PRIVACY POLICY OF INHUS GROUP OF COMPANIES

This privacy policy of INHUS group of companies (hereinafter - the **Privacy Policy**) is intended for entities and persons who purchase goods, use the Company‘s services, supply goods or provide services to the Company from the INHUS group of companies (hereinafter any of the INHUS group companies – the **Company**, the **Data Controller** or **We**), visit the Company‘s territory or premises, are interested in employment at the Company or visit the following websites:

- www.inhus.eu
- www.inhusengineering.eu
- www.inhusprefab.eu
- www.inhusconstruction.eu
- www.scandikran.se (hereinafter any of the aforementioned websites - the **Website**).

DATA CONTROLLER

The data controller:

- INHUS Group, UAB, company number 302664113, registered headquarters address – Žarijų g. 6, Vilnius, LT, business address – Žarijų g. 6A, Vilnius, Lithuania;
- INHUS, UAB, company number 302863631, registered headquarters address – Žarijų g. 6, Vilnius, LT, business address – Žarijų g. 6A, Vilnius, Lithuania;
- INHUS Prefab, UAB, company number 121559766, registered headquarters address – Žarijų g. 6, Vilnius, LT, business address – Žarijų g. 6A, Vilnius, Lithuania;
- INHUS Construction, UAB, company number 302891837, registered headquarters address – Žarijų g. 6, Vilnius, LT, business address – Žarijų g. 6A, Vilnius, Lithuania;
- INHUS Engineering, UAB, company number 301545597, registered headquarters address – Žarijų g. 6, Vilnius, LT, business address – Žarijų g. 6A, Vilnius, Lithuania;
- INHUS AB, company number Articles 556866-6977, address c/o ECIT Services AB, Box 30080, 104 25, Stockholm, Sweden;
- INHUS, AS, company number 913144031, address c/o Merisma AS, St. Olavs gate 24, 0166, Oslo, Norway;
- INHUS LIMITED, company number 12429993, address Mills & Reeve Llp, 1 City Square, Leeds, West Yorkshire, United Kingdom LS1 2ES;
- INHUS Engineering Oy, company number 3164704-2, address c/o Properta Asianajotoimisto Oy Unioninkatu 7 B 17, 00130, Helsinki, Finland;
- UAB Scandikran, company number 305745435, address Žarijų g. 6A, Vilnius, Lithuania;
- Mo service Sverige AB, company number 559090-0329, address c/o Adbus Affärspartner, Ladugårdsvägen 1, 234 35 Lomma, Sweden.

GENERAL PROVISIONS

The Privacy Policy establishes and defines the fundamental principles of personal data processing and the implementation of the data subject's rights. Additional information may be provided in sales, service and other contracts, as well as in separate notices.

By using Our services, purchasing goods, visiting Our premises or territory, sending or otherwise submitting a CV to the Company, contacting the Company, providing the Company with his data, continuing to browse the Website, the data subject confirms that he has read this Privacy Policy, understands its provisions and agrees to comply with it.

PRINCIPLES OF PROCESSING PERSONAL DATA

The Data Controller processes personal data in accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and which repeals Directive 95/46/EC (hereinafter – the **Regulation** or **GDPR**), the law on legal protection of personal data of the Republic of Lithuania and other legal acts regulating the processing of personal data.

The Data Controller is guided by the following basic principles of data processing:

- personal data is processed lawfully, fairly and in transparent manner (**principle of lawfulness, fairness and transparency**);
- personal data is collected for specified, explicit and legitimate purposes (**principle of purpose limitation**);
- processed personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (**principle of data minimisation**);
- personal data are constantly updated (**principle of accuracy**);
- personal data is stored safely and for no longer than required by the established purposes of data processing or legal acts (**principle of storage limitation**);
- personal data is processed only by employees of the Data Controller who have been granted such a right based on their work functions, or by data processors who provide services to the Data Controller and process personal data on behalf of the Data Controller and fot the benefit of the Data Controller or tha data subject (**principle of integrity and confidentiality**);
- The Data Controller is responsible for the observance of the above-mentioned principles (**principle of accountability**).

