Data Protection Notice of NoBoVersum Zrt.
Regarding the processing of personal data of data subjects

INTRODUCTION

In compliance with the regulation in effect since April 27, 2016, titled "On the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Regulation (EC) No. 95/46/EC," set forth by the European Parliament and Council (EU) 2016/679 (hereinafter: General Data Protection Regulation, GDPR), the Company fulfills its legal obligations to provide data subjects with concise, transparent, comprehensible, and easily accessible information regarding personal data processing through the provisions and rules outlined below. The Data Protection Policy and notice will be published on the Data Controller's website and will also be available free of charge in physical form at the Company's headquarters.

CHAPTER I
NAME OF THE DATA CONTROLLER

The publisher of this notice, and the Data Controller:

Company Name: **NoBoVersum Closed Company Limited by Shares**
Headquarters: **1134 Budapest, Váci út 49, 6th floor**
Company Registration Number: **01 10 141942**
Tax Number: **32019667-2-41**
Website: www.noboversum.hu
(hereinafter: Company or Data Controller)

CHAPTER II
DATA PROTECTION NOTICE ON ADULT EDUCATION

In accordance with Sections 16 and 21 of Act LXXVII of 2013 on adult education and the provisions of the General Data Protection Regulation (GDPR) (EU) 2016/679, we hereby inform you, as a Data Subject, about the processing of your personal data.

Data Controller Information:

Company Name: NoBoVersum Zrt.
Headquarters: 1134 Budapest, Váci út 49, VI. floor
Email: info@noboversum.hu
Institution Registration Number: B/2023/000519
Institution Authorization Number: E/2023/000048

1. **DATA SCOPE:**

Legal Basis for Data Processing: GDPR Article 6 (1) (c) [considering Sections 16 and 21 of Act LXXVII of 2013 on Adult Education], meaning that data processing is necessary for compliance with a legal obligation to which the Data Controller is subject.

Purpose of Data Processing: To carry out training falling under the Adult Education Act and to fulfill the data processing and reporting obligations prescribed by law.

Duration of Data Processing: The Data Controller processes the data until the last day of the eighth year following the conclusion of the Adult Education Contract. The data of the Adult Education Administrative Body (Pest County Government Office) are processed until the last day of the fiftieth year following their creation, after which they will be handed over to the relevant archive and deleted.

Data Scope:
a) The individual participating in the training
   aa) personal identification data (name, birth name, mother's name, place and date of birth),
   ab) email address,
   ac) highest educational qualification.
b) Data related to the training of the individual participating in it, including
   ba) the highest educational qualification, professional qualification, and foreign language knowledge,
   bb) their entry into the training and completion of the training, or in the absence of completion, their withdrawal from the training,
   bc) evaluation and qualification during the training,
   bd) payment obligations related to the training and any training loans taken.

Data Processors:
1. Pest County Government Office: Budapest, Városház u. 7, 1052, felnottkepzes@pest.gov.hu, (+36-1) 485-6900
2. Central Statistical Office: 1024 Budapest, Keleti Károly utca 5–7., (+36-1) 345-6789

Data Transfer:
The Data Controller will transfer the data specified in point a) to the Pest County Government Office's FAR system (Adult Education Data Reporting System). The data may be used for statistical purposes and may be shared in a manner that does not allow for personal identification; furthermore, it may be shared with the Central Statistical Office for statistical purposes in a way that allows for individual identification without charge. The data must be forwarded to bodies controlling the utilization of public funds or European Union sources for the purpose of verification. The Data Controller must maintain, keep records of, and preserve for eight years following their creation the following documents, which may contain personal data, to ensure that the supervisory body of adult education has the ability to exercise its oversight rights:
a) attendance sheets signed by the individual participating in the training, as well as documents verifying professional preparation and checks conducted with the individual participating in the training via electronic means,
b) personal data processed according to Section 21 (1) of the Act, as well as original documents or certified copies confirming the conditions required to begin participation in the education and training, as well as documents proving the initial competency assessment and prior knowledge assessment.

2. **DATA SCOPE:**

Legal Basis for Data Processing: Legitimate interest of the training provider.
Purpose of Data Processing: Maintaining contact during the execution of training falling under the Adult Education Act.
Duration of Data Processing: Until the last day of the eighth year following the conclusion of the Adult Education Contract.
Data Scope: Email address and phone number of the individual participating in the training.
Data Processor: NoBoVersum Zrt.
Data Transfer: None.

3. **DATA SCOPE:**

Legal Basis for Data Processing: Fulfillment of legal obligations.
Purpose of Data Processing: Issuing an invoice during training under the Adult Education Act.
Duration of Data Processing: Until the last day of the eighth year following the conclusion of the Adult Education Contract.
Data Scope: Billing address of the individual participating in the training.
Data Processor: NoBoVersum Zrt.
Data Transfer: None.

