireland Ltd. in relation to the joint processing are divided as follows.

Meta Platforms Ireland Ltd. assumes primary responsibility for the processing of analytics data under the GDPR and for complying with all applicable obligations under the GDPR in relation to the processing of analytics data. Meta Platforms Ireland Ltd. informs data subjects about the processing of their data in the "Information about the Page Analytics feature data" area on the Facebook page.

Meta Platforms Ireland Ltd. shall designate the communication channels for contacting the data subject. If the data subjects exercise their rights against the Data Controller in relation to the processing of analytics data, or if the Data Controller is approached by a supervisory authority in relation to the processing of analytics data, the Data Controller shall transmit to Meta Platforms Ireland Ltd. all relevant data relating to such requests without undue delay and in any case within 7 calendar days. Meta Platforms Ireland Ltd. undertakes to respond adequately to the data subjects' requests in order to fulfil its obligation. The Data Controller shall not act or respond on behalf of Meta Platforms Ireland Ltd. The Controller ensures that it has adequate legal basis under the GDPR to process the analytics data.

The Data Controller does not request from Meta Platforms Ireland Ltd. any specific personal data processed in the course of the Site Analytics, the Data Controller only sees the statistics and statements produced by Meta Platforms Ireland Ltd. and not the underlying personal data. For further information on the joint data management agreement between the Data Controller and Meta Platforms Ireland Ltd. for the Facebook Page, please see the contact details below: https://www.facebook.com/legal/terms/information_about_page_insights_data

Purpose of data processing	Processing of data relating to the use of the Facebook page.
Scope of data processed	As a general rule, the Data Controller only processes statistical data, such as the number of people who have liked, the number of new likes, the number of people who have read, liked, commented or shared a post on the Facebook page, the number of times a post has been marked as spam, It also treats age, gender, and location as statistics for people who like a Facebook page.
Scope of data subjects	Facebook page visitors.
Legal basis for processing	Consent of the data subject pursuant to Article 6(1)(a) GDPR.
Time limit for data storage	Until the data subject's consent is withdrawn.
Method of data processing	Electronically
Source of data	Data collected from the data subject.
Possible consequences of not providing data	Competent employees of the data controller, employees of Meta Platforms Ireland Ltd. and of any data processors. The current list of the Data Controller's data processors is set out in Section 5 of this Privacy Policy.
Automated decision-making and profiling	No data will be transferred to third countries or international organisations.

4.3. Data processing in relation to the company's LinkedIn page

The Data Controller operates a Facebook page on the website https://www.linkedin.com/, which can be accessed at the following link:

https://www.linkedin.com/company/danubius-it-solutions

The Data Controller publishes information and informal news about its services and activities on its LinkedIn page. Visitors to the page have the opportunity to express their views on the services of the Data Controller. The Data Controller collects data and analyses the activity of visitors to its LinkedIn page through the Page Analysis function.

With regard to the personal data collected through the Page Analytics on the LinkedIn Page, the Controller and LinkedIn Ireland UC. are joint controllers pursuant to Article 26 of the GDPR, as the Controller and LinkedIn Ireland UC. jointly determine the purposes and means of the processing. For any other processing of personal data relating to the LinkedIn page and associated content where the purposes and means are not jointly determined, LinkedIn Ireland UC. and the Controller, as the case may be, remain independent and separate controllers. The main obligations and responsibilities of the Data Controller and LinkedIn Ireland UC. in relation to the joint processing are divided as follows. LinkedIn Ireland UC. assumes primary responsibility for the processing of analytics data under the GDPR and for complying with all applicable obligations under the GDPR in relation to the processing of analytics data. LinkedIn Ireland UC. informs data subjects about the processing of their data in the "Information about the Page Analytics feature data" area on the LinkedIn page. LinkedIn Ireland UC. shall designate the communication channels for contacting the data subject.

If the data subjects exercise their rights against the Data Controller in relation to the processing of analytics data, or if the Data Controller is approached by a supervisory authority in relation to the processing of analytics data, the Data Controller shall transmit to Meta Platforms Ireland Ltd. all relevant data relating to such requests without undue delay and in any case within 7

calendar days. LinkedIn Ireland UC. undertakes to respond adequately to the data subjects' requests in order to fulfil its obligation. The Data Controller shall not act or respond on behalf of LinkedIn Ireland UC.

