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
- www.tmbelement.ee (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, address for correspondence – Žarijų g. 6A, Vilnius, Lithuania;
- INHUS, UAB, company number 302863631, registered headquarters address – Žarijų g. 6, Vilnius, LT, address for correspondence – Žarijų g. 6A, Vilnius, Lithuania;
- INHUS Prefab, UAB, company number 121559766, registered headquarters address – Žarijų g. 6, Vilnius, LT, address for correspondence – Žarijų g. 6A, Vilnius, Lithuania;
- INHUS Construction, UAB, company number 302891837, registered headquarters address – Žarijų g. 6, Vilnius, LT, address for correspondence – Žarijų g. 6A, Vilnius, Lithuania;
- INHUS Engineering, UAB, company number 301545597, registered headquarters address – Žarijų g. 6, Vilnius, LT, address for correspondence – 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 LIMITED, company number 12429993, address Mills & Reeve Llp, 1 City Square, Leeds, West Yorkshire, United Kingdom LS1 2ES;
- INHUS Prefab sp. z o. o, company number 0000931280, address Al. Ujazdowskie 41, 00-540 Warszawa, Poland;
- INHUS Engineering Oy, company number 3164704-2, address c/o Properta Asianajotoimisto Oy Bulevardi 6 C 22 00120, Helsinki, Finland (Entrance to the premises: c/o Properta Asianajotoimisto Oy Yrjönkatu 7 C 00120 Helsinki);
- 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;
- INHUS Prefab OÜ, company number 12560626, address Betooni tn 7, 51014, Tartu, Estonia.

GENERAL PROVISIONS

The Privacy Policy establishes and defines the basic principles for the processing of personal data and exercising of the rights of the data subject. Additional information may be included in sales, service and other contracts, as well as in separate statements.

By using Our services, purchasing goods, visiting Our premises or territory, sending or otherwise submitting a CV to the Company, contacting the Company, submitting his/her data to the Company, as

well as by continuing browsing the Website, the data subject confirms that he/she has read this Privacy Policy, understood its provisions and agrees to comply with it.

PRINCIPLES OF PROCESSING OF 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 of the Republic of Lithuania on Legal Protection of Personal Data 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 subject‘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/electronic signature of the signatory, 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.

When handling contracts with group companies, the following personal data are processed: the name, surname, job title, signature/electronic signature of the signatory, the name of the legal entity represented, a power of attorney or its copy.

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

Personal data retention period: 10 years after the end of the contract.

2. For the purpose of internal administration of personnel, the following personal data of the Data Controller's employees are processed: the name, surname, signature, personal identification number, address, e-mail address, telephone number, bank account number, application/non-application of the monthly tax-free income rate, amount of the advance payment, data contained in children's birth certificates (gender, date of birth), information contained in children's disability document, information contained in court decisions on the determination of the child's place of residence, health cards, education, certificates, attestations, applications, car registration number, car brand, vehicle identification number, test results.

Legal basis: performance of obligations under an employment contract (Article 6 (1)(b) of GDPR) and compliance with legal obligations (Article 6 (1)(c) of GDPR), legitimate interest of the Data Controller for the performance of internal administration (Article 6 (1)(f) of GDPR), processing of the health data necessary for carrying out the obligations and exercising specific rights of the Data Controller or of the Data Subject in the field of employment and social security and social protection law (Article 9 (2)(b) of GPRR).

Personal data retention period: We will keep the employment contract, its annexes and the personal file for 50 years after the end of the employment contract, and We will keep other data for the period of time provided for by law.

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

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

Personal data retention period: up to 10 years.

4. For the purpose of communication with business partners, the following personal data are processed: the company representative‘s name, surname, job title, telephone number, e-mail address.

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

Personal data retention period: no longer than necessary for the purpose.