4. **Rights of Data Subjects:**

The rights of data subjects are contained in Chapter VII of this Data Protection Notice.

5. **Other Information:**

Participation in training requires the provision of the above personal data, which the Participant is obliged to provide to the Data Controller; failure to do so may result in ineligibility for participation in the training.

CHAPTER III
DATA PROCESSING RELATED TO EMPLOYMENT
(SUMMARY)

1. Processing of Data of Job Applicants, Applications, Resumes:

(1) The scope of personal data that can be processed includes: name, date and place of birth, mother's name, address, qualification data, photo, phone number, email address, and employer notes made about the applicant.

(2) The purpose of processing personal data: application assessment and the conclusion of an employment contract with the selected candidate. The applicant must be informed if they are not selected for the position.

(3) Legal basis for data processing: the consent of the data subject.

(4) Recipients of personal data, or categories of recipients: a manager authorized to exercise employer rights at the Company, HR and personnel workers.

(5) Duration of storage of personal data: until the application is assessed. The personal data of unsuccessful applicants must be deleted. The data of individuals who withdraw their application must also be deleted.

(6) The employer may only retain applications based on the explicit, clear, and voluntary consent of the data subject, provided that retention is necessary to achieve a legally compliant purpose. This consent must be requested from applicants after the selection process has been completed.

(7) The rules for individuals applying for a position must be communicated in accordance with the provisions of the Regulation and the Information Act.

CHAPTER IV
DATA MANAGEMENT RELATED TO OBLIGATORY LEGAL RELATIONSHIPS

1. Management of Contracting Partners' Data

(1) The Company manages the name, birth name, date of birth, mother's name, address, tax identification number, VAT number, entrepreneur or agricultural producer identification number, personal identification number, residence address, registered office, site address, phone number, email address, website address, bank account number, customer number (client number, order number), and online identifier of the contracted natural person for the purpose of contract execution, contract conclusion, performance, termination, and the provision of contractual benefits. This data management is considered lawful even if it is necessary for steps taken at the request of the data subject before the conclusion of the contract. The recipients of the personal data are the employees

of the Company performing customer service tasks, employees responsible for accounting and taxation, and data processors. The duration of storage of personal data is 5 years following the termination of the contract.

(2) Before commencing data management, the data subject must be informed that the data management is based on the execution of the contract, and this information can also be provided in the contract. The data subject must be informed about the transfer of their personal data to data processors.

2. Contact Details of Natural Persons Representing Legal Entity Clients

(1) The scope of manageable personal data: the name, address, phone number, email address, and online identifier (if applicable) of the natural person.

(2) The purpose of managing personal data: to fulfill the contract concluded with the Company's legal entity partner and to maintain business relations.

(3) The legal basis for data management: the consent of the data subject.

(4) The recipients of personal data and the categories of recipients: the Company’s executives, their deputies, and other employees involved in partner relationship management tasks.

(5) The duration of storage of personal data: for 5 years following the maintenance of the business relationship or the representative status of the data subject.

3. Visitor Data Management on the Company’s Website

(1) Cookies are small data files placed on the user's computer by the visited website. The purpose of cookies is to facilitate and enhance the given information and internet services. There are many types, but they can generally be classified into two main groups. One is temporary cookies, which are placed on the user’s device only during a specific session (e.g., during a secure internet banking identification), and the other is persistent cookies (e.g., a website's language settings), which remain on the computer until the user deletes them. According to the guidelines of the European Commission, cookies [except those essential for using the service] can only be placed on the user’s device with the user's permission.

(2) For cookies that do not require the user's consent, information must be provided during the first visit to the website. It is not necessary for the full text of the cookie notification to be displayed on the website; it is sufficient for the website operators to briefly summarize the essence of the notification and refer to the availability of the full notification through a link.

(3) For cookies that require consent, the information may also be linked to the first visit to the website if the data management associated with the use of cookies begins with visiting the page. If the application of the cookie is related to a function explicitly requested by the user, then the information may also appear regarding the use of that function. In this case, it is not necessary for the full text of the cookie notification to be displayed on the website; a brief summary of the essence of the notification and a link to the availability of the full notification is sufficient.

4. Information on the Use of Cookies

(1) A cookie is a small file containing only letters and numbers, which can be stored on a user's computer, mobile phone, or other internet-accessing devices. A cookie is an information package sent by the web server to the browser, which then returns it to the server with each request directed to the server. Cookies are "passive," meaning they do not contain executable files, viruses, or spyware, nor do they access the user's hard drive data. These files enable the recognition of the user's device used for internet browsing and thereby facilitate the display of relevant content tailored to the user's needs. Cookies provide a simpler browsing experience for the user and help the Company to provide as comfortable services as possible. These include online data security requirements or relevant advertisements. By utilizing the obtained statistical results, the Company can adapt the structure and content of the site according to demands while preserving users' anonymity.

