

PRIVACY NOTICE

INTRODUCTION

The purpose of this notice is to enable the **Centre for Long-Term Sustainability LLC** (hereinafter referred to as the **Company**), as controller, to inform data subjects adequately about the material circumstances of the processing and the rights of the data subjects and to comply with the obligations to provide information under Articles 13 and 14 of the Regulation¹.

This notice is continuously available on the Company's website (www.bc4ls.com) and, upon request, the Company will send it to the data subjects directly as well.

CHAPTER I NAME OF CONTROLLER

The publisher of this information and the Controller:

Company name: Centre for Long-Term-Sustainability LLC

Registered Office: 1014 Budapest, Úri utca 72., Hungary

Company register number: 01-09-384747

Tax number: 29256994-1-41

Representative during the processing activity:

Email: adel.modensieder@bc4ls.com

Website: www.bc4ls.com

(hereinafter: Company)

CHAPTER II Principles relating to processing of data

The following principles shall apply to all stages of processing, and their maximum enforcement shall be ensured. The Company, as controller, shall be responsible for enforcing the following principles of processing at all times based on the **principle of accountability**.

lawfulness, fairness and transparency: data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject;

purpose limitation: personal data shall be collected for specified, explicit and legitimate purposes only, and the collected data shall not be used in any manner that is incompatible with or different from the initial purposes;

data minimisation: the data processed shall be adequate, relevant and limited to what is necessary for the purposes for which they are processed;

accuracy: the data processed shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, is erased or rectified without delay;

storage limitation: personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed;

integrity and confidentiality: personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures;

Foundations

The Company shall not perform any processing activities.

¹ REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL (27 April 2016) on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC

The Company shall aim to obtain all personal data it processes directly from the data subject. No data protection officer shall be appointed at the Company pursuant to Article 37 (1) of the Regulation and Article 25/L of Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information (hereinafter: Info Act), as the conditions set out therein do not apply to the Company as controller.

The Company does not carry out any processing activities in relation to personal data within the meaning of Article 35 of the Regulation. The Company shall carry out a data protection impact assessment when possibly planning any processing activity pursuant to Article 35 (1), in particular Paragraph (3) of the Regulation.

CHAPTER III Legal grounds for processing

The processing of personal data is lawful only if and to the extent that at least one of the following legal grounds for processing applies ***in accordance with Article 6 of the Regulation***:

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

The legal basis for the actually performed processing operations by the Company is the consent of the data subject, the performance of a contract or legal obligation, or the assertion of the legitimate interest of the Company as controller. The termination of one of the legal grounds for processing does not preclude the processing of the data on another legal ground.

CHAPTER IV Processing based on the consent of the data subject

The consent of the data subject may serve as the basis for processing when no legitimate grounds for the processing of personal data for a specific purpose is provided by the performance of a contract, the fulfilment of a legal obligation or the assertion of a legitimate interest.

In the case of processing based on consent, the data subject's consent to the processing of his or her personal data must be requested on a form.

The consent shall cover all processing activities carried out for the same purpose or purposes. If the processing serves several purposes at the same time, the consent must be given for all processing purposes for which the data is processed.

At the Company, consent cannot be given in a written declaration that also applies to other matters. The Company shall not subject the conclusion or performance of a contract to the condition of giving consent to the processing of personal data that is not necessary for the performance of that contract. The data subject may withdraw his or her consent by any statement communicated to the Company by e-mail or to an employee acting within the scope of the Company's activities by verbal communication. In the event of verbal withdrawal of consent, the employee shall give a written notice to the current managing director of the Company, providing all information necessary for the

termination of processing as soon as possible, in particular the data subject's name, the date of withdrawal and the scope of data affected by the withdrawal.

If the personal data has been collected with the consent of the data subject, the controller may, unless otherwise provided by law, process the collected data without further special consent in order to fulfil the legal obligation applicable to the controller.