5. When processing personal data of executives, members of management bodies, shareholders and ultimate beneficial owners for the purposes of internal administration and carrying out of legal obligations, the following personal data shall be processed: data concerning shareholders: the name, surname, signature, personal identification number, residential address, a copy of the ID document; data concerning shareholders and ultimate beneficial owners: the name, surname, date of birth, country of birth, personal identification number, residential address, nationality, country of residence for tax purposes, tax identification number, information on the ID document (the type, number, country of issue, expiry date), copy of the ID document; data concerning executives and members of the management board: the name, surname, signature, personal identification number, address of the actual and declared residence, a copy of the ID document.

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

Personal data retention period: personal data of shareholders and ultimate beneficial owners shall be retained for 10 years after the period of being a shareholder (ultimate beneficial owner) ends or until appropriate; personal data of executives and members of management bodies shall be retained for 10 years after the period of being a manager or a member of a management body ends or until appropriate.

Data recipients: JADIS, JANGIS (Lithuania) / Bolagsverket (Swedish Companies Registration Office) (Sweden) / Companies House (United Kingdom) / Krajowy Rejestr Sądowy (Poland) / Finnish Patent and Registration Office Trade Register (Finland) / Business Register (Estonia)

6. For the purpose of safeguarding personal security and property and ensuring uninterrupted and stable corporate operations at the Company (registration of visitors), the following personal data may be collected: the name and surname of an interested party (the person visiting the Company), the name of the organisation, the name of the Company's employee visited by the interested party, the telephone number and e-mail address of such employee, and the time of arrival and departure.

The data of the involved parties may be recorded in a register or stored in electronic format on Proxyclick SA servers in accordance with the personal data policy https://www.proxyclick.com/privacy.

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

Personal data retention period: 1 working day or until appropriate.

7. For the purpose of video surveillance (to ensure the safety of the Company's employees and workplaces, compliance with work safety requirements, including the protection of property), the following data are 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 protection of individuals and property (Article 6(1)(f) of GDPR).

Personal data retention period: 30 calendar days. After the expiry of the retention period, the data of video recordings are automatically deleted. Where there are grounds for believing that a breach of work duties, accident, criminal offence or other unlawful acts has been recorded, the video recordings are kept separately stored on a computer or on a removable 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 are destroyed as soon as they are no longer required.

8. For the purpose of employment in the Company, the following personal data provided by potential employees of the Company (candidates, job applicants) may be collected: the curriculum vitae (CV), name, surname, contact information, interview notes.

It should be pointed out that potential employees are informed about the processing of their personal data and the retention period of data at the time of first contact.

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

Personal data retention period: if a potential employee applies for a specific position, but no job is offered to him/her, the potential employee's data shall be retained 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. the 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 in the event of an accident to an employee or another emergency, the name and telephone number of the contact person are collected.

When entering into an employment contract with the Company, the employee may provide the Company with the above-mentioned data of the contact person of his/her choice, i.e. the person who should be informed if an accident happens to the employee or in the event of another emergency occurring during the working hours of the employee who has provided the contact.

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

Legal basis: the legitimate interests of the Company to notify the contact person designated by the Company's employee in the event of an accident to an employee or another emergency (Article 6(1)(f) of GDPR).

Personal data retention period: until the end of the employment contract with the Company's employee who has designated the contact person or until the Company receives the contact person's denial of consent/objection to the processing of the contact person's personal data for the purpose of contacting him/her in the event of an accident to the employee or another emergency.

10. For the purpose of customer service (enquiry management) and record-keeping the following personal data are processed: the name, surname, e-mail address, telephone number, city, text of enquiry, and other data provided by the data subject.

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

Personal data retention period: 3 years after the response to the enquiry.

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 GDPR).

Personal data retention period: 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 GDPR).

Personal data retention period: 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: the 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 pursued by the Data Controller (contractor) or by 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 GDPR).

Personal data retention period: 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, online meetings, video conferences and/or webinars, the following personal data provided to the Company by the persons participating in online meetings may be collected: the information about the participants in the meeting (the name, surname, telephone number, e-mail address, password (if not using co-registration), profile picture, department), meeting data (the topic, description, IP address of participants, hardware information of the device, start and end times of the video conference), recordings, telephone data (if joined by phone; the telephone numbers of the incoming and outgoing call, the country, start and end times of the call), text data.