(2) Our company's website records and manages the following data about the visitor and the device used for browsing during the use of the website:

- the IP address used by the visitor,
- the type of browser,
- the characteristics of the operating system of the device used for browsing (set language),
- the date and time of the visit,
- the (sub)page, feature, or service visited.

(3) Acceptance and authorization of cookies are not mandatory. You can reset your browser settings to reject all cookies or to alert you when a cookie is sent. Although most browsers automatically accept cookies by default, these settings can usually be changed to prevent automatic acceptance and offer the option to choose every time.

You can find information on cookie settings for the most popular browsers at the following links:

- Google Chrome: https://support.google.com/accounts/answer/61416?hl=hu
- Firefox:https://support.mozilla.org/hu/kb/sutik-engedelyezese-es-tiltasa-amit-weboldak-haszn
- Microsoft Internet Explorer 11: http://windows.microsoft.com/hu-hu/internet-explorer/delete-manage-cookies#ie=ie11
- Microsoft Internet Explorer 10: http://windows.microsoft.com/hu-hu/internet-explorer/delete-manage-cookies#ie=ie10-win-7
- Microsoft Internet Explorer 9: http://windows.microsoft.com/hu-hu/internet-explorer/delete-manage-cookies#ie=ie-9
- Microsoft Internet Explorer 8: http://windows.microsoft.com/hu-hu/internet-explorer/delete-manage-cookies#ie=ie-8
- Microsoft Edge: http://windows.microsoft.com/hu-hu/windows-10/edge-privacy-faq
- Safari: https://support.apple.com/hu-hu/HT201265

However, we would like to draw your attention to the fact that certain website functions or services may not function properly without cookies.

(4) The cookies used on the website are not suitable for identifying the user on their own. The website uses two types of cookies: session cookies and persistent cookies. The former are temporary files that remain on the user's device until the logged-in session ends or the application (browser) is closed. Persistent cookies remain on the user's device for the duration specified in their parameters (or until manually deleted).

CHAPTER V
DATA MANAGEMENT BASED ON LEGAL OBLIGATIONS

1. Data Management for Tax and Accounting Obligations

(1) The Company manages the legally required data of natural persons entering into business relationships with it as a customer or supplier to fulfill legal obligations, specifically tax and accounting obligations (accounting, taxation). The managed data are particularly those specified in Section 169 and Section 202 of Act CXXVII of 2007 on Value Added Tax, including: tax number, name, address, tax status, as per Section 167 of Act C of 2000 on Accounting: name, address, the identification of the person or organization ordering the economic operation, the person authorizing and verifying the execution, and, depending on the organization, the signature of the auditor; on inventory movement documents and cash management documents, the signature of the recipient, and on counter receipts, the signature of the payer, according to Act CXVII of 1995 on Personal Income Tax: entrepreneur identification number, agricultural producer identification number, tax identification number.

(2) The duration of storage of personal data is 8 years following the termination of the legal relationship providing the legal basis.

(3) The recipients of personal data are the Company's executives, their deputies, and employees and data processors responsible for the Company's taxation, bookkeeping, payroll, and social security tasks.

2. Data Management for Payer Obligations

(1) The Company manages the personal data of affected individuals – employees, their family members, other beneficiaries – required by tax laws, for the purpose of fulfilling legal obligations related to tax and contribution obligations (determining tax, advance tax, contributions, payroll, social security administration). The scope of the managed data is defined by Section 50 of the Act on the Rules of Taxation (2017 CL. Act) 7§31, highlighting specifically: the natural person's identification data (including previous names and title), gender, nationality, tax identification number, social security identification number (TAJ number). If tax laws attach legal consequences to it, the Company may manage employees' health (Section 40 of the Income Tax Act) and union membership data (Section 47(2)(b) of the Income Tax Act) for the fulfillment of tax and contribution obligations (payroll, social security administration).

(2) The duration of storage of personal data is 50 years following the termination of the legal relationship providing the legal basis.

(3) The recipients of personal data are the Company's employees and data processors responsible for taxation, payroll, and social security (payer) tasks.

3. Data Management to Fulfill Anti-Money Laundering Obligations

(1) The Company manages personal data for the purpose of fulfilling anti-money laundering obligations defined in the Act on the Prevention and Combating of Money Laundering and Terrorist Financing. The scope of managed data: the name, birth name, date of birth, tax identification number, address, bank account number, and any other data that allow the Company to identify the data subject. The purpose of managing personal data is to fulfill legal obligations (regarding data management) related to the fight against money laundering and terrorist financing.