PERSONAL DATA SOURCES

Personal data is obtained:

- **directly from the data subject** (e.g. when he sends his curriculum vitae (CV) or otherwise contacts the Company, when he uses the Company‘s services or purchases goods from the Company, or when he participates in virtual meetings organised by the Company);
- **from third parties** (e.g. the Company‘s partners, law enforcement authorities, bailiffs, third parties);
- **from public registers**;
- **when data subject visits the Website** (when cookies uses on the Website are placed on the data subjet‘s terminal device).

PURPOSES, CATEGORIES AND TERMS FOR PROCESSING PERSONAL DATA

1. For the purpose of administering contracts with customers, suppliers, service providers and other third parties, the following personal data are processed: name, surname, title, signature, name of the represented legal entity, power of attorney or a copy of it, email address, telephone number, address, copy of the business or individual activity certificate, personal identification number.

In cases where contracts with group companies are administered, the following personal data shall be processed: name, surname, title, signature, name of the legal entity represented, power of attorney or copy thereof.

Legal basis: performance of contractual obligations (Article 6(1)(b) of the GDPR) and the legitimate interest of the Data Controller in the development of its business (Article 6(1)(f) of the GDPR).

Term of personal data storage: 10 years after the expiration of the contract.

2. For the purpose of internal personnel administration, the following personal data of the Data Controller's employees are processed: name, surname, signature, personal identification number, address, e-mail address, telephone number, bank account number, application/non-application of the

NPD (monthly tax-free income rate), amount of the advance payment, data on children's birth certificates (name, surname, date of birth, document no.), court decisions on the determination of the child's place of residence, health books, education, certificates, attestations, applications, car registration number, car brand, vehicle identification number, test results.

Legal basis: fulfillment of the obligations provided for in the employment contract (Article 6 (1)(b) of the GDPR) and fulfillment of the requirements provided for in legal acts (Article 6 (1)(c) of the GDPR), the legitimate interest of the data controller to carry out internal administration (Article 6 (1)(f) of the GDPR), health data is processed so that the Data Controller or data subject can fulfill obligations and exercise special rights in the field of labor and social security law (Article 9 (2)(b) of the GPRR).

Term of personal data storage: We will keep the contract of employment and its annexes, the personal file for 50 years after the expiration of the contract of employment, and We will keep other data for the period provided for by law.

3. For the purpose of analysing business performance, the personal data on employees, suppliers and customers contained in the accounting systems are processed.

Legal basis: the legitimate interest of the Data Controller in the development of the business (Article 6(1)(f) of the GDPR).

Period of storage of personal data: no longer than is necessary to achieve this purpose.

4. For the purpose of communication with business partners, the following personal data is processed: company representative‘s name, surname, title, telephone number, email address.

Legal basis: the legitimate interest of the Data Controller in the performance of its activities (Article 6(1)(f) of the GDPR).

Term of personal data storage: no longer than necessary for the purpose.

5. When processing personal data of managers and members of management bodies for the purposes of internal administration and the performance of their legal duties, the following personal data shall be processed: name, surname, signature, personal identification number, address of the actual and declared place of residence, and a copy of the personal document.

Legal basis: compliance with legal requirements (Article 6 (1)(c) of the GDPR).

Term of personal data storage: 10 years after the end of the period of being a manager or member of the management body.

6. For the purpose of protection of personal safety and property, ensuring continuous and stable operation of the Company (registration of visitors), the following personal data may be collected: name and surname of the interested party (person visiting the Company), name of the organisation, name of the Company's employee to whom the interested party has come to visit, telephone number of such employee, e-mail address, time of arrival and departure.

The data of the interested party may be recorded and stored in a log or in electronic format on the servers of Proxyclick SA, in accordance with the personal data policy https://www.proxyclick.com/privacy.

Legal basis: The legitimate interest of the Data Controller in ensuring the protection of persons and property (Article 6 (1)(f) of the GDPR).

Term of personal data storage: 1 working day or as long as it is appropriate.