CHAPTER V Processing based on the performance of a legal obligation

1.) The processing based on the performance of a legal obligation is independent of the consent of the data subject, since the processing is determined by law. In such cases, the data subject must be informed of the compulsory nature of the processing before the processing starts and clear and detailed information must be provided on all the facts relating to the processing of his or her data, in particular the purposes and legal basis for the processing, the identity of the controller and the processor, the duration of the processing, the fact that the controller is processing the data subject's personal data under a legal obligation and the persons who may access the data. The information must also cover the rights and remedies of the data subject in relation to the processing. In the case of mandatory processing, the information may also be provided by publishing a reference to the legal provisions containing the aforementioned information.

2.) The Company processes the data of natural persons who interact with it as employees (see details in Chapter V), customers, suppliers, sponsors or scholarship holders for the purposes of fulfilling legal obligations, tax and accounting obligations (accounting, taxation), for the purposes of statutory charge obligations and for the purposes of claiming social security cash benefits. The scope of the data processed is defined by Article 167 of Act C of 2000 on Accounting, Articles 169 and 202 of Act CXXVII of 2017 on Value Added Tax, Act CXVII of 1995 on Personal Income Tax and certain rules of law providing for social security contribution obligations and benefits. The period of storage of personal data is 8 years after the termination of the legal relationship giving rise to the legal grounds.

Persons entitled to know the personal data under this point 2.) are the employees and processors performing tax, accounting, payroll and social security tasks. The personal data under this point 2.) will be transferred to the respective entities in contractual relation with the Company at all times for the performance of accounting (OPTIMA Befektetési Zrt.) and payroll (RUHAN Kft.) tasks, which are also the recipients of the personal data. Employees and data processors performing tax, accounting, payroll and social security tasks at the recipients have the right to access the personal data under this point 2.).

CHAPTER VI Processing of data (CVs) of job applicants

The Company processes the content of the CVs provided by job applicants and any other personal information provided during the application process.

The scope of personal data that can be requested from applicants: name of the natural person, date of birth, address, qualification data, data on previous employment, other relevant experience, photo, telephone number, e-mail address.

The purpose of the processing of personal data: to assess the application and conclude an employment contract with the selected person.

Legal basis of processing: the legitimate interest of the Company.

Recipients of the personal data: the person exercising the employer's rights in the Company.

The period of storage of personal data: Until the conclusion of an employment contract with the selected candidate.

CHAPTER VII Processing related to contracts

➤ **Natural person and sole trader contractual partners**

The Company shall, under the title of performing a contract and for the purposes of the conclusion, performance or termination of a contract, process the name, name at birth, date of birth, mother's name, address, tax identification code, tax number, number of the sole trader's identity card, number of personal identity card, address, address of registered office, address of place of business, telephone number, e-mail address, bank account number, social security number of the natural person contracted by the Company as customer, supplier, sponsored person, scholarship holder, etc.

Recipients of the personal data: the employee of the Company appointed to take part in performing the contract. In order to fulfil the contractual and statutory obligations for tax, accounting and payroll services, the personal data necessary for the fulfilment of these obligations are transferred to the Company's tax, accounting, payroll and social security service provider as processor.

The period of storage of personal data: 5 years after the termination of the contract.

Legal grounds for processing personal data: performance of a contract and legal obligations.

The natural person data subject must be informed when the contract is concluded that the purpose of processing is the performance of the contract.

➤ **Contracts concluded with organisations**

The Company shall process the personal data of the contact person and representative appointed by the entities that have contractual relations with the Company as a customer or supplier which have come to its knowledge in the course of the performance of the contract for the purposes of the contract.

The scope of personal data that may be processed: name, telephone number and e-mail address of the natural person.

Purpose of processing personal data: performing the contracts of the Company.

Legal grounds for processing personal data: performing the contract.

