

DATA PROCESSING AGREEMENT

[town/ city]

UAB "Ignitis grupės paslaugų centras", legal entity code 303200016, registered office address Laisvės pr. 10, LT-04215, the Republic of Lithuania, and

Retcon Sp. z o.o., legal entity code 0000345088, registered office address Al. Jerozolimskie 172, 02-486 Warsaw,

the Controller and the Processor shall hereinafter be jointly referred to as Parties and each of them individually shall hereinafter be referred to as the Party, have concluded this Data Processing Agreement (hereinafter referred to as the **Data Processing Agreement**):

1. Concepts used in the Agreement

- 1.1. **Personal Data** (or the **Data**) shall mean any information related to a natural person (data subject), whose identity is known or could be determined by using this data (for instance, name, surname, personal number, date of birth, contact information, meter data, IP address, etc.), one or several characteristics of a physical, physiological, psychological, economic, cultural, or social nature typical to the person.
- 1.2. **Data Processing** shall mean any action involving the Personal Data: collection, recording, accumulation, storage, classification, publication, grouping, changing, combination, use, logic and (or) arithmetic operations, search, dissemination, destruction, provision, other action or a set of actions.
- 1.3. **Technical and Organizational Security Measures** shall mean measures designed for protection of the Personal Data against accidental or unlawful destruction, changing, disclosure as well as against any other unlawful processing. The aforementioned measures shall ensure such a level of security, which would correspond to the nature of the Personal Data subject to protection and the risks associated with processing thereof.
- 1.4. **Legislation on the Protection of Personal Data** shall mean legislation regulating protection of the Personal Data and/or establishing the requirements applicable to data security measures, including, but not limited to, Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016 on the protection of natural persons with regard to the processing personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation (hereinafter – the GDPR), Law on Legal Protection of Personal Data of the Republic of Lithuania, Law on Electronic Communications of the Republic of Lithuania as well as other legislations of the European Union and the Republic of Lithuania, including amendments thereof.
- 1.5. Other concepts used in the Data Processing Agreement shall be construed based on the definitions thereof given in the Legislation on the Protection of Personal Data.

2. Basis and purpose for the provision of data

- 2.1. The Data Processing Agreement, in implementation of Article 28 (3) of the GDPR, shall establish the rights and obligations of the Controller and the Processor when processing personal data on behalf of the Controller. The purpose of the Agreement is to protect the rights of data subjects, to reduce the specific risk of personal data protection and to ensure the clarity of the relationship between the Controller and the Processor and the respective rights and obligations.
- 2.2. Personal Data shall be collected and processed for a lawful purpose: in order to ensure proper implementation of the obligations assumed by the Processor under licence for the localisation of the Microsoft Dynamics 365 (Whitelist and NBP) solution for Poland and its configuration in

the Buyer's existing accounting system Microsoft Dynamics 365 contract (hereinafter referred to as the **Contract**)

- 2.3. In cases where the Controller processes personal data on behalf of AB "Ignitis grupė" group of companies for the purposes specified in the Data Processing Agreement and uses the Processor's service to perform these actions, then the Controller acts as the Processor, the Processor as the Sub-Processor and they must comply with the provisions of this Data Processing Agreement, which apply to the Processor and the Sub-Processor used by him.
- 2.4. This Contract shall not release the Processor from the obligations applicable to the Processor under the GDPR or other legal acts.

3. Obligations of the Controller

- 3.1. The Controller does hereby confirm that processing of the Personal Data specified in Annex No 1 based on the Contract and the Data Processing Agreement concluded by the Parties is lawful and meets the Legislation on the Protection of Personal Data.
- 3.2. The Controller hereby confirms that it has provided in the Data Processing Agreement and in the annexes thereof, and, if will be required so, will additionally provide during the term of the Contract and the Data Processing Agreement necessary instructions to the Processor regarding the processing of Personal Data at the order of the Controller.
- 3.3. The Controller shall hereby undertake to provide the Processor immediately upon receipt of the Processor's request, but no later than within 5 (business) days, with the required information related to the processing of Personal Data being processed on the basis of this Data Processing Agreement in accordance with the requirements of this Data Processing Agreement and the legislation.