The Controller ensures that it has adequate legal basis under the GDPR to process the analytics data. The Data Controller does not request from LinkedIn Ireland UC. any specific personal data processed in the course of the Site Analytics, the Data Controller only sees the statistics and statements produced by LinkedIn Ireland UC. and not the underlying personal data.

For further information on the joint data management agreement between the Data Controller and LinkedIn Ireland UC. for the LinkedIn Page, please see the contact details below:

https://www.linkedin.com/legal/privacy-policy

Purpose of data processing	Processing of data relating to the use of the LinkedIn page.
Scope of data processed	As a general rule, the Data Controller only processes statistical data, such as the number of people who have liked, the number of new likes, the number of people who have read, liked, commented or shared a post on the LinkedIn page, the number of times a post has been marked as spam, It also treats age, gender, and location as statistics for people who like a LinkedIn page.
Scope of data subjects	LinkedIn page visitors.
Legal basis for processing	Consent of the data subject pursuant to Article 6(1)(a) GDPR.
Time limit for data storage	Until the data subject's consent is withdrawn.
Method of data processing	Electronically
Source of data	Data collected from the data subject.
Possible consequences of not providing data	Competent employees of the data controller, employees of LinkedIn Ireland UC. and of any data processors. The current list of the Data Controller's data processors is set out in Section 5 of this Privacy Policy.
Automated decision-making and profiling	No data will be transferred to third countries or international organisations.

4.4. Contact

The Data Controller can be contacted using one of the contact details provided on the Websites.

Purpose of data processing	Contacting users, contacting the Data Controller.
Scope of data processed	The name, email address, possibly telephone number of the data subject and other data related to the request.
Scope of data subjects	Persons contacting the Data Controller.
Legal basis for processing	The data subject's consent pursuant to Article 6(1)(a) of the GDPR.
Time limit for data storage	Until the purpose is fulfilled, at the most until erasure at the request ofthe data subject.
Method of data processing	Electronically
Source of data	Data collected from the data subject
Possible consequences of not providing data	If the data subject does not provide the Data Controller with the data, he/she will not be able to contact the Data Controller.
Automated decision-making and profiling	The Data Controller does not use automated decision-making or profiling.
Who can access the data?	Competent employees of the Controller and any employees of the processors referred to in point 5 of this Privacy Policy.
Transfers to third countries or international organisations	No data will be transferred to third countries or international organisations.

4.5. Data processing related to record keeping in connection with the exercise of data subjects' rights under the GDPR

Purpose of data processing	Data processing related to record keeping in connection with the exercise of data subject rights as defined in the GDPR.
Scope of data processed	Applicant's name, date and place of birth, mother's name, address, postal address, request to exercise data subject rights under the GDPR
Scope of data subjects	Person exercising the right of data subject under the GDPR.

Legal basis for processing	The legal basis for the processing is the fulfilment of a legal obligation pursuant to Article 6(1)(c) ofthe GDPRand legitimate interest pursuant to Article 6(1)(f) of the GDPR.
Time limit for data storage	5 years from the date of the request.
Method of data processing	On paper and/or electronically
Source of data	Data collected from the data subject
Possible consequences of not providing data	Processing of data is necessary for the Data Controller to comply with the requirements of the GDPR
Automated decision-making and profiling	The Data Controller does not use automated decision-making or profiling.
Who can access the data?	Competent employees ofthe Data Controller and any employees of the processors named in point 5 of this Privacy Policy
Transfers to third countries or international organisations	No data will be transferred to third countries or international organisations.

