AGREEMENT FOR ENTRUSTING THE PROCESSING OF PERSONAL DATA (the Agreement or the DPA)

Concluded between:

[you], hereinafter referred to as the

Controller, and

Krzysztof Gustalik - PROGUS with its registered office in Sklepowa 27, Radomsko 97-500, Poland, hereinafter referred to as the Processor.

The Controller and the Processor are hereinafter collectively referred to as the 'Parties,' and each of them individually as the 'Party.'

PREAMBLE

Due to the Parties' cooperation involving the processing of personal data, the Controller of which is the entrusting entity, and in view of the obligations under Article 28 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/WE (General Data Protection Regulation, hereinafter also referred to as 'the Regulation' or 'GDPR'), the Parties have agreed to enter this Personal Data Processing Agreement as follows.

§ 1. ENTRUSTING THE PROCESSING OF PERSONAL DATA

1. The Controller entrusts the Processor with personal data for processing, pursuant to Article 28 of

   Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation, hereinafter also referred to as 'the Regulation' or 'GDPR'), and under the terms and for the purpose set out in this Agreement.
2. The Processor undertakes to process the personal data entrusted to it in accordance with this Agreement, the Regulation and other provisions of generally applicable laws that protect the rights of data subjects.
3. The Processor declares that applies security measures that meet the requirements of the Regulation.

§ 2. SCOPE AND PURPOSE OF DATA PROCESSING

1. The **Processor** will process the personal data entrusted under the Agreement, in particular:
   1) Identification data e.g.:
      a. First name,
      b. Last name,
      c. Registration data (e.g. national court register number),
      d. Tax ID number,
   2) Contact data e.g.:
      a. Email address,
      b. Phone number,
   3) Device data e.g.:
      a. IP address,
      b. Location data,
   4) Transactional and sales data e.g.
      a. Payment receipts,
      b. Credit/debit card data,
      c. PayPal account data,
      d. Order information
   5) Data proceeded during interactions with end-users via the communication channels,
   6) Other data processed in regard to Services (applicable to the specific type and scope of Services).
2. Data processing will concern the following categories of data subjects:
   1) End-users – individuals who interact with the **Controller** by way of the PROGUS communication platform; end-users provide the personal data willingly.
3. Personal data shall be entrusted for the purpose of providing services by the **Processor**
4. The **Processor** may process personal data entrusted to it only to the extent and for the purpose specified in the Agreement and to the extent and for the purpose necessary to provide services specified in the main agreement entered into between the Controller and the Processor (hereinafter "**Main Agreement**").

§ 3. TERM OF CONTRACT

1. The Processor is authorized to perform processing activities on behalf of the Controller for the term of the Agreement.

2. The Agreement shall be concluded for the period of validity of the Main Agreement, and the termination, cancellation or expiration of the Main Agreement shall result in the simultaneous termination, cancellation or expiration of the Agreement, respectively, without the need for the Parties to make additional statements in this regard.

§ 4. OBLIGATIONS OF THE PROCESSOR

1. The **Processor** hereby declares that it has the infrastructure, resources, experience, knowledge and qualified personnel, to the extent enabling the proper execution of the Agreement, in accordance with applicable laws. In particular, the **Processor** declares that it is familiar with the principles of processing and securing personal data resulting from:
   1) GDPR;
   2) the applicable national regulations.
2. The **Processor** is obliged to:
   1) process entrusted personal data only on the basis of the Agreement and process the personal data only on the documented instructions of the **Controller,** unless this is required by law to which the **Processor** is subject . In a situation where the **Processor**'s obligation to process personal data arises from legal provisions, the **Processor** shall inform the **Controller** by electronic means of this legal requirement, unless that law prohibits such information due to important public interest considerations;
   2) process entrusted personal data in accordance with the Regulation, regulations adopted to enable the Regulation to be applied, other applicable legal provisions, the Agreement and the **Controller's instructions**;
   3) grant access to the entrusted personal data only to persons who, due to the scope of their tasks, have been authorized by the **Processor** to process them, and have undertaken to maintain the confidentiality of the processed data;
   4) implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk of violating the rights or freedoms of individuals whose personal data will be processed under the Agreement (Article 32 of the GDPR) and to ensure the implementation of principles of data protection by design and data protection by default (specified in Article 25 of the GDPR);
   5) maintain documentation describing the processing of data by the **Processor**, including, in particular, the record of processing activities (Article 30 of the GDPR);
   6) immediately notify the **Controller** of any violation of personal data protection;
   7) support the **Controller** in the performance of the duties specified in art. 32-36 GDPR taking into account the nature of processing and the information available to **the Processor**;
   8) taking into account the nature of the processing support the **Controller** (through the application of appropriate technical and organizational measures) in the fulfilment of the obligation to respond to requests of data subjects in the exercise of their rights set out in Chapter III of the Regulation;