4. Obligations of the Processor

- 4.1. The Processor shall hereby undertake to follow the requirements established by the Legislation on the Protection of Personal Data, the Data Processing Agreement and the Annexes thereof as well as other assignments given by the Controller within the course of processing of Personal Data. Personal Data processed at the order given by the Controller, the purpose, scope, and conditions of processing thereof are specified in Annex No 1 to the Data Processing Agreement.
- 4.2. The Processor shall immediately notify the Controller if, in the opinion of the Processor, the instructions given by the Controller on the nature of data processing, technical and organizational measures are in conflict with the GDPR or other EU or Lithuanian legislation governing the data processing.
- 4.3. The Processor shall hereby undertake to ensure at its own cost, in the course of Personal Data processing, protection of the Personal Data being processed through implementing proper technical and organizational measures designed for the protection of Personal Data being processed against accidental or unlawful destruction, corruption, changing, loss, disclosure as well as against any other unlawful processing. These measures should ensure the required level of protection, which would correspond to the nature of the Personal Data being processed and the risks associated with processing thereof as well as to the requirements of the legislation.
- 4.4. The Processor shall hereby undertake to ensure confidentiality of Personal Data and guarantees that access to Personal Data will be granted only to those employees of the Processor or to the persons authorized by the Processor who need it for the implementation of their functions, and that data would only be used for the actions for the performance of which the Processor has been granted rights, only those activities to which the Processor has been granted rights shall be performed with the Personal Data to the extent required for the proper fulfilment of this Data Processing Agreement. The Processor shall hereby undertake to make sure that the persons authorized to process Personal Data would be properly informed about confidentiality of Personal Data, would be properly trained on the implementation of their duties and following the requirements applicable to Personal Data processing provided for in the Data Processing Agreement, in the assignments given by the Controller and in the legislation, and

that they are committed to maintaining the confidentiality of Personal Data. The list of persons granted access to personal data must be reviewed periodically at least every 6 months. Following this review, such access to personal data shall be revoked if such access is no longer required. In the event of a change in the personal data of the Controller, their access rights to the personal data of the Controller shall be revoked no later than the last day of his/her work with the personal data of the Controller entrusted to him/her and, in the event of termination of the employment of the Processor, no later than on the last day of his/her employment.

- 4.5. The Processor shall hereby undertake to ensure the protection measures specified in the Security Requirements (Annex No 2 to the Data Processing Agreement). The Processor shall hereby undertake to make sure that these protection measures are introduced prior to starting processing of Personal Data and are subject to continuous oversight, and are upgraded, whenever needed, monitored and controlled. Upon receipt of the Controller's request, the Processor shall immediately, but not later than within 10 (business) days notify the Controller on how the Processor complies and how it ensures that the persons related to and authorized by the Processor comply with these Security Requirements, and what steps the Processor has taken to ensure compliance with the Security Requirements.
- 4.6. The Processor must hold and provide the updated records of data processing activities, including the name, contact details, representative (including the Data Protection Officer, if appointed) and domicile of each entity acting as a sub-processor.

5. Transfer of data to third countries

- 5.1. The Processor may transfer personal data to third countries or international organisations only upon receipt of the instructions documented by the Controller and in accordance with the requirements of Chapter V of the GDPR.
- 5.2. If personal data need to be transferred to third countries or international organisations in accordance with the legislation of the European Union or its Member State, which must be complied with by the Processor, even though the Controller has not instructed the Processor to do so, the Processor shall inform the Controller of this legal requirement prior to the transfer of the data, unless that law prohibits the transfer of such information.
- 5.3. The Processor may not, without documented instructions from the Controller or without a specific requirement under the law of the European Union or its Member State, in accordance with this Agreement:
 - 5.3.1. to transfer personal data to a controller or processor in a third country or international organisation;
 - 5.3.2. to transfer the processing of personal data to an subsidiary processor in a third country;
 - 5.3.3. to allow personal data to be processed by a processor in a third country.
- 5.4. This Data Processing Agreement is not a standard data protection Clause as defined in Article 46 (2) (c) and (d) of the GDPR, and the parties may not invoke the Data Processing Agreement as a basis for the transfer of personal data to third countries or international organisations under Chapter V of the GDPR.