(2) The duration of storage of personal data is 8 years following the termination of the legal relationship providing the legal basis.

(3) The recipients of personal data are the Company's employees and data processors responsible for fulfilling the Company's anti-money laundering obligations.

CHAPTER VI
SUMMARY INFORMATION ON THE RIGHTS OF THE DATA SUBJECT

1. Definitions

The concepts and provisions defined here are fully consistent with the terms and requirements of the Regulation. In this chapter, for the sake of clarity and transparency, we briefly summarize the rights of the data subject, with detailed information on exercising these rights provided in the next chapter. Communication with the Data Controller can be done through the contact details listed for the Data Controller.

Right to Preliminary Information

The data subject has the right to receive information about the facts and circumstances related to data processing prior to the commencement of the data processing. (Regulation Articles 13-14)

Right of Access

The data subject has the right to obtain confirmation from the Data Controller as to whether personal data concerning them is being processed, and if such processing is ongoing, they are entitled to access their personal data and related information as specified in the Regulation. (Regulation Article 15)

Right to Rectification

The data subject has the right to request the rectification of inaccurate personal data concerning them without undue delay by the Data Controller. Considering the purpose of the data processing, the data subject has the right to request the completion of incomplete personal data, including by means of a supplementary statement. (Regulation Article 16)

Right to Erasure ("Right to be Forgotten")

The data subject has the right to request the deletion of personal data concerning them without undue delay, and the Data Controller is obliged to delete personal data concerning the data subject without undue delay if any of the grounds specified in the Regulation exist. (Regulation Article 17)

Right to Restrict Processing

The data subject has the right to request the restriction of processing by the Data Controller if the conditions specified in the Regulation are met. (Regulation Article 18)

Notification Obligation Regarding Rectification, Erasure, or Restriction of Processing

The Data Controller shall inform all recipients of any rectification, erasure, or restriction of processing regarding personal data communicated to them, unless this proves impossible or involves a disproportionate effort. Upon request, the Data Controller shall inform the data subject of these recipients. (Regulation Article 19)

Right to Data Portability

Under the conditions laid down in the Regulation, the data subject has the right to receive the personal data concerning them, which they have provided to a Data Controller, in a structured, commonly used, and machine-readable format, and to transmit those data to another Data Controller without hindrance from the original Data Controller. (Regulation Article 20)

Right to Object

The data subject has the right to object at any time to the processing of personal data concerning them for reasons related to their particular situation, where the processing is based on point (e) (processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Data Controller) or point (f) (processing necessary for the purposes of legitimate interests pursued by the Data Controller or a third party). (Regulation Article 21)

Automated Decision-Making in Individual Cases, Including Profiling

The data subject has the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning them or similarly significantly affects them. (Regulation Article 22)

Limitations

Union or member state law may provide for legislative measures that restrict the rights and obligations laid out in Articles 12–22 and Article 34 in accordance with the Regulation. (Regulation Article 23)

Information to the Data Subject about a Data Breach

If a data breach is likely to result in a high risk to the rights and freedoms of natural persons, the Data Controller shall notify the data subject of the data breach without undue delay. (Regulation Article 34)

Right to Lodge a Complaint with a Supervisory Authority (Right to Administrative Remedy)

The data subject has the right to lodge a complaint with a supervisory authority—particularly in the member state of their habitual residence, place of work, or the place of the alleged infringement—if they consider that the processing of personal data concerning them infringes the Regulation. (Regulation Article 77)

Right to Effective Judicial Remedy Against a Supervisory Authority

Every natural and legal person has the right to an effective judicial remedy against a legally binding decision of a supervisory authority concerning them, or if the supervisory authority does not handle the complaint, or does not inform the data subject about the procedural developments or the outcome of the complaint within three months. (Regulation Article 78)

Right to Effective Judicial Remedy Against the Data Controller or Processor

Every data subject has the right to an effective judicial remedy if they consider that their rights under this Regulation have been infringed as a result of the processing of their personal data in non-compliance with this Regulation. (Regulation Article 79)

2. Detailed Information on the Rights of the Data Subject

Right to Preliminary Information

The data subject has the right to receive information about the facts and circumstances related to data processing prior to the commencement of the data processing.

A) Information to be Provided When Personal Data is Collected from the Data Subject

(1) If personal data concerning the data subject is collected from the data subject, the Data Controller shall provide the following information at the time of data collection:

a) The identity and contact details of the Data Controller and, where applicable, of the Data Controller's representative;
b) The contact details of the data protection officer, if any;
c) The purpose of the intended processing of personal data and the legal basis for the processing;
d) In cases where the processing is based on point (f) of Article 6(1) (legitimate interest), the legitimate interests pursued by the Data Controller or a third party;
e) Where applicable, the recipients of personal data or categories of recipients;
f) Where applicable, the fact that the Data Controller intends to transfer personal data to a third country or an international organization, as well as the existence or absence of a Commission adequacy decision, or in the case of transfers referred to in Articles 46, 47, or 49(1) second subparagraph of the Regulation, the appropriate and suitable safeguards, as

well as references to the means to obtain a copy of them or the place where they are made available.