7. For the purpose of video surveillance (to ensure the safety of the Company's employees and workplaces, compliance with work safety requirements and prevention of criminal offences, including the protection of property), the following data is collected: a person's image, a video without sound, the time and date of the video recording, and the number of the vehicle entering the territory.

Video surveillance in the Company shall only be carried out in premises and/or areas managed by the Company.

Legal basis: The legitimate interest of the Data Controller in ensuring the protection of property (Article 6(1)(f) of the GDPR).

Term of personal data storage: 30 days. After the expiry of the storage period, the video data will be automatically deleted. Where there is reason to believe that a breach of work duties, an accident, a criminal offence or other unlawful acts have been recorded, the video recordings shall be kept separately recorded on a computer or portable medium until the end of the relevant investigation and/or proceedings, or the expiry of the limitation period within which the employee may apply for a retraction and shall be destroyed as soon as they are no longer required.

8. For the purpose of employment with the Company, the following personal data may be collected from potential employees of the Company (candidates, job seekers) provided to the Company: curriculum vitae (CV), name, surname, contacts, interview notes.

In addition, We would like to mention that potential employees are informed about the processing of their personal data and the data storage periods at the time of first contact.

Legal basis: conclusion of an employment contract with the potential employee (Article 6(1)(b) of the GDPR), consent of the data subject (Article 6(1)(a) of the GDPR).

Term of personal data storage: if a potential employee applies for a specific position but is not offered a job, for 3 years after the end of the recruitment process (with the consent of the former candidate).

In cases where there is no selection of employees or trainees for a specific position advertised by the Company, but the data subject applies for one or more positions or, without specifying a specific position, and in order to undertake a traineeship with the Company, voluntarily contacts the Company using the contact details on the Company's website, and provides the Company with his personal data (e.g. curriculum vitae (CV), name and surname and contact details), such data subject's personal data shall not be stored (except for cases where the data subject expresses consent to the processing of such personal data on the Company's website).

9. For the purpose of contacting the disaster for an employee or other emergency, the name and telephone number of the contact person shall be collected.

When entering into an employment contract with the Company, the employee shall provide the Company with the aforementioned data of the contact person of his/her choice, i.e. the person who should be informed in the event of an accident or other emergency during the course of the work of the employee who has provided the contact.

By providing the Company with information about a contact person, the employee confirms that he/she is providing the information with the contact person's knowledge and consent and that he/she has been informed about this Privacy Policy. In the event that the contact person does not consent to the processing of his/her personal data by the Company for the purpose set out above, he/she shall contact the Company using the contact details provided in this Privacy Policy.

Legal basis: the legitimate interests of the Company to ensure that in the event of an employee's accident or other emergency, the contact person specified by the Company‘s employee is notified (Article 6(1)(f) of the GDPR).

Term of personal data storage: until the end of the employment contract with the Company's employee who identified the contact person or until the receipt of the contact person's refusal/objection to the processing of his/her personal data by the Company for the purpose of contacting in the event of a disaster for the employee or for the purpose of any other extraordinary event.

10. For the purpose of customer service (request administration), clerical work the following personal data are processed: name, surname, e-mail mail, phone number, city, request text, other data provided by the data subject.

Legal basis: the legitimate interest of the Company in administrating requests (Article 6(1)(f) of the GDPR).

Term of personal data storage: 3 years after the response to the request.

11. For the purpose of asset protection (access control) (only applicable to INHUS Construction, UAB and INHUS Prefab, UAB), the registration number of the car, date and time of entry, and a copy of the consignment note are processed.

Legal basis: the legitimate interest of the Company in the protection of its property (Article 6(1)(f) of the GDPR).

Term of personal data storage: data are processed in real time.

12. For the purpose of asset protection (monitoring of alarm system alarms, on/off control), the name, surname, telephone number, alarm system activation/deactivation actions of the responsible personnel are collected.

Legal basis: legitimate interest of the Company (Article 6(1)(f) of the GDPR).

Period of personal data storage: security system alarm data - 3 months, contact details of responsible employees - until the end of the employment relationship or the end of the functions for which the employee's data were transferred.