6. Processor's assistance to the Controller

- 6.1. In cases where the authorized public authorities, officers or any other person, including the data subject, has filed a request, complaint, claim directly related to the data processed under the Data Processing Agreement and the Contract, the Processor must immediately, but not later than within 3 (business) days, transfer such request to the Controller by sending it to the contact e-mail address of the Controller. If the request/complaint/claim are not related exclusively with the rights of the data subjects under the General Data Protection Regulation, the Controller and the Processor, depending on the situation and the nature of the matter, shall agree that they shall prepare and submit reply to the data subject.
- 6.2. Upon receipt of request to exercise the rights of the data subject laid down in the General Data Protection Legislation, the Processor shall, within the deadline and using the measures specified in Clause, transfer the request to the Controller.
- 6.3. The Parties hereby agree that the rights of data subjects laid down in the General Data Protection Legislation shall be implemented and reply to the request of the subject shall be

provided by the Controller. The Processor, having regard to the nature of data processing and the request submitted, shall help the Controller in implementing the rights of data subjects and replying to the requests submitted by providing necessary documents, information, using appropriate technical and organizational measures to fulfil the requests.

- 6.4. Given the nature of the data processing and the status of the processor, the Processor shall assist the Controller in ensuring compliance with the obligations laid down in Articles 32 through 36 of the General Data Protection Regulation:
- a) immediately notifying the Controller of any data security breach in order the Controller could fulfil its duty to notify the State Data Protection Inspectorate of the breach not later than within 72 hours;
 - b) assisting in communication with data subjects in case where, following a data security breach, a high risk necessitates the notification of data subjects;
 - c) providing advice and assistance in assessing potential risks in carrying out data protection impact assessment in cases where data processing is done using tools, systems and processes developed by the Controller, and where a data protection impact assessment is necessary under the legislation on the Protection of Personal Data;
 - d) if necessary, within its competence, on participating together with the Controller in prior consultation with the State Data Protection Inspectorate, where such consultation is mandatory in accordance with the legislation on the Protection of Personal Data.
- 6.5. The Processor shall undertake to provide the Controller free of charge with all information that is necessary for proving that all obligations provided for in the Data Processing Agreement and in the legal acts are being fulfilled.

7. Notice on data security breach

- 7.1. If data security breach occurs or it is suspected to having occurred, or any other procedural actions of the State Data Protection Inspectorate related to the processing of Personal Data processed under the Data Processing Agreement and/or the Contract are being carried out the Processor shall immediately, but in any case not later than within 24 (twenty-four) hours following the identification of the security incident, notify the Controller in writing thereof.
- 7.2. The Processor shall submit to the Controller a Notice containing all information which, under the legislation on the Protection of Personal Data, is necessary for the Controller to be able to properly fulfil its obligation to notify the State Data Protection Inspectorate and data subjects, and to eliminate and minimize the consequences of data security breach.
- 7.3. The Processor must take urgent actions to prevent further damage as a result of the data security breach and to minimize the consequences of such breach.
- 7.4. Upon receipt of recommendations and/or instructions from the Controller in connection with the data security breach, the Processor must immediately implement them.
- 7.5. The Processor shall register all security violations of the Personal Data being processed on the basis of this Data Processing Agreement and the Contract, including the facts related to the violation, the consequences thereof and the implemented corrective actions.

8. Use of subsidiary subsidiary data processors

- 8.1. The Processor shall have the general written permission of the Controller to use subsidiary subsidiary processors.
- 8.2. Before using a new or replacing an existing subsidiary subsidiary data processor, the Processor shall inform the Controller in advance in writing (by e-mail), providing the details of the subsidiary subsidiary processor and other information related to personal data processing activities.
- 8.3. The Controller shall have the right to object to the use of a new subsidiary processor and to inform the Processor thereof within 5 (five) business days from the day of receipt of the Processor's notice, giving reasons and only for material reasons (e.g. due to a real threat to the security of processed personal data). If the Controller objects to the transfer of Personal

Data to the subsidiary processor, the Processor must continue to fulfil its obligations under the Data Processing Agreement without the use of the subsidiary processor.