Recipients of personal data: the employee of the Company appointed to take part in concluding and performing the contract. In order to fulfil the contractual and statutory obligations for tax, accounting and payroll services, the personal data necessary for the fulfilment of these obligations are transferred to the Company's service providers at all times for accounting (OPTIMA Befektetési Zrt.) and payroll (RUHAN Kft.) services, as processors. Employees and data processors performing tax, accounting, payroll and social security tasks have the right to get acquainted with the personal data.

The period of storage of personal data: 5 years after the termination of the contractual business relationship.

The data subject shall be informed in a verifiable manner of the circumstances of the processing described in this point by the employee of the Company designated for the conclusion and performance of the contract.

CHAPTER VIII Data processing on the Company's website

The Company uses cookies on its website **bc4ls.com** in order to enhance user experience. In general, cookies facilitate the use of the website, help the website to provide users with a real web experience and an effective source of information, and enable the website operator to monitor the functioning of the site, prevent abuse and ensure the smooth and adequate provision of services on the website.

Cookies used on the website <https://bc4ls.com>

Cookies are necessary to allow visitors to browse the website and to make smooth and full use of its functions and the services available through it, including, but not limited to, the memorisation of actions taken by the visitor on the pages during a visit.

The website **<https://bc4ls.com>** collects and processes the following data about the visitor and the device used for browsing:

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

Accepting the use of cookies is not mandatory, but certain website features or services may not function properly without cookies.

The cookies used on the website are not in themselves suitable for identifying the user, i.e. the above-mentioned data created and processed from a technical point of view cannot be identified, the duration of the cookie's processing is limited to the actual visit of the visitor, and this type of cookie is automatically deleted from the visitor's computer at the end of the session or when the browser is closed.

Scope of the data processed: AVChatUserId, JSESSIONID, portal referer.

The legal grounds for this processing is Article 13/A (3) of Act CVIII of 2001 on Certain Aspects of Electronic Commerce Services and Information Society Services (hereinafter: Electronic Commerce Act).

Purpose of processing: to ensure the proper functioning of the website.

Detailed information on how cookies work on this website can be found at the following addresses:

WordPress: <https://wordpress.org/support/article/cookies/>

WooCommerce: <https://docs.woocommerce.com/document/woocommerce-cookies/>

GoogleAnalytics: <https://developers.google.com/analytics/devguides/collection/analyticsjs/cookie-usage?hl=hu>

FacebookPixel: <https://www.facebook.com/business/help/471978536642445?id=1205376682832142>

Hotjar: <https://help.hotjar.com/hc/en-us/articles/115011789248-Hotjar-Cookies>

The html code of **<https://bc4ls.com>** operated by the Company contains links from and to external servers independent of the Company. The server of the external service provider is directly connected to the computer of the user concerned. The providers of these links are able to collect user data (e.g. IP address, data related to the browser and the operating system, address of the visited page and the time of visit) due to the direct connection to their server and the direct communication with the user's browser.

The contents possibly personalised for the Data Subject are served by the server of the external service provider.

The independent measurement and auditing of traffic and other web analytics data of the **<https://bc4ls.com>** website is supported by the server of Google Analytics as external service provider. More information about the processing performed by www.google.com/analytics is available at <http://www.google.com/intl/hu/policies/>.

CHAPTER IX Processing based on the data subject's voluntary participation

Applications from researchers and other contributors

One of the purposes of the Company is to create a community of researchers.

On the website <https://bc4ls.com>, under the "Apply" menu, or via email sent to the Company, it is possible for the person concerned to submit an application if he or she wishes to participate as a researcher in the professional and research activities of the Company.

The following data must be provided: name, contact details (e-mail address and telephone number) and, for the purposes of assessing the application, the CV of the applicant with the information content voluntarily determined by the applicant.