13. Processing of personal data of employees engaged by the subcontractor to perform the works (applicable to INHUS, UAB; INHUS Construction, UAB; INHUS Prefab, UAB; INHUS AB). As a contractor, we process the personal data of certain employees of our subcontractors engaged for the performance of the works, concerning the remuneration they receive in connection with the performance of the subcontract, including increased payment for overtime work, night work, work on weekends (rest days) and holidays and other mandatory payments. The following personal data of the employees employed by the subcontractor may be received and processed: name, surname, date of birth, position, information on the remuneration they receive in connection with the performance of the subcontract, including increased payment for overtime work, night work, work on weekends (rest days) and holidays and other mandatory payments.

Legal basis: the processing is necessary for the purposes of the legitimate interests of the Data Controller (contractor) or of a third party, except where such interests are overridden by the ineterests or fundamental rights and freedoms of the data subject which require protection of personal data (Article 6 (1) (f) of the GDPR).

Period of personal data storage: to the extent necessary to fulfill the parties' obligations under the subcontract. At the end of the subcontract, the data is stored for no longer than the limitation period specified in the Civil Code of the Republic of Lithuania (maximum 10 years).

14. For the purpose of organising and conducting conference calls, virtual meetings, video conferences and/or webinars, the following personal data may be collected from the persons participating in the virtual meetings and provided to the Company: information about meeting participants (name, surname, telephone number, email address, password (if not using a general registration), profile picture, department), meeting data (topic, description, IP address of the participants, hardware information of the device, start and end time of the videoconference), recordings, telephone data (if connected by telephone; telephone number initiating the call and the number answering it, country, start and end time of the call), and textual data.

We would also like to mention that the persons participating in virtual meetings are additionally informed about the processing of their personal data, the terms of data storage before the processing of such personal data begins, i.e. before the virtual meeting.

Legal basis: the legitimate interests of the Data Controller to ensure the organization and execution of remote meetings, convenient and secure communication (Article 6(1)(f) of the GDPR).

Period of personal data storage: the personal data referred to above will be processed for as long as they are necessary for the organisation and conduct of the virtual meetings/meetings and the related services.

15. For the purpose of implementing the provisions of the Labour Code on the prevention of violence and (or) harassment at work, the following personal data shall be processed: name, surname, position in the Company or relationship with the Company, contact information (telephone number, e-mail address), name, address, address, telephone number, email address, and telephone number of the person who has reported violence and/or harassment at work, and personal data of the person (who may have experienced or may have carried out the violence and/or harassment). (e.g. contact details, e-mail address), details of the event (time, duration, other circumstances), explanation, signature.

Legal basis: the legitimate interest of the Company in the proper implementation of the provisions of the Labour Code on the prevention of violence and (or) harassment at work (Article 6(1)(f) of the GDPR).

Period of personal data storage: 5 years after the last decision taken when examining the information provided.

JOINT CONTROLLERS

The Company may process personal data as a separate controller, but the Company may also process personal data together with other controllers (i.e. joint controllers within the meaning of Article 26 of the GDPR). A contract is concluded between the joint controllers, in which the joint controllers determine in a transparent manner their respective responsibilities for the fulfilment of obligations under the GDPR, defines the respective actual functions of the joint controllers and their relationship towards the data subjects. In case of the written request of the data subject, the data subject shall be given access to the essential provisions of this contract. The data subject may exercise his rights under the GDPR in relation to each of the data controllers.

COMPANY MANAGED ACCOUNTS ON SOCIAL MEDIA

We manage accounts on Facebook, LinkedIn, Instagram social media. Information provided by a person on social media (including messages, use of the "Like" and "Follow" fields, and other communications) or received by a person visiting Our accounts on social media is controlled by social network managers, Meta Platforms Ireland Limited, LinkedIn Ireland Unlimited Company. Facebook, LinkedIn, Instagram social network managers collect information about the type of content a person views, what they perform on a social network, with whom they interact, and other information. Therefore, We recommend that you read the privacy notices of social networking managers.