- 8.4. The Processor shall be responsible for ensuring that the contracts with the subsidiary processors provide for at least the data protection measures specified in this Data Processing Agreement.
- 8.5. The Controller, in order to ensure that the contract signed between the Processor and the subsidiary processor lays down the same requirements as apply to the Processor, shall have the right to request a copy of the data processing agreement and/or its amendments signed with the subsidiary processor. The Processor must provide such a copy of the agreement or its part, in which only data processing issues are discussed.
- 8.6. The Processor must ensure that the subsidiary processors used by him process the data in accordance with all relevant processing instructions and only to the extent and in the manner necessary for the provision of the relevant services. The Processor must oblige the subsidiary processors to ensure that, in the case of other subsidiary processors, the data processing agreements contain measures for the protection of personal data at least equivalent to those laid down in this agreement. The Processor shall not inform the Controller about the subsidiary processors used by the subsidiary processors.
- 8.7. The Processor shall be liable for the acts and omissions of the subsidiary processors employed by him, including the persons or employees employed by him, which result in non-compliance with the requirements of the legal acts regulating the processing of personal data.
- 8.8. Subsidiary processors used by the Processor and acceptable to the Controller shall be listed in Annex No 3 to this Agreement.

9. Audit

- 9.1. The Controller shall have the right, after having submitted a prior notice, without interrupting the activities of the Controller and free of charge, to conduct inspections and/or audit of the Processor in the premises of the Processor's office during normal business hours. Such audit or inspections may be carried out by the employees of the Controller or by other persons authorized by the Controller who are bound by appropriate confidentiality obligations.
- 9.2. The Processor shall undertake to provide all necessary information, documents and access to the facilities operated by the Processor to the extent necessary to carry out the audit of the data processing and to evaluate the technical and organizational measures taken, without prejudice to the trade secrets of the Controller.
- 9.3. The Parties hereby agree that the costs of audit or inspections incurred by the Controller shall be borne by the Controller itself. However, if the audit or inspection reveals failure to fulfil or improper fulfilment of obligations, failure to comply with the legal acts and/or instructions of the Controller by the Processor, by the persons authorized by or related to it (including the sub-processors engaged by it), the Processor must reimburse the Controller for the costs of the audit and/or inspections, and must immediately remedy any identified inconsistencies.

10. End of the processing of Personal Data

- 10.1. When processing of Personal Data is no longer necessary for fulfilment of the Processor's obligations under the Agreement or when the Agreement expires or is terminated, the Processor must immediately, but not later than the deadline specified by the Controller, without imposing any extra fee, submit (return) to the Controller all Personal Data and any other data processed by the Processor at the order of the Controller in the execution of the Agreement, as well as any available copies of such data. Personal data, other data and copies thereof shall be submitted (returned) in the manner and form specified by the Controller. If it is impossible to submit (return) the Personal Data, other data, and copies thereof, or if instructed so by the Controller, the Processor must immediately destroy Personal Data, other data, and copies thereof, and provide the Controller a written confirmation of the destruction of data and copies thereof.

11. Liability

- 11.1. The Processor shall be liable for all and any expenses, costs, compensations, damages, and losses caused to the subjects of Personal Data, the Controller, the Controller's client, cooperation partner, or the third party by the Processor, its employee or sub-processor as a result of inadequate implementation and/or violation of the Data Processing Agreement, the Contract, the Controller's instructions, and/or the Legislation on the Protection of Personal Data.
- 11.2. The Processor shall hereby undertake to reimburse the Controller for all direct losses, including, but not limited to, losses related to fines imposed by the public authorities.
- 11.3. The Processor shall be fully liable for the actions of its employees and compliance with the Security Requirements specified in Annex No 2.
- 11.4. Any violation of the Processor's obligations specified in the Legislation on the Protection of Personal Data or in the Data Processing Agreement committed by the Processor (or by its sub-processors) will be regarded as material violation of the Data Processing Agreement and/or the Contract.