The purpose of the processing is to assess the data subject's application to join as a researcher or other contributor, and the legal grounds for the processing is the data subject's voluntary consent and legitimate interest. The recipient of the data is the employee responsible for the administrative processing of job applications and the Advisory Board of the Company which assesses the merits of the applications. Duration of data processing: until the job application has been assessed, but no later than 2 years from the date of sending the application during which period the applicant may be selected at any time.

In case the applicant requests the termination of data processing, it can be notified to the e-mail address adel.modensieder@bc4ls.com, which the Company will comply with by deleting the documents of the submitted application within 8 days from the receipt of the e-mail.

Newsletter function

The data subject can subscribe to the newsletter function by going to the webpage <https://bc4ls.com> and clicking on "Subscribe". This allows the data subject to express his or her wish to receive the electronic newsletter prepared periodically by the Company to his or her e-mail address. On this ground, the Company will process the name and e-mail address of the data subject. The legal basis for the processing the data subject's voluntary consent and legitimate interest. The recipient of data is the employee compiling the mailing list for sending the newsletters. The Company will process the name and e-mail address of the data subject until they indicates that they no longer wish to receive the newsletter by clicking on the "Unsubscribe" link in the letter containing the newsletter or by sending a letter to the Company to the e-mail address bc4ls@bc4ls.com.

Application for a scholarship program

The Company creates a scholarship program and manages the CVs submitted by the applicants and the data provided therein and disclosed by the applicants.

The purpose of data management is to enable the Company to select from among the applicants those who shall receive a scholarship.

The period of data management is 2 (two) years from the submission of the application, during which the data subject may be selected among the scholarship holders at any time based on its application.

The addressee of the data management is the employee of the Company managing the scholarship program, as well as the Advisory Board of the Company, which evaluates the merits of the applications. The legal basis for data processing is the voluntary consent and legitimate interest of the data subject.

If the data subject requests the termination of the data processing, it can indicated at any time at adel.modensieder@bc4ls.com, and the Company will comply with the request by deleting the documents of the submitted application within 8 days from the receipt of the e-mail.

CHAPTER X PHOTO AND VIDEO RECORDING AT THE COMPANY'S REGISTERED SEAT

Means of personal and property protection

At the Company's registered seat, in the Building at 72 Úri utca, Budapest, its operator operates a camera surveillance system installed in the entire indoor area of the facility. The purpose of operating the camera surveillance system is to protect human life, physical integrity, personal liberty and property. The camera surveillance system also enables image and sound recording, on the basis of which the behaviour of the data subjects in the facility is also recorded as personal data. No recording shall be made in a room where observation would violate human dignity, especially in toilets.

The legal basis for this data management is the legitimate interest of the owner of the Building in the protection of property and the occupants of the Building in the protection of personal and property.

Information on the use of the camera surveillance system on the site of the facility shall be provided in a clearly visible and legible manner at each entrance, together with the availability of this data management policy.

Recorded recordings are available at the facility during storage period and will not be transmitted if not requested for further use.

During the registration as a condition of participation in the event held on the property, the data subject consents to the processing of the following personal data:

- name,
- e-mail address.

The purpose of data management is to identify the persons entering the property. The recipient of the data is the people performing personal and property security services in the property at all times. Duration of data management: 5 days after participating in the program concerned.

The Company is not a data controller with respect to these data processes. With regard to personal data processed in connection with the protection of persons and property, Raw Facility Management Kft. (1024 Budapest, Fény u. 16., company registration number: 01-09-340669, e-mail: rawdevelopment@gmail.com) is the Data Controller, so this data management this Company's privacy policy, which is available on site, shall govern.

Documentation of the Company's programs and events

The Company is entitled to document the events organized at the entire indoor area of the Building, as the facility located at Budapest Úri u. 72. by recording images and videos. These images and video recordings (hereinafter together: recordings) are recorded using a non-installed technical system, with the assistance of the person recording the present recording.

The purpose of the recordings is to enable the Company to document its activities and report on its website and social media interfaces. The Company may later use the recordings to create an album, archive or any other printed or digital document or film.