You can learn more about social network manager Facebook's privacy policy at: https://www.facebook.com/policy.php, you can learn more about the social network manager's LinkedIn privacy policy here: https://www.linkedin.com/legal/privacypolicy, You can learn more about social network Instagram's privacy policy here: https://help.instagram.com/402411646841720.

As administrators of social network accounts, We select the appropriate settings based on our target audience and our business management and promotion goals. By creating and administering accounts on social networks, We cannot control what information about the data subject will be collected by social network managers when We create accounts on social networks.

All such settings may affect the processing of personal data when the data subject uses social media, visits Our accounts or reads/views Our posts on social networks. Generally, social network managers process the data subject's personal data (even those collected by Us through additional account settings) for the purposes set by the social network managers, based on the privacy policies of social network managers. However, when a data subject uses social networks, communicates with Us through social networks, visits Our accounts on social networks, monitors posts on them, We receive information about the data subject. The amount of data We receive depends on the account settings We choose, the agreements with social network managers on ordering additional services and the cookies set by social network managers.

PROVISION OF PERSONAL DATA

The Data Controller undertakes to respect the duty of confidentiality towards data subjects. Personal data may be disclosed to third parties only if necessary for the conclusion and performance of a contract for the benefit of the data subject or for other legitimate reasons.

The Data Controller may provide your personal data:

- to public bodies and institutions, other persons performing functions assigned to them by law (e.g. law enforcement authorities, bailiffs, notaries, tax administration, supervisory authorities, authorities carrying out financial crime investigation activities);
- authorised auditors, legal and financial advisors;
- to third parties involved in the provision of services, registry operators, debt collection companies, insurance companies, travel agencies, airlines, hotels, visa issuing entities/authorities, mobile phone service providers, credit and financial institutions, postal service providers.

Data may be processed by data processors providing accounting, website hosting, data centre and/or server rental, IT systems maintenance, external audit, security, legal, data protection officer and other services to the Company.

Processors shall have the right to process personal data only on the instructions of the Company and only to the extent necessary for the proper performance of the obligations set out in the data processing agreement. The Company, with the help of data processing, seeks to obtain confirmation from the data processors that the data processors have also implemented appropriate organisational and technical security measures and will maintain the confidentiality of personal data.

TRANSFER OF PERSONAL DATA OUTSIDE THE EU/EEE TERRITORY

We generally process and store data subjects' personal data within the territory of the European Union or the European Economic Area (EU/EEA), but we may also transfer personal data outside the EU/EEA where this is necessary to fulfil the purposes for which it was collected and controlled.

We will transfer your personal data outside the EU/EEA in accordance with the requirements of Chapter V of the GDPR if at least one of the following measures is implemented:

- The European Commission has recognised that the country to which the data is transferred ensures an adequate level of protection of personal data;
- a contract has been concluded in accordance with standard terms and conditions approved by the European Commission;
- codes of conduct or other safeguards are in place in accordance with the Regulation;
- we have the individual and freely given consent of the data subject for the transfer of data outside the EU/EEA.

DATA PROTECTION OFFICER

The Company has a designated data procetion officer. The data protection officer can be contacted by e-mail dap@conretus.lt.

RIGHTS OF THE DATA SUBJECTS

Every data subject has the following rights:

a) the right to know (be informed) about the processing of your personal data;

b) the right to access personal data processed by the data processors and the manner in which they are processed, namely, to obtain information on the period of storage of personal data, technical and organizational measures applied to ensure data security, to obtain information from what sources, and what of one’s personal data is collected, for what purpose they are processed, to whom they are provided;

c) the right to request the correction, destruction or deletion of personal data or to discontinue the processing of personal data, except the storage, when the data are processed without complying with legal provisions;

d) the right to disagree with the processing of one’s personal data, except where such personal data are processed due to a legitimate interest pursued by the later controller or a third person to whom personal data are provided and if the interests of the data subject are not more important;

e) the right to require that the personal data provided be destroyed;

f) the right to demand the restriction of processing of personal data;

g) the right to require that the personal data provided by him, if they are processed on the basis of his consent or contract, and if they are processed by automated means, would be forwarded by the data controller to another data controller, if this is technically feasible (data portability);

h) the right to submit a complaint regarding the processing of personal data to the State Data Protection Inspectorate.