12. Other terms and conditions

- 12.1. The Parties hereby agree to keep confidential this Data Processing Agreement and all information communicated to each other on its basis for an indefinite period, regardless of whether that information is provided orally or in writing. The Parties hereby agree not to disclose confidential information to any third party without the prior written consent of the Party having provided it, unless such information must be disclosed for the proper performance of this Agreement, to a legal, financial or other professional/advisor or lender. The person to whom the Party discloses confidential information must assume the obligation of confidentiality under this clause, and use such information only for the purpose for which it was provided. The provisions of this Article shall not apply to information which is or becomes publicly available, or has been or is to be disclosed in accordance with legal requirements. The Party in breach of its obligations under this Agreement to protect confidential information and not disclose it, must reimburse the other Party for losses resulting from the violation of this Agreement, and must take all reasonable steps to remedy the consequences of such disclosure within the shortest possible period of time. This clause of the Agreement shall continue to apply after its termination (for an indefinite period of time).
- 12.2. All communications under the Data Processing Agreement must be made in writing and shall be deemed to have been properly received: (i) if 5 (business) days have passed following mailing thereof via recorded mail to the address of the Party's registered office, (ii) in case of serving against signature: on the day when the recipient affixes his/ her signature confirming receipt of the document submitted to him/ her, (iii) in case of e-mailing to the e-mail addresses of the Parties to the contact persons specified in Annex No 1: on the same day of e-mailing thereof.
- 12.3. The legal relations of the Parties under this Data Processing Agreement shall be subject to the Legislation on the Protection of Personal Data, which shall include the law of the country of the Controller's registered office - the laws and other legislation of the Republic of Lithuania, including the directly applicable EU legislation.
- 12.4. All disputes arising in connection with the Data Processing Agreement shall be settled by a mutual consensus between the Parties. In the event of failure by the Parties to reach a consensus, any disputes, disagreements, or claims arising out of this Data Processing Agreement or related to it, violation, termination, or validity thereof, not resolved by a mutual consensus between the Parties, shall be resolved at the court of the Republic of Lithuania based on the location of the Controller's registered office, unless stipulated otherwise by the legal acts.
- 12.5. In the event of conflict between the terms and conditions of this Data Processing Agreement and of other contracts entered into between the Parties, the provisions of this Data Processing Agreement shall apply.

13. Validity, amendment, and termination of the Agreement

- 13.1. The Data Processing Agreement shall enter into force from the date of its signature and shall, depending on whichever comes first, remain in force:
- 13.1.1. as long as the Agreement is valid; or
 - 13.1.2. until the deadline specified in a separate notification given by the Controller to the Processor on termination of the Data Processing Agreement.
- 13.2. The Processor's confidentiality obligations shall remain in force after the expiry of this Data Processing Agreement and/or of the Contract.
- 13.3. All amendments and supplements to the Data Processing Agreement shall be valid if made in writing and confirmed with affixed signatures of the representatives of both Parties.
- 13.4. The Parties shall hereby confirm and guarantee that they have all authorisations required for concluding and fulfilling the Data Processing Agreement.
- 13.5. The Data Processing Agreement has been concluded in 2 (two) copies of equal legal power, one copy for each Party.

14. Annexes to the Agreement

- 14.1. The Annexes form an integral part of the Data Processing Agreement and shall be construed in accordance with the provisions of the Data Processing Agreement. Each Party to the Agreement is given 1 (one) copy of each Annex to the Data Processing Agreement.
- 14.2. The Annexes to this Data Processing Agreement:
- 14.2.1. Annex No 1 – Terms and conditions of personal data processing.
 - 14.2.2. Annex No 2 – Security requirements.
 - 14.2.3. Annex No 3 – Sub-processors engaged by the Processor.

15. Details and signatures of the Parties:

CONTROLLER:

UAB "Ignitis Grupės Paslaugų Centras"

(Signature)

PROCESSOR:

Retcon Sp. z o.o.

(Signature)

Terms and conditions of the processing of Personal Data

1. Purpose of data processing:

The Processor shall process data:

- 1) Configuring localization according to Polish law;
- 2) provision of Services to the Controller

2. Data subjects:

The Personal Data being processed is related to the following categories of data subjects:

- 1) Customers of the Controller, their representatives;
- 2) Suppliers of the Controller;
- 3) Customers and Suppliers of the Controller clients.

3. Processed data:

Personal Data processed is or could be Personal Data of the type indicated below:

- 1) Information on the clients, for example:
 - Forename, surname
 - Client code
 - Object address
 - Contact details (address, telephone number, e-mail)
- 2) Invoice details, for example:
 - Amount specified on the invoice
 - Data of provided purchased services
 - Payment information

4. Methods of data provision

- 1) providing access to the Manager's information systems (Dynamics)

5. Contact persons

The Parties shall specify the contact persons who will be in charge for control of the implementation of the Data Processing Agreement.

The contact persons (employees) authorised by the Controller:

Ser. No	Forename, surname	E-mail	Tel. No
1.			

The contact persons (employees) authorised by the Processor:

Ser. No	Forename, surname	E-mail	Tel. No
1.			

6. Details and signatures of the Parties:

CONTROLLER:

UAB "Ignitis Grupės Paslaugų Centras"

(Signature)

PROCESSOR:

Retcon Sp. z o.o.