Information on the possibility of recording shall be provided in a clearly visible conspicuous place next to each entrance to the premises of the facility, together with an indication of the contact details of this data management policy.

The legal basis of this data management is the enforcement of the legitimate interests of the Company, which the data subject acknowledges and accepts by entering the territory of the facility on the basis of the information.

The Company provides the data subject with the opportunity to indicate to the person making the record that he or she wishes not to be recorded, such a request shall be accepted and fulfilled by the person making the recording.

The data subject may initiate the deletion or deactivation of recordings at the e-mail address bc4ls@bc4ls.com, on which he or she can be identified and thus the recording constitutes a personal data.

The Company shall contact the data subject with such an indication within 24 hours on working days, otherwise on the next working day and shall delete or make them inaccessible within 8 hours from the identification of the affected data.

If the data subject's request for cancellation or inaccessibility as described above is made in such a way that the recordings (personal data) are identified together with the request, the Company will comply with the data subject's request within 24 hours of its receipt, otherwise on the next business day.

In the absence of the above request, the period of storage of personal data will last until the existence of such a legitimate interest of the Company.

The recipient of the recordings, thus personal data, is the employee of the Company entrusted with the organization of the given event.

CHAPTER XI Processors

The Company does not process data controlled by others.

Processors in a contractual relationship with the Company as principal:

Accounting service provider:

Company name: Optima Befektetési Zrt.

Registered Office: 1013 Budapest, Döbrentei utca 2., Hungary

Company register number: 01-10-048464

Tax number: 25294848-2-41

Representative: Dr Zoltán Fekete, CEO

Email: info@optimabudapest.hu

Payroll service provider:

Company name: RUHAN Számviteli és Munkaügyi Kft.

Registered Office: 2092 Budakeszi, Knáb János utca 38., Hungary

Company register number: 13-09-134511

Tax number: 11735036-2-13

Representative: Anikó Varga, Managing Director

Email: anikoridacs@t-online.hu

CHAPTER XII Data security measures

The Company shall take the technical and organisational measures necessary to enforce the provisions of the Regulation and the Info Act in order to ensure the security of personal data for all purposes and legal grounds.

In order to ensure an adequate level of security of the personal data processed, the Company takes technical and organisational measures appropriate to the level of risk posed by the processing in order to safeguard the fundamental rights of data subjects.

In designing and implementing these measures, the Company shall take into account all the circumstances of the processing, in particular the state of the art, the cost of implementing the measures, the nature, scope and purposes of the processing, and the risks of varying likelihood and severity to the rights of data subjects posed by the processing.

The Company will ensure through data security measures:

- the denial of access by unauthorised persons to the means used for the processing by storing the assets in a secure place protected from unauthorised persons and/or by keeping them in the custody of employees;
- the prevention of unauthorised reading, copying, modification or removal of data media;
- the prevention of unauthorised input of personal data into the processing system and unauthorised access, modification or deletion of personal data stored in the processing system;
- the prevention of the use of processing systems by unauthorised persons via data transmission equipment;
- that persons authorised to use the system have access only to the personal data necessary for the performance of their tasks;
- the ability to verify and establish, by means of logs and verifications, the recipients to which the personal data has been or may be transmitted or made available by means of a data transmission installation;
- the ability to verify and establish ex post, through logging, which personal data has been entered into the processing system by whom and at what time;
- the prevention of unauthorised access to, copying, modification or deletion of personal data during transmission or transport of the data carrier;
- that the processing system can be restored in the event of a malfunction; and
- that the processing system is operational, that any errors in its operation are reported in the form of logs and employee reports, and that the personal data stored cannot be altered even by the false operation of the system.

The Company shall take appropriate measures to protect the personal data it processes against accidental or unlawful destruction, loss, alteration, damage and unauthorised disclosure or access.