(2) In addition to the information mentioned in point 1, the Data Controller shall inform the data subject of the following supplementary information at the time of data collection to ensure fair and transparent processing:

a) The period for which the personal data will be stored, or if this is not possible, the criteria used to determine that period;
b) The right of the data subject to request access to personal data concerning them, to request rectification, erasure, or restriction of processing, and to object to the processing of such personal data, as well as the right to data portability;
c) Where the processing is based on point (a) of Article 6(1) (consent) or point (a) of Article 9(2) (consent), the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
d) The right to lodge a complaint with a supervisory authority;
e) Whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and the possible consequences of failing to provide such data;
f) The fact of automated decision-making, including profiling, as referred to in Articles 22(1) and (4), and, at least in those cases, meaningful information about the logic involved, as well as the significance and expected consequences of such processing for the data subject.

(3) If the Data Controller intends to carry out further processing of the personal data for a purpose other than that for which the data was collected, they shall provide the data subject with information about that other purpose and all relevant supplementary information referred to in paragraph (2) before the further processing.

(4) Points 1-3 do not apply to the extent that the data subject already has the information. (Regulation Article 13)

B) Information to be Provided When Personal Data Is Not Collected from the Data Subject

(1) If personal data has not been collected from the data subject, the data controller shall provide the data subject with the following information:

a) The identity and contact details of the data controller and, if applicable, the representative of the data controller;
b) The contact details of the data protection officer, if available;
c) The intended purposes of processing the personal data, as well as the legal basis for the processing;
d) The categories of personal data concerned;
e) The recipients or categories of recipients of the personal data, if any;
f) If applicable, the fact that the data controller intends to transfer personal data to a third country or international organization, as well as the existence or absence of an adequacy decision by the Commission, or in the case of transfers mentioned in Articles 46, 47, or the second subparagraph of Article 49(1) of the Regulation, the identification of the appropriate

and suitable safeguards, as well as a reference to the means of obtaining a copy of these safeguards or the availability thereof.

(2) In addition to the information mentioned in point 1, the data controller shall provide the following additional information necessary to ensure fair and transparent processing of personal data:

a) The duration for which the personal data will be stored, or, if not possible, the criteria used to determine that duration;
b) If the processing is based on legitimate interests as per Article 6(1)(f) of the Regulation, the legitimate interests pursued by the data controller or a third party;
c) The data subject's right to request from the data controller access to their personal data, the rectification, erasure, or restriction of processing of their personal data, and to object to such processing, as well as the right to data portability;
d) In the case of processing based on consent as per Article 6(1)(a) or Article 9(2)(a) of the Regulation, the right to withdraw consent at any time, which does not affect the lawfulness of processing based on consent before its withdrawal;
e) The right to lodge a complaint with a supervisory authority;
f) The source of the personal data and, if applicable, whether the data comes from publicly accessible sources; and
g) The existence of automated decision-making, including profiling, as referred to in Articles 22(1) and (4) of the Regulation, including at least in those cases the logic involved and the significance and the anticipated consequences of such processing for the data subject.

(3) The data controller provides the information referred to in points 1 and 2:

a) Within a reasonable period after obtaining the personal data, but no later than one month;
b) If the personal data is to be used for communication with the data subject, at the latest at the time of the first communication; or
c) If the data is to be communicated to another recipient, at the latest when the personal data is first disclosed.

(4) If the data controller intends to further process the personal data for a purpose other than that for which the personal data were collected, the data controller shall provide the data subject prior to that further processing with information regarding that other purpose and any relevant further information mentioned in point 2.

(5) The provisions of points 1 to 5 shall not apply if and to the extent that:

a) The data subject already has the information;
b) The provision of the information proves impossible or would involve a disproportionate effort, in particular for processing for archiving purposes in the public interest, for scientific and historical research purposes, or for statistical purposes, in accordance with the conditions and safeguards laid down in Article 89(1) of the Regulation, or if the obligation referred to in paragraph 1 is likely to render impossible or seriously jeopardize the achievement of the objectives of such processing. In such cases, the data controller shall take appropriate measures – including making the information publicly available – to protect the rights, freedoms, and legitimate interests of the data subject;

c) The provision of the information is expressly laid down by Union or Member State law applicable to the data controller, which also provides for appropriate measures to protect the legitimate interests of the data subject; or
d) The personal data must remain confidential under a legal obligation of professional secrecy which is based on Union or Member State law. (Regulation Article 14)