9) make available to the **Controller** upon request, no later than within 30 working days, all information necessary to demonstrate the **Processor**'s compliance with the obligations set forth in the applicable law, in particular the Regulation, including information on the safeguards used, identified risks and incidents in the area of personal data protection;

10) immediately notify the **Controller** if, in its opinion, the instruction violates this Regulation or other Union or Member State data protection provisions;

11) without undue delay inform (if it does not lead to violation of the applicable law) the **Controller** of any proceedings, in particular administrative or judicial ones, concerning the processing of personal data by the **Processor**, any administrative decision or rulings concerning the processing of personal data entrusted to

12) inform **Controller** of any controls and inspections regarding the processing of personal data entrusted to the **Processor**, in particular those carried out by the supervisory authority, as well as any complaints from data subjects related to the processing of their personal data;

13) store personal data only for as long as designated by the **Controller**, and without undue delay update, correct, modify, anonymize, limit processing or delete personal data in accordance with the **Controller's** instructions (if such action would result in the inability to continue implementation of the processing activities, the **Processor** will inform the **Controller** prior to taking such action, and then follow the **Controller's** instructions);

14) return or delete in a permanent manner, upon the termination, expiration or termination of this Agreement, all personal data provided by the **Controller** and delete existing copies, unless Union, Member State law or state law to which the **Processor** is subject in the United States of America, requires storage of the personal data.

§ 5. PERSONAL DATA SECURITY

1. In order to assure the personal data security, the **Processor** has established certain defense mechanisms that are interrelated. These mechanisms include physical securities, equipment-related measures, organizational procedures and IT solutions. The Parties agree that by appropriate technical and organizational measures they mean the safeguards indicated below.
2. The **Processor** assures that the physical securities include, in particular:
   1) Access to personal data by the authorized persons only;
   2) Storing physical data collections in the locked cabinets / premises, including servers that store data in electronic form;
   3) 24-hour protection of the premises where personal data are stored.
3. The **Processor** assures that the measures related to equipment include, in particular:
   1) Equipment used within the IT system which is applied for personal data processing providing appropriate data access securities;
   2) Storage of personal data on servers of third-party companies that provide adequate standards for the protection of personal data supported by contractual provisions providing for the terms of storage of data by third parties;

3) Management of personal data processing equipment has been entrusted to professionals operating within the Processor;

4) Using a shredder to effectively remove all the documents containing personal data.

4. The **Processor** assures that the organizational procedures include, in particular:

1) Training of the personnel having access to the data;

2) Periodical audits regarding personal data protection;

3) Application of mechanisms of privacy by design and privacy by default;

4) Assessment of the influence on the data processing case by case;

5) Obligation to exercise due diligence to ensure that data protection complies with the actually binding requirements, including adjustment of the Policy and Directives to the changing legal environment.

5. The **Processor** assures that the protective measures within IT solutions consist in, in particular:

1) Restrict access to devices and applications via ID and a password;

2) Restrict a user's access to only certain resources by providing them with a specific range of privileges from the administrator's level;

3) Application of programs aiming at the actual monitoring of the malicious software presence;

4) Updating the used software on current basis;

5) Protection of the local network against the actions initiated from outside by using a firewall;

6) Making back-ups.