(Signature)

Security requirements

The Controller shall determine the organizational and technical means for the processing of data entrusted to the Processor. The Processor, the persons related to and authorised by the Processor must ensure the compliance with the following Security Requirements.

1. Organizational Data Security Measures

- 1.1. Personal data security policy and procedures:
 - 1.1.1. The security of personal data and their processing in the organization must be documented as part of the information security policy.
 - 1.1.2. The Security Policy must be reviewed and, where necessary, updated at least once a year.
- 1.2. Roles and responsibilities:
 - 1.2.1. Roles and responsibilities related to the processing of personal data must be clearly defined and distributed in accordance with security policy.
 - 1.2.2. The cancellation of employees' rights and obligations must be clearly defined through appropriate procedures for the transfer or assignment of roles and responsibilities (during the internal restructuring or layoffs, change of functions).
- 1.3. Access and control policy:
 - 1.3.1. Each role related to the processing of personal data must have specific access control rights, in accordance with the need to know principle.
- 1.4. Resource and asset management:
 - 1.4.1. The Processor must have a register of IT resources used to process personal data (a list of hardware, software, and network hardware). The register of IT resources must include at least the following information: type of IT resources (e.g., server, computer workstation), place (physical or electronic). The management of the registry must be assigned to a specific person, for example, IT specialist.
 - 1.4.2. The register of IT resources must be regularly reviewed and updated.
- 1.5. Change management:
 - 1.5.1. The Processor must ensure that all material changes to the IT systems are monitored and registered by specific person (for example, IT or security specialist);
 - 1.5.2. Software development should be performed in a special environment that is not connected to the IT systems used for the processing of personal data. When testing is needed, dummy data should be used (not real data). In cases that this is not possible, specific procedures should be in place for the protection of personal data used in testing.
- 1.6. Human resources:
 - 1.6.1. The Processor shall make sure that its employees process information subject to the degree of confidentiality required under the Contract and this Data Processing Agreement.
 - 1.6.2. The Processor shall make sure that respective employees of the Processor are familiar with the requirements applicable to use of information, equipment, and systems (including the established restrictions for use) in accordance with the Contract and this Data Processing Agreement. The Controller shall have the right to require the Processor to provide evidences that its employees have made themselves familiar with the content of security requirements and agree to comply with them.
 - 1.6.3. The Processor shall make sure that the Processor's employees in charge for security have been properly trained to fulfil their security-related duties;
 - 1.6.4. The Processor must ensure that at least one person having adequate competence in the area of security is responsible for the implementation of the security measures indicated in the Security Requirements.

- 1.6.5. The Processor should ensure that all employees are adequately informed about the security controls of the IT system that relate to their everyday work. Employees involved in the processing of personal data should also be properly informed about relevant data protection requirements and legal obligations through regular awareness campaigns.

2. Technical data security measures

2.1. Access control and authentication

- 2.1.1. An access control system applicable to all users accessing the IT system should be implemented. The system should allow creating, approving, reviewing and deleting user accounts.
- 2.1.2. The use of common user accounts should be avoided. In cases where this is necessary, it should be ensured that all users of the common account have the same roles and responsibilities.
- 2.1.3. An authentication mechanism should be in place, allowing access to the IT system (based on the access control policy and system). As a minimum a username/password combination should be used.
- 2.1.4. The password must be at least 8 characters long, it must include uppercase, lowercase letters and numbers.
- 2.1.5. The access control system should have the ability to detect and not allow the usage of passwords that don't respect a certain (configurable) level of complexity.
- 2.1.6. User passwords must be stored using a hash form.
- 2.1.7. A specific password policy should be defined and documented. The policy should include at least password length, complexity, validity period, as well as number of acceptable unsuccessful login attempts.

2.2. Technical journal entries and monitoring:

- 2.2.1. The records of technical journals must be implemented for each IT system, application program used for processing personal data. Technical journals must display all possible types of access to personal data records (such as date, time, review, change, cancellation).
- 2.2.2. Technical journal entries must be timestamped and protected from possible damage, tampering, or unauthorized access. Time accounting mechanisms used in IT systems must be synchronized with a common time reference source.