4.6. Cookies

The Data Controller uses cookies on the Websites, detailed information on which is available via the following link: https://danubius.io/en/cookie-policy/

5. Data processors

Processors do not take independent decisions, they are only entitled to act in accordance with the contract concluded with the Data Controller and the instructions received. Processors shall record, process or handle personal data transmitted to them by the Controller and processed or handled by them in accordance with the provisions of the GDPR. Processors shall carry out processing operations on the personal data provided by data subjects within the time limits for use indicated in this Privacy policy, in accordance with the purposes for which the data are processed. The Data Controller uses the following processors in connection with its processing activities as indicated in this Privacy policy:

Data processor category	Purpose of data processing	Data processor		
		Name	Address	Registration number
Hosting and cloud service provider	Hosting and cloud service	Google Ireland	Gordon House, Barrow Street, Dublin 4, Ireland	-
Collection of statistical data (Google Analytics), marketing (Google Ads)	Statistics on website visitors, marketing activities	Google Ireland	Gordon House, Barrow Street, Dublin 4, Ireland	-
Marketing (Meta Pixel)	Marketing activities	Meta Platforms Ireland Ltd.	4 Grand Canal Square Grand Canal Harbour Dublin 2, Ireland	-
Marketing (LinkedIn Tag)	Marketing activities	LinkedIn Ireland UC.	Wilton Plaza, Wilton Place, Dublin 2, D02 R296, Ireland	-

5. Enforcement of data subjects' rights

The data subject may request information on the processing of his or her personal data; request the rectification of his or her personal data; request the restriction of processing; request the erasure of his or her data directly from the Data Controller at the e-mail address office@danubiusinfo.hu and exercise his or her right to data portability and the right to judicial remedy and the right to withdraw consent. In the event of a complaint, the data subject may lodge a complaint with the National Authority for Data Protection and Freedom of Information or, at his/her option, with a court in Hungary. The court of law has jurisdiction in court proceedings. The Data Controller shall, in case of fulfilling the data subject's request for the processing of personal data, identify the data subject in accordance with this Privacy Policy with regard to the capacity of the data subject (customer, requester, etc.) and the Data Controller shall be entitled to fulfil the data subject's request/request only after the data subject has been identified to the appropriate level.

If the applicant has not made a request for personal data processing in accordance with this Privacy Policy and the Data Controller has not been able to identify the applicant adequately (as required for data security and/or confidentiality (as set out in this Privacy Policy)), the Data Controller will invite the applicant to complete the request and, in the event of failure to do so or to comply with the request, the Data Controller will not be able to respond to the request.

The time elapsed between the request by the Data Controller to provide the required personal data/perform the missing activity and the provision of the personal data shall not be counted in the time limit for responding to the request.

The Controller shall inform each recipient to whom or with which the personal data have been disclosed of any rectification, erasure or restriction of processing, unless this proves impossible or involves a disproportionate effort. The Data Controller shall inform the data subject, at his or her request, of these recipients .

a) Right to information and access

In accordance with the obligation under Article 13 of the GDPR, the Data Controller is obliged to provide data subjects with the following information on the processing of personal data, where the personal data originate from the data subject at the time of obtaining the personal data:

(a) the identity and contact details of the Data Controller and its representative; (b) the contact details of the Data Protection Officer, if any;

(c) the purposes for which the personal data are intended to be processed and the legal basis for the processing;

(d) where applicable, the recipients of the personal data and the categories of recipients, if any;

(e) the duration of the storage of the personal data or, where this is not possible, the criteria for determining that duration;

(f) information on the data subject's right to obtain from the Data Controller access to, rectification, erasure or restriction of processing of personal data relating to him or her and to object to the processing of such personal data, and on the data subject's right to data portability;

(g) in the case of processing based on consent, the right to withdraw consent at any time, without prejudice to the lawfulness of the processing carried out on the basis of consent prior to its withdrawal;

(h) the right to lodge a complaint with a supervisory authority;

(i) whether the provision of the personal data is based on a legal or contractual obligation or is a precondition for the conclusion of a contract, whether the data subject is under an obligation to provide the personal data and the possible consequences of not providing the data.

Where the personal data have not been obtained from the data subject, the Data Controller shall provide the data subject with the above information and, in addition, the following information in accordance with Article 14 of the GDPR:

(a) the categories of personal data concerned;

(b) the recipients of the personal data or categories of recipients, if any;

(c) the source of the personal data and, where applicable, whether the data originate from publicly available sources.

Where the personal data have not been obtained from the data subject, the Data Controller shall provide the information:

(a) within a reasonable period from the date of obtaining the personal data, but not later than one month;

(b) where the personal data are used for the purpose of contacting the data subject, at least at the time of the first contact with the data subject; or

(c) if the data are likely to be disclosed to other recipients, no later than the first disclosure of the personal data.