The Right of Access of the Data Subject

(1) The data subject has the right to obtain from the data controller confirmation as to whether or not personal data concerning them are being processed, and, if that is the case, access to the personal data and the following information:

a) The purposes of the processing;
b) The categories of personal data concerned;
c) The recipients or categories of recipients to whom the personal data have been or will be disclosed, including in particular recipients in third countries or international organizations;
d) If applicable, the planned duration of storage of the personal data or, if not possible, the criteria used to determine that duration;
e) The data subject's right to request from the data controller rectification, erasure, or restriction of processing of personal data concerning them, and to object to such processing;
f) The right to lodge a complaint with a supervisory authority;
g) If the data have not been collected from the data subject, any available information as to their source;
h) The existence of automated decision-making, including profiling, as referred to in Articles 22(1) and (4) of the Regulation, and at least in those cases, meaningful information about the logic involved, as well as the significance and the anticipated consequences of such processing for the data subject.

(2) If personal data are transferred to a third country or to an international organization, the data subject has the right to be informed about the appropriate safeguards pursuant to Article 46 of the Regulation relating to the transfer.

(3) The data controller shall provide a copy of the personal data undergoing processing to the data subject. For any further copies requested by the data subject, the data controller may charge a reasonable fee based on the administrative costs. If the data subject submits the request by electronic means, the information shall be provided in a commonly used electronic format, unless the data subject requests otherwise. The right to request a copy shall not adversely affect the rights and freedoms of others. (Regulation Article 15)

The Right to Erasure ('Right to be Forgotten')

(1) The data subject has the right to obtain from the data controller the erasure of personal data concerning them without undue delay, and the data controller is obliged to erase personal data 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 consent on which the processing is based as per Article 6(1)(a) or Article 9(2)(a) of the Regulation, and where there is no other legal ground for the processing;
c) The data subject objects to the processing as per Article 21(1) of the Regulation, and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing as per Article 21(2);
d) The personal data have been unlawfully processed;
e) The personal data have to be erased for compliance with a legal obligation to which the data controller is subject under Union or Member State law;
f) The personal data have been collected in relation to the offer of information society services referred to in Article 8(1) of the Regulation.

(2) If the data controller has made the personal data public and is obliged to erase it under paragraph 1, it shall take reasonable steps, taking available technology and the cost of implementation into account, to inform data controllers that the data subject has requested the erasure of any links to, or copies or replications of, those personal data.

(3) Paragraphs 1 and 2 shall not apply to the extent that the processing is necessary:

a) For exercising the right to freedom of expression and information;
b) For compliance with a legal obligation under Union or Member State law to which the data controller is subject, or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller;
c) For reasons of public interest in the area of public health in accordance with Articles 9(2)(h) and (i) and 9(3) of the Regulation;
d) For archiving purposes in the public interest, scientific or historical research purposes, or for statistical purposes in accordance with Article 89(1), in so far as the right to erasure is likely to render impossible or seriously jeopardize the achievement of the objectives of that processing; or
e) For the establishment, exercise, or defense of legal claims. (Regulation Article 17)

The Right to Restriction of Processing

(1) The data subject has the right to obtain from the data controller restriction of processing where one of the following applies:

a) The data subject contests the accuracy of the personal data, for a period enabling the data controller to verify the accuracy of the personal data;
b) The processing is unlawful, and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;
c) The data 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 defense of legal claims; or
d) The data subject has objected to processing pending the verification whether the legitimate grounds of the data controller override those of the data subject.

(2) Where processing has been restricted under paragraph 1, such personal data shall, except for storage, only be processed with the data subject's consent, for the establishment, exercise or defense of legal claims, for the protection of the rights of another natural or legal person, or for reasons of important public interest of the Union or of a Member State.

(3) A data subject who has obtained restriction of processing shall be informed by the data controller before the restriction of processing is lifted. (Regulation Article 18)

The Right to Data Portability

(1) The data subject has the right to receive the personal data concerning them, which they have provided to a data controller, in a structured, commonly used, and machine-readable format, and has the right to transmit those data to another data controller without hindrance from the data controller to which the personal data have been provided, where:

a) The processing is based on consent as per Article 6(1)(a) or Article 9(2)(a) of the Regulation, or on a contract as per Article 6(1)(b); and
b) The processing is carried out by automated means.

(2) In exercising their right to data portability under paragraph 1, the data subject has the right to have the personal data transmitted directly from one data controller to another, where technically feasible.

(3) The exercise of the right referred to in paragraph 1 shall be without prejudice to the right to erasure. That right shall not apply to the processing of personal data necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller.