You can submit your request to the Company in person or through a representative:

- to dap@concretus.lt (the request must be signed with a qualified electronic signature);
- by post or by courier (a copy of the identity document must be attached to the request);
- by coming to the office at Žarijų str. 6A, Vilnius (the application can be made and (or) submitted at the Company's office upon presentation of an identity document).

Where the request is submitted on behalf of the data subject, the representative must submit with the request a power of attorney issued by the data subject and notarised by the notary.

The request for video recordings must specify the exact circumstances of the incident, including the address of the premises/area under the Company's control, the specific location within those premises/area where the incident occurred, and the date and time of the incident (to the nearest half-hour).

Upon receipt of a request, no later than 30 calendar days after receipt of the request, We will:

- will provide a response in the same form in which the request was received, or in the form specified in the request if the data subject or the person making the request (representative of the data subject) confirms that providing a response in this form will ensure the security of the data; or
- information on the refusal to comply with such a request, stating the reasons for the refusal.

ASSURANCE OF DATA SECURITY

The Company aims to implement appropriate, technically feasible and economically reasonable organisational and technical data security measures to protect personal data from accidental or unlawful destruction, alteration, disclosure, as well as from any other unlawful processing. All personal data and other information provided by the data subject shall be treated as confidential.

Only those Company employees, service providers and authorized data processors who need personal data to perform the functions assigned to their organizational unit have access to personal data. Access to personal data is granted to the General Manager UAB "Concretus group" and INHUS Group, UAB (in relation to other Companies than INHUS Group, UAB).

COOKIES

The Company's Website uses cookies for statistical and marketing purposes - small pieces of text information that are automatically created when you browse the Website and stored on your computer or other device.

Cookies are used to collect data about visitors' actions while browsing the Website. The information collected by cookies enables us to ensure the proper functioning of the Website, to make the Website more user-friendly for visitors, to provide suggestions and to learn more about the behaviour of visitors to the Website, to analyse trends and to improve both the Website and the services it provides.

Description of the cookies used on Website:

Name	Purpose	Validity time
_ga	These cookies allow Us to count visits and traffic sources so We can measure and improve your site's performance.	2 years
_gat_gtag	These cookies allow Us to count visits and traffic sources so We can measure and improve your site's performance.	1 day
_gid	These cookies allow Us to count visits and traffic sources so We can measure and improve your site's performance.	1 day
_hjAbsoluteSessionInProgress	These cookies allow Us to count visits and traffic sources so We can measure and improve your	30 min.

	site's performance.	
_hjid	These cookies allow Us to count visits and traffic sources so We can measure and improve your site's performance.	Before closing the browser
_hjIncludedInSample	These cookies allow Us to count visits and traffic sources so We can measure and improve your site's performance.	Before closing the browser
october_session	Saving the website language setting.	1 hours

When you visit the Website, you can indicate whether you accept the use of statistical and marketing cookies. If you agree to the placement of non-essential (statistical and marketing) cookies on your computer or other device, please click on the "I agree" button. If you do not consent to the placing of non-essential cookies on your computer or other terminal device, you can object to the placing of such cookies on the Website by clicking on the "Disagree" button. However, please note that in some cases this may slow down your internet browsing speed, limit the functionality of certain features of the Website, or block access to the Website. You can enable/disable the cookies of your choice at any time.

The Website contains links to other people's websites. Please note that the Company is not responsible for the content of such websites or the privacy practices employed by them. Therefore, if you follow a link from the Website to other websites, we suggest that you consult their privacy policies.

To learn more about cookies, you can visit http://www.allaboutcookies.org.

To find out how to stop tracking web pages with Google Analytics cookies, you can visit http://tools.google.com/dlpage/gaoptout.

OTHER PROVISIONS

We may, in Our sole discretion, change this Privacy Policy, which shall take effect upon its publication on Our Websites. Last updated on 2023-08-07.