The obligation to provide the information described above need not be fulfilled if:

- the data subject already has the information referred to in these points,
- the provision of such information proves impossible or would involve a disproportionate effort,
- the obtaining or disclosure of the data is expressly required by EU or Hungarian law applicable to the Data Controller, which also provides for adequate measures to protect the legitimate interests of the data subject, or
- the personal data must remain confidential pursuant to an obligation of professional secrecy under EU or applicable Hungarian law.

The data subject's right of access, as defined in Article 15 of the GDPR, includes the right to provide the following information:

- purposes of the processing;
- categories of personal data concerned;
- the recipients to whom the personal data are or will be disclosed;
- the intended duration of the storage of personal data;
- rights of the data subject with regard to the processing of personal data; - the source of the data, if not collected from the data subject;
- information on automated decision-making.

In all cases, the Controller shall endeavour to ensure that the information it provides to the data subject is, as far as possible, concise, transparent, intelligible, easily accessible, clear and plain, in compliance with the rules laid down by the GDPR. The Data Controller is responsible for providing the information and taking action. The Controller shall provide all information to the data subject in writing, including by electronic means. With regard to the data security rules set out in Article 15 and Article 32 of the GDPR, the Controller shall provide information to the data subject only and exclusively if the Controller is satisfied as to the identity of the data subject. If the identity is not verified, the Controller shall reject the data subject's request to exercise his or her rights and shall inform the data subject of the means of exercising his or her rights.

The Data Controller shall inform the data subject within one month of receipt of the request in the event of a request concerning his or her rights, duly notified in a statement. Taking into account the complexity of the request and the number of requests, this one-month period may be extended by a further two months by means of a reasoned communication from the Controller to the data subject within one month of the submission/receipt of the request to the Controller.

A reasonable communication or receipt shall be deemed to have been made when the written request is sent by the data subject to the Data Controller's official address or to the email address provided for that purpose and is received by the Data Controller.

Requests not communicated in accordance with the above shall not be taken into account by the Data Controller.

The information and communication relating to the processing of personal data shall be easily accessible and comprehensible and shall be drafted in clear and plain language. This principle shall apply in particular to the information provided to data subjects on the identity of the controller and the purposes of the processing, as well as to further information to ensure fair

and transparent processing of their personal data, and to the information that data subjects have the right to obtain confirmation and information about the data processed concerning them.

The Controller shall provide the information and take the measures referred to in this point free of charge, and shall charge a fee only in the cases provided for in Article 12(5) of the GDPR.

b) Right to rectification

The data subject shall have the right to obtain from the Data Controller, upon his or her request and without undue delay, the rectification of inaccurate personal data relating to him or her. Having regard to the purposes of the processing, the data subject shall have the right to obtain the rectification of incomplete personal data, including by means of a supplementary declaration.

c) Right to object

The data subject may object to the processing of his or her personal data by means of a statement addressed to the Controller, if the legal basis for the processing is.

- public interest within the meaning of Article 6(1)(e) of the GDPR , or
- legitimate interest under Article 6(1)(f) of the GDPR.

In the event of the exercise of the right to object, the Controller may no longer process the personal data unless the Controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims. The management of the Controller shall decide whether the processing is justified by compelling legitimate grounds.

It shall inform the data subject of its position in an opinion. For the period until the determination, the personal data shall be restricted accordingly.

d) Right to restriction of processing

Restriction of processing may take place if:

- the data subject contests the accuracy of the data, the Controller shall restrict the processing of personal data for a period of time until the accuracy of the data is established;

- processing is unlawful and the data subject requests restriction of use instead of erasure;

- The data controller no longer needs the data but the data subject requests them for the purpose of pursuing legal claims;
- the data subject objects to the processing of personal data pursuant to Article 21 of the GDPR, pending the outcome of the assessment of the objection.

For the duration of the assessment of the data subject's objection to the processing of his or her personal data, but for a maximum period of 5 days, the Controller shall suspend the processing, examine the grounds for the objection and take a decision, which shall be notified to the applicant.