Please note that the persons attending online meetings are additionally informed about the processing of their personal data and the retention periods before the processing of such personal data starts, i.e. before the online meeting.

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

Personal data retention period: the personal data referred to above will be processed for the period determined by the virtual meeting platform.

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 of the persons who have reported or allegedly experienced or committed violence and/or harassment at work, also witnesses and employees conducting the investigation is processed: the name, surname, job title in the Company or the relationship with the Company, contact information (telephone number, e-mail address), the information about 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 GDPR).

Personal data retention period: 5 years after the last decision taken in examining the information submitted.

JOINT CONTROLLERS

The Company can process personal data as a separate controller, but the Company can also process personal data together with other data controllers (i.e. joint controllers within the meaning of Article 26 of GDPR). An agreement shall be concluded between joint controllers, establishing their respective responsibilities for the fulfilment of the obligations under GDPR in a transparent manner, defining the individual functions of joint controllers and their relationship with data subjects. The data subject shall have access to the essential provisions of this agreement at the written request of the data subject. The data subject may exercise his/her rights under GDPR in respect of 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, judicial officers (bailiffs), notaries, tax administrators, supervisory authorities, agencies carrying out financial crime investigation activities);
- authorised auditors, legal and financial advisors;
- to third parties involved in the provision of services, registry managers, debt collection companies, insurance companies, travel agencies, airlines, hotels, visa issuing entities/authorities, mobile phone service providers, credit and financial institutions, postal service providers.

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

The data processors shall have the right to process personal data only upon instructions from the Company and only to the extent necessary for the proper performance of the obligations under the data processing agreement. The Company seeks assurance from the data processors that the data processors have also implemented appropriate organisational and technical security measures and 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 the data procection officer. The data protection officer can be contacted by e-mail at dap@conretus.lt.

RIGHTS OF DATA SUBJECTS

Each data subject shall have the following rights:

a) right to information about the processing of your personal data;

b) right of access to his/her processed personal data and the way of processing, namely to obtain information on the period of retention of personal data, the technical and organisational measures taken to ensure data security, to receive information from which sources and for what purpose his/her personal data is collected, to whom it is transferred/provided;

c) right to rectification and erasure or blocking, other than storage, of his/her data, where the processing is not carried out under legal provisions;

d) right to object to the processing of his/her personal data, unless such processing is required for the legitimate interest of the data controller or a third party to whom the personal data is provided, and the interests of the data subject are not overriding;

e) right to erasure of the submitted personal data;

f) right to restriction of processing of personal data;

g) right to require that the personal data provided by him/her be transmitted by the data controller to another data controller, if it is processed based on the data subject's consent or contract and by automated means, and where it is technically possible (data portability);

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

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

- by e-mail dap@concretus.lt (the request must be certified by a qualified electronic signature);
- by post or by courier (a copy of your identity document must be attached to your request);
- by arriving in person in the office at Žarijų str. 6A, Vilnius (you can write and/or submit your request at the Company's office upon presentation of your identity document).

Where the request is made on behalf of the data subject, the representative must submit a power of attorney issued to him/her by the data subject and certified by the notary along with the request.

The request for video recordings must specify the exact circumstances of the incident (including: the address of the premises/territory controlled by the Company, the specific location within those premises/in the territory where the incident occurred, the date and time of the incident (up to half-hour accuracy).

At least within 30 calendar days from the date of receipt of the request, We 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 (the data subject's representative) confirms that providing a response in this form will ensure the data security; or
- the information on the refusal to comply with such a request, stating the reasons for the refusal.

ENSURING DATA SECURITY

The Company aims to implement appropriate, technically feasible and cost-effective organisational and technical data security measures to protect personal data against accidental or unlawful destruction, alteration, disclosure, and any other illegal processing. All personal data and additional information provided by the data subject are treated as confidential.

Access to personal data is limited to those Company employees, service providers and authorised data processors who need personal data to perform the functions assigned to them by their organisational unit. 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 can be found in the website's cookie policy.

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

The Company is free to change this Privacy Policy, which will come into effect from its publication on Our Websites. Last updated on 2024-12-19.