The Company, as employer, shall require all employees to comply with this policy in order to protect personal data. Personal data may be accessed by employees of the Company in accordance with this policy.

The Company shall protect its IT system serving also for the storage of personal data with firewall and virus protection. The information technology system operated by the Company shall ensure that personal data is accessed only for the intended purpose, under controlled conditions and only by those persons who need to have access to it in order to perform their tasks.

Only the competent administrators may have access to the documents under processing. The Company shall keep the documents containing personnel, payroll, labour and other personal data securely locked, and only the employee whose job is to control and forward these data to the processor (Chapter V) may have access to them.

The Company shall ensure the adequate physical protection of data and the media and documents carrying it.

Accesses and access attempts shall be logged on IT systems and continuously analysed in order to detect and handle personal data breaches without delay.

CHAPTER XIII Handling personal data breaches

Personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

The prevention and handling of personal data breaches and compliance with the relevant legal requirements are the responsibility of the Company's Managing Director at all times.

If any employee of the Company becomes aware that a personal data breach has occurred or is likely to occur, they must notify the Company's Managing Director.

The detection of a personal data breach can be reported to the e-mail address of the Managing Director at all times (adel.modensieder@bc4ls.com).

In the first instance, the data subjects and employees of the Company have the right to report a personal data breach, but any personal data breach shall be obligatorily and properly investigated irrespective of the reporting person.

In the event of a notification of a personal data breach, the Company's Managing Director shall investigate the notification without delay. In doing so, the Managing Director determines the facts and decides whether it is a real incident or a false alarm.

The decision on the merits shall state:

- the time and place of the incident;
- the description, circumstances and effects of the incident;
- the scope and quantity of data compromised in the incident;
- the range of data subjects affected by compromised data;
- the description of the measures taken to deal with the incident;
- a description of the measures taken to prevent, remedy or reduce the damage.

In the event of a personal data breach, the affected systems, persons and data shall be contained and separated, and care shall be taken to collect and preserve evidence on the occurrence of the breach. After that, damage restoration and return to lawful operation can begin.

Recording of personal data breaches

Records of personal data breaches must be kept, including:

- a) the scope of affected personal data;
- b) the scope of data subjects affected by the personal data breach;
- c) the time of the personal data breach;
- d) the circumstances and effects of the personal data breach;
- e) the measures taken to remedy the data breach;
- f) other data specified in the legislation providing for the processing.

The data regarding personal data breaches in the register must be kept for 5 years from the date of the decision.

CHAPTER XIV Rights of the data subject

The data subject's right to adequate information

The Company will keep this Privacy Policy available at its headquarters and will send it to the data subject individually upon request.

Right to prior information

The data subject has the right to be informed of the facts and information relating to the processing before the processing starts. (See details in Chapter XI)

If the Company intends to carry out further processing of personal data for purposes other than those for which it was collected, the data subject must be informed of this different purpose and of any additional information relevant as set out above before further processing.

Right of access by the data subject

The data subject shall be entitled to receive feedback from the Company as to whether or not his or her personal data is being processed and, if such processing is taking place, to have access to the personal data and information relating to the processing.

Right to rectification

The data subject shall have the right to obtain, at his or her request and without undue delay, rectification by the Controller of inaccurate personal data relating to him or her. Taking into account the purpose of the processing, the data subject has the right to request the completion of incomplete personal data.

Right to erasure ('right to be forgotten')

The data subject shall be entitled to have the personal data relating to him or her erased by the Company without undue delay at his or her request if

- a) the personal data is no longer necessary for the purposes for which it was collected or otherwise processed;
- b) the data subject withdraws the consent on which the processing is based and there is no other legal basis for the processing;
- c) the data subject objects to the processing and there are no overriding legitimate grounds for the processing;
- d) the personal data has been unlawfully processed;
- e) the personal data must be erased in order to comply with a legal obligation under Union or Member State law applicable to the Company;
- f) the personal data was collected in connection with offering services related to information society.