(4) The provisions of paragraph 1 shall not apply to processing which is not based on consent or on a contract. (Regulation Article 20)

The Right to Object

(1) The data subject has the right to object at any time, on grounds relating to their particular situation, to the processing of personal data concerning them based on Article 6(1)(e) (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) or Article 6(1)(f) (processing necessary for the purposes of legitimate interests pursued by the controller or a third party), including profiling based on those provisions. In this case, 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 defense of legal claims.

(2) If the processing of personal data is for direct marketing purposes, the data subject has the right to object at any time to the processing of personal data concerning them for such marketing, including profiling to the extent that it is related to such direct marketing.

(3) If the data subject objects to the processing of personal data for direct marketing purposes, the personal data may no longer be processed for such purposes.

(4) The right referred to in paragraphs 1 and 2 shall be explicitly brought to the attention of the data subject at the latest at the time of the first communication with them, and the information regarding this right must be presented clearly and separately from any other information.

(5) In the context of the provision of information society services and notwithstanding Directive 2002/58/EC, the data subject may exercise the right to object through automated means using technical specifications.

(6) If personal data are processed for scientific and historical research purposes or for statistical purposes in accordance with Article 89(1), the data subject has the right to object to the processing of personal data concerning them on grounds relating to their particular situation, unless the processing is necessary for the performance of a task carried out in the public interest. (Regulation Article 21)

Automated Decision-Making in Individual Cases, Including Profiling

(1) The data subject has the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning them or similarly significantly affects them.

(2) The right in paragraph 1 shall not apply in the following cases:
a) The decision is necessary for entering into, or performance of, a contract between the data subject and the controller;
b) The decision is authorized by Union or Member State law applicable to the controller, which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or
c) The decision is based on the data subject's explicit consent.

(3) In the cases referred to in points (a) and (c) of paragraph 2, the controller shall implement suitable measures to safeguard the data subject's rights, freedoms, and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express their point of view, and to contest the decision.

(4) Decisions referred to in paragraph 2 shall not be based on special categories of personal data referred to in Article 9(1), unless Article 9(2)(a) or (g) applies and suitable measures are in place to safeguard the data subject's rights, freedoms, and legitimate interests. (Regulation Article 22)

Restrictions

(1) Union or Member State law may provide for legislative measures that restrict the scope of the rights and obligations provided for in Articles 12 to 22 and Article 34, provided that such measures respect the essence of the fundamental rights and freedoms and are a necessary and proportionate measure in a democratic society for:
a) National security;

b) Defence;
c) Public security;
d) The prevention, investigation, detection, or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;
e) Important objectives of general public interest of the Union or of a Member State, in particular important economic or financial interests of the Union or of a Member State, including monetary, budgetary, and taxation matters, public health, and social security;
f) The independence of the judiciary and the judicial proceedings;
g) The prevention, investigation, detection, or prosecution of ethical violations in regulated professions and the related proceedings;
h) Oversight, investigation, or regulatory activities related to the performance of public functions in cases referred to in points (a) to (e) and (g);
i) The protection of the data subject or the rights and freedoms of others;
j) The establishment, exercise, or defense of legal claims.

(2) Legislative measures referred to in paragraph 1 shall include provisions that specify at least:
a) The purposes of the processing or the categories of processing;
b) The categories of personal data;
c) The scope of the restrictions introduced;
d) Safeguards to prevent abuse or unlawful access to or transfer of personal data;
e) The identification of the controller or the categories of controllers;
f) The duration of storage and the applicable safeguards, taking into account the nature, scope, and purposes of the processing or categories of processing;
g) Risks to the rights and freedoms of data subjects; and
h) The right of data subjects to be informed about the restriction, unless this would adversely affect the purpose of the restriction. (Regulation Article 23)

Notification of Data Subjects about Data Breaches

(1) If a personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall notify the data subject of the personal data breach without undue delay.

(2) The notification referred to in paragraph 1 shall describe in clear and plain language the nature of the personal data breach and contain at least the information and measures referred to in Article 33(3)(b), (c), and (d).

(3) The data subject does not need to be informed in accordance with paragraph 1 if any of the following conditions are met:
a) The controller has implemented appropriate technical and organizational protection measures, and those measures were applied to the personal data affected by the breach, in particular those that render the data unintelligible to any person not authorized to access it, such as encryption;
b) The controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of the data subjects is no longer likely to materialize; or
c) It would involve a disproportionate effort. In such cases, the data subjects shall be informed through publicly available means or similar measures that ensure effective communication to the data subjects.

(4) If the controller has not yet notified the data subject of the personal data breach, the supervisory authority may require the data subject to be notified after assessing whether the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, or determine whether any of the conditions in paragraph 3 are met. (Regulation Article 34)

Notification of the Supervisory Authority about Data Breaches

(1) The controller shall notify the supervisory authority of a personal data breach without undue delay and, where feasible, no later than 72 hours after becoming aware of it, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. If notification is not made within 72 hours, the controller shall provide reasons for the delay when notifying.