If the objection is justified, the Data Controller shall restrict the data, i.e. only storage as processing may take place until:

- the data subject consents to the processing;
- processing of personal data is necessary for the exercise of legal claims;
- processing of personal data is necessary to protect the rights of another natural or legal person;
- or processing is required by law in the public interest.

Where the restriction on processing is lifted by the Controller, the Controller shall, prior to lifting the restriction, inform in writing the data subject at whose request the restriction was lifted of the fact of the lifting of the restriction, unless this proves impossible or involves a disproportionate effort. Where the restriction of processing has been requested by the data subject, the controller shall inform the data subject in advance of the lifting of the restriction.

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

The data subject shall have the right to obtain from the Data Controller the erasure of personal data relating to him or her without undue delay and the Data Controller shall be obliged to erase personal data relating to him or her without undue delay if one of the following grounds applies:

(a) the personal data are no longer necessary for the purposes for which they were collected or otherwise processed;

(b) the data subject withdraws the consent on the basis of which the processing was carried out and there is no other legal basis for the processing;

(c) the personal data have been unlawfully processed;

(d) the personal data must be erased in order to comply with a legal obligation under Union or Member State law to which the controller is subject;

(e) the personal data have been collected in connection with the provision of information society services.

The restriction of the data subject's right to erasure may only be made if the following exceptions in the GDPR apply, i.e. if the above grounds are met, the continued retention of personal data may be considered lawful,

(a) where the exercise of the right to freedom of expression and information, or

(b) to comply with a legal obligation (i.e. in the case of an activity recorded in the Register of Data Processing as a legal obligation, for a period of time adequate for the purposes of the processing), or

(c) where the performance of a task carried out in the public interest; or (d) in the exercise of official authority vested in the controller; or

(e) where it is in the public interest in the field of public health,

(f) for archiving purposes in the public interest; or

(g) for scientific or historical research purposes or for statistical purposes; or (h) where necessary for the establishment, exercise or defence of legal claims.

f) The right to data portability

The data subject shall have the right to receive the personal data concerning him or her which he or she has provided to the Controller in a structured, commonly used, machine-readable format and the right to transmit such data to another controller without hindrance from the controller to which he or she has provided the personal data, provided that:

- the legal basis for the processing is the consent of the data subject or the processing was necessary for the performance of a contract to which the data subject is a party or for the purposes of taking steps at the request of the data subject prior to entering into that contract [Article 6(1)(a) or (b) or Article 9(2)(a) GDPR]
- processing is carried out by automated means.

The right under this point shall not apply to the data subject if the 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, or if it would adversely affect the rights and freedoms of others.

Where the Data Controller is required to disclose personal data to a third party other than the data subject on the basis of the data subject's right to data portability, the Data Controller shall inform and draw the attention of that third party to the fact that the personal data disclosed by the Data Controller in relation to the data subject shall not be used for its own purposes and shall be processed for the purposes for which they were disclosed only in accordance with the provisions of the applicable data protection legislation. The Data Controller shall not be liable for the use by a third party of personal data duly transmitted to a third party at the request of the data subject.

g) Right to withdraw consent

Where the legal basis for the processing of the data subject's personal data by the Controller is the data subject's consent, the data subject may withdraw his or her consent to the processing at any time. In this regard, the Controller informs data subjects that the Controller may process their personal data for the purposes of complying with a legal obligation or pursuing legitimate interests even after the withdrawal of their consent, if the pursuit of those interests is proportionate to the restriction of the right to the protection of personal data.

6. Legal remedies

The data subject has the right to contact the Data Controller directly at the following e-mail address: office@danubiusinfo.hu to remedy the infringement or to lodge any other complaint.

If the data subject considers the data processing of the Data Controller to be prejudicial, he or she may lodge a complaint with the National Authority for Data Protection and Freedom of Information (address: 1055 Budapest, Falk Miksa utca 9-11., postal address: 1363 Budapest, Pf. 9., telephone number: +36 (1) 391-1400, e-mail: ugyfelszolgalat@naih.hu, website: www.naih.hu). In such a case, they are free to decide whether to bring their action before the courts for the place of residence (permanent address) or the place of stay (temporary address) (http://birosag.hu/torvenyszekek). You can find the court of your domicile or residence at http://birosag.hu/ugyfelkapcsolati-portal/birosag-kereso.