Right to restriction of processing

The data subject shall have the right to obtain, at his or her request, the restriction of processing by the Controller if

- a) the data subject contests the accuracy of the personal data, in which case the restriction shall apply for the period of time necessary to allow the Company to verify the accuracy of the personal data;
- b) the processing is unlawful and the data subject opposes the erasure of the data but requests instead the restriction of their use;
- c) the Company no longer needs the personal data for the purposes of processing, but the data subject requires it for the submission, exercise or defence of legal claims; or
- d) the data subject has objected to the processing; in this case, the restriction shall apply to the period until it is established whether the legitimate grounds of the Company prevail over the legitimate grounds of the data subject.

The Controller shall inform each recipient to whom the personal data has been disclosed of any rectification, erasure or restriction of processing, unless this proves impossible or involves a disproportionate effort. Upon request, the Company will inform the data subject of these recipients.

Right to object

The data subject shall have the right to object at any time, on grounds relating to his or her particular situation, to the processing of his or her personal data necessary for the performance of a task carried out in the public interest or in the exercise of official authority, or based on the legitimate interests of

the Controller or a third party. In this case, the Company may no longer process the personal data, unless it can demonstrate compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject, or which are related to the submission, enforcement or protection of legal claims.

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

Restrictions

Union or Member State law applicable to the Company or its contracted processors may, by legislative measures, limit the scope of certain rights and obligations set out in the Regulation for the reasons set out therein.

Communication of a personal data breach to the data subject

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

The information shall clearly and plainly describe the nature of the personal data breach, its possible consequences and the measures taken or envisaged to remedy the personal data breach, including, where appropriate, the measures to mitigate any possible adverse consequences of the personal data breach.

The information of the data subject may be omitted if:

- a) the Company has implemented appropriate technical and organisational protection measures and these measures have been applied to the data affected by the personal data breach, in particular measures, such as the use of encryption, which render the data unintelligible to persons not authorised to access the personal data;
- b) the Company has taken additional measures following the personal data breach to ensure that the high risk to the rights and freedoms of the data subject is no longer likely to materialise;
- c) the provision of information would require a disproportionate effort; in such cases, the data subjects shall be informed by means of publicly disclosed information or by a similar measure ensuring that the data subjects are informed in an equally effective manner.

Right to lodge a complaint with the supervisory authority (right to official remedy)

The data subject has the right to lodge a complaint with a supervisory authority if he or she considers that the processing of personal data relating to him or her infringes the rules of the Regulation.

The data subject shall have the right to an effective judicial remedy against a legally binding decision of the supervisory authority concerning him or her, or if the supervisory authority does not deal with the complaint or does not inform the data subject within three months of the procedural developments concerning the complaint lodged or of the outcome of the complaint.

details of the supervisory authority:

Hungarian National Authority for Data Protection and Freedom of Information

<http://naih.hu>

Mailing address: 1530 Budapest, Pf. 5., Hungary

Email: ugyfelszolgalat@naih.hu

Telephone: +36 (1) 391-1400

Right to an effective judicial remedy against the controller or processor

Every data subject has the right to an effective judicial remedy if he or she considers that his or her rights have been infringed as a result of the processing of his or her personal data not in accordance with the Regulation.

CHAPTER XV Submission of the data subject's request

The Company, as controller, shall inform the data subject of the measures taken in response to his or her request to exercise his or her rights without undue delay, but no later than 8 days from the receipt of the request.

The data subject may submit his or her request electronically to the address adel@modensieder@bc4ls.com. When the data subject has submitted the request by electronic means, the information shall be provided by electronic means where possible, unless the data subject requests otherwise.

Requests may be made on paper or in person at the registered office of the Company or by post addressed to its registered office.

If the Company has reasonable doubts as to the identity of the natural person submitting the request, it may request additional information to confirm the identity of the data subject.