(2) The notification referred to in paragraph 1 shall:

- Describe the nature of the personal data breach, and, where possible, the categories and approximate number of data subjects concerned, as well as the categories and approximate number of personal data records concerned;
- Provide the name and contact details of the data protection officer or other contact point where more information can be obtained;
- Describe the likely consequences of the personal data breach;
- Describe the measures taken or proposed to be taken by the controller to remedy the personal data breach, including, where appropriate, measures to mitigate any possible adverse effects.

(3) If it is not possible to provide the information at the same time, it may be provided in phases without undue further delay.

(4) The controller shall maintain a record of personal data breaches, comprising the facts relating to the breaches, their effects, and the remedial measures taken.

Right to Lodge a Complaint with the Supervisory Authority

(1) Without prejudice to other administrative or judicial remedies, any affected individual has the right to lodge a complaint with a supervisory authority—particularly in the member state of their usual residence, workplace, or the place where the alleged infringement occurred—if they believe that the processing of their personal data violates this regulation.

(2) The supervisory authority to which the complaint is submitted is obliged to inform the complainant about the developments in the proceedings related to the complaint and its outcome, including that the complainant is entitled to seek judicial remedies under Article 78 of the Regulation. (Regulation Article 77)

Right to Effective Judicial Remedy Against a Supervisory Authority

(1) Without prejudice to other administrative or non-judicial remedies, every natural and legal person has the right to an effective judicial remedy against a legally binding decision of the supervisory authority concerning them.

(2) Without prejudice to other administrative or non-judicial remedies, any affected individual has the right to an effective judicial remedy if the supervisory authority competent under Articles 55 or 56 of the Regulation does not address the complaint or does not inform the affected individual of the developments in the proceedings related to the complaint lodged under Article 77 within three months.

(3) Proceedings against a supervisory authority must be initiated before the court of the member state where the supervisory authority is established.

(4) If proceedings are initiated against a decision of the supervisory authority for which the Board previously issued an opinion or decision under the consistency mechanism, the supervisory authority must submit that opinion or decision to the court. (Regulation Article 78)

Right to Effective Judicial Remedy Against the Data Controller or Processor

(1) Without prejudice to available administrative or non-judicial remedies—including the right to lodge a complaint with a supervisory authority under Article 77 of the Regulation—every affected individual is entitled to an effective judicial remedy if they believe that the processing of their personal data has infringed their rights under this Regulation.

(2) Proceedings against the data controller or processor must be initiated before the court of the member state where the data controller or processor has its establishment. Such proceedings may also be initiated before the court of the member state where the affected individual has their habitual residence, unless the data controller or processor is a public authority acting in the exercise of its public powers. (Regulation Article 79)

Chapter VII
SUBMISSION OF THE REQUEST BY THE AFFECTED INDIVIDUAL, ACTIONS BY THE DATA CONTROLLER

(1) The data controller shall inform the affected individual, without undue delay, but in any case within one month of receiving the request, about the assessment of their request to exercise their rights and about any measures taken as a result.

(2) If necessary, taking into account the complexity of the request and the number of requests, this deadline may be extended by a further two months. The data controller shall inform the affected individual about the extension of the deadline, indicating the reasons for the delay, within one month of receiving the request.

(3) If the affected individual submitted the request electronically, the information shall be provided electronically where possible, unless the affected individual requests otherwise.

(4) If the data controller does not take action on the request of the affected individual, they shall inform the affected individual without delay, but at the latest within one month of receiving the request, about the reasons for not taking action, as well as about the possibility for the affected individual to lodge a complaint with a supervisory authority and to exercise their right to judicial remedies.

(5) The data controller shall provide the information and notification regarding the affected individual's rights under Articles 13 and 14 of the Regulation (Articles 15-22 and 34) free of charge. If the affected individual's request is manifestly unfounded or excessive, particularly due to its repetitive nature, the data controller may, considering the administrative costs of providing the requested information or notification or taking the requested action:

a) charge a fee, or

b) refuse to act on the request.

(6) If the data controller has reasonable doubts regarding the identity of the natural person submitting the request, they may request additional information necessary to confirm the identity of the affected individual—until reasonable doubts are credibly and satisfactorily resolved, the data controller is entitled to refrain from taking action.

Chapter VIII
FINAL PROVISIONS

1. Establishment and Amendment of the Notification

The establishment and amendment of the Notification—following the approval and publication of the new or amended rules of the Company's Data Management Policy—shall be the responsibility of the Company's senior executive.

NoBoVersum Closed Company Limited by Shares