2.3. Protection of servers, databases:

- 2.3.1. The databases and application server servers must be configured to work properly and use a separate account with the lowest operating system privileges assigned.
- 2.3.2. Databases and Application Servers must process only those personal data that is required for work that meets the data processing objectives

2.4. Workstation protection:

- 2.4.1. Users should not be able to turn off or bypass, avoid security settings.
- 2.4.2. Antivirus applications and their virus database information must be updated at least weekly, or, as recommended, once daily or more frequently.
- 2.4.3. Users must not have the privileges (rights) of installing, removing, administering unauthorized software.
- 2.4.4. IT systems must have a set session time, i.e. outs when the user has not been active for a certain time period. Inactive session time - not more than 15 minutes.
- 2.4.5. Critical security updates released by the operating system developer should be installed regularly and without delay.
- 2.4.6. Antivirus applications and their databases of virus and malware information must be updated at least daily.

2.5. Network/Communication security:

- 2.5.1. Whenever access is performed through the Internet, communication should be encrypted through cryptographic protocols (TLS/SSL).
- 2.5.2. Any movement of data from/to the IT system must be monitored and controlled using firewalls and intrusion detection and prevention systems.
- 2.6. Back-ups:
 - 2.6.1. Backup and data restore procedures should be defined, documented and clearly linked to roles and responsibilities;
 - 2.6.2. Backups should be given an appropriate level of physical and environmental protection consistent with the standards applied on the originating data;
 - 2.6.3. Execution of backups should be monitored to ensure completeness;
 - 2.6.4. Full backups should be carried out regularly. Recommended backup frequency: daily for attached backup, weekly for full backup.
- 2.7. Mobile, portable devices:
 - 2.7.1. Mobile and portable device management procedures should be defined and documented establishing clear rules for their proper use;
 - 2.7.2. Mobile and portable devices that will be used for work and are allowed to access the information systems should be pre-registered and pre-authorized;
 - 2.7.3. Mobile and portable devices should be subject to the same sufficient levels of access control procedures (to the data processing system) as other equipment used for data processing;
 - 2.7.4. The functions and responsibilities of mobile and portable devices must be clearly defined.
- 2.8. Software security:
 - 2.8.1. Software used in information systems (for processing personal data) must comply with software security best practices, software development frameworks and standards (for example, Agile, OWASP, etc.);
 - 2.8.2. Programming standards and best practices ensuring data security must be adhered to;
 - 2.8.3. After software development, testing and verification, the basic safety requirements must already be met before the system is installed and operational;
 - 2.8.4. In cases where the Processor uses cloud services to process personal data received from the Controller (for example, storing and retaining personal data in the cloud storage):
 - 2.8.4.1. The Processor or cloud service provider must be ISO 27001 certified;
 - 2.8.4.2. Service Data Centres must be located in a country within the European Economic Area and retained data cannot be transferred outside the European Economic Area.
- 2.9. Data deletion/disposal:
 - 2.9.1. Before removing any data storage media, all data contained in it must be destroyed using software designed for that purpose, which supports reliable data-erasure algorithms. If this is not possible (for example, DVD media), physical destruction of the data medium must be performed without the possibility of recovery.
 - 2.9.2. Paper and portable data media (for example, DVD media) in which personal data was retained or stored must be destroyed by dedicated shredders or other mechanical means.
- 2.10. Physical access control:
 - 2.10.1. The physical protection of the environment, premises in which the IT system infrastructure is located, must be implemented from unauthorized access.

3. Compliance

- 3.1. At the request of the Controller, the Processor shall immediately submit to the Controller a report on compliance with the Security Requirements. The Controller will submit the report form to the Processor along with the request.
- 3.2. The aforementioned requirements shall apply at not lesser extent to all Sub-processor engaged by the Processor, provided that the Controller does not object to the engagement of sub-processors by the Processor.
- 3.3. As stated in Paragraph 8 of the Data Processing Agreement, the Controller shall have the right to make sure, through an audit, that the Service provider complies with these requirements

4. Details and signatures of the Parties:

CONTROLLER:

UAB "Ignitis Grupės Paslaugų Centras"

(Signature)

PROCESSOR:

Retcon Sp. z o.o.

(Signature)

Sub-processor engaged by the Processor

Company name	Code	Address

Details and signatures of the Parties:

CONTROLLER:

UAB "Ignitis Grupės Paslaugų Centras"

(Signature)

PROCESSOR:

Retcon Sp. z o.o.

(Signature)