6. Selected aspects of the **Processor's** security measures applied under the Agreement are described on the website: https://www.PROGUS.com/knowledge/faq/how-are-the-security-matters-handled- at-PROGUS/

§ 6. OBLIGATIONS OF THE CONTROLLER

1. The **Controller** is obliged to:

1) cooperate with the **Processor** in the implementation of the provisions of this Agreement, provide explanations in the event of doubts as to the legality of the **Controller's** instructions, as well as perform its specified duties in a timely manner;

2) entrust only those Personal Data that has been obtained and are processed by the **Controller** in accordance with applicable laws, including the GDPR. In particular, the **Controller** confirms that (i) it has collected and holds the legally required consents for direct marketing activities, including consents to send commercial information by electronic means and to use telecommunication means and automatic systems for direct marketing purposes - if such activities are carried out, (ii) has provided data subjects with information about the processing of their data to the extent and in the manner required by the GDPR, and (iii) is authorized to process the Personal Data and entrust it to the **Processor** for processing within the scope and purpose specified in § 2 above. In addition, if the

Controller is not the controller of the Personal Data, it confirms that it has obtained the consent of the relevant **Controller** to entrust **Processor** with further processing of the Personal Data for such purpose and scope.

§ 7. RIGHT OF CONTROL - AUDIT

1. The **Controller** is authorized to audit the compliance of the processing of personal data by the **Processor** with the Agreement and applicable law. The audit may only cover the control of the relevant documentation and the right to obtain the necessary information / explanations. The **Processor** has the right to refuse to provide documentation or to provide information / explanations to the extent that the audit could threaten the disclose personal data other than those processed by the Processor under the Agreement or to disclose company secrets.
2. The audit referred to in item 1 above may be performed by the **Controller** or third parties to whom the **Controller** entrusts the performance of the audit at the place where personal data are processed.
3. The **Processor** is required to cooperate with the **Controller** and auditors authorized by the **Controller.**
4. The audit is subject to the following conditions:
    1) it may only concern Personal Data entrusted to **Processor** for processing pursuant to the Agreement;
    2) it shall be conducted efficiently and in the shortest possible time, not longer than 2 working days;
    3) take place no more frequently than once a year, unless an audit is required by law or by the applicable supervisory authority, or immediately upon discovery of a material breach of the Personal Data processed under the Agreement,
    4) may be performed during the **Processor's** normal business hours, in a manner that does not interfering with Processor's business activities and in accordance with the **Processor's** security policies;
    5) the **Controller** will notify the **Processor** of the intention to carry out the audit by email or letter at least 14 working days before the scheduled audit date. In the event that the **Processor** is unable to conduct the audit on the scheduled date or other unforeseen obstacles, the **Processor** will notify the **Controller** of these circumstances and will propose a new audit date, but not later than within 7 working days from the date indicated by the **Controller**;
    6) Costs associated with the audit shall be borne by the **Controller** without the right to claim reimbursement of such costs or payment of additional compensation;
    7) The audit must not aim at or lead to the disclosure of legally protected secrets (including business secrets of the **Processor**). The **Controller** is obliged to create an audit report summarizing the findings of this audit. The report will be provided to the **Processor** and will constitute confidential information about the **Processor**, which cannot be disclosed to third parties without the consent of the **Processor**, unless required by applicable law.

§ 8. FURTHER ENTRUSTING DATA FOR PROCESSING

1. The **Processor** may entrust the processing of personal data covered by the Agreement to a third party – (general consent of the **Controller)**.
2. In the event of further entrustment of personal data covered by this Agreement, the **Processor** guarantees that the entities to which it has entrusted these data meet all the conditions for processing personal data referred to in the Regulation, and will fulfill all the obligations set forth in this Agreement.
3. The **Processor** declares that in the performance of the agreement it will use the services of:
   a) Krzysztof Gustalik - PROGUS as an entity which is a member of the capital group to which the **Processor** belongs in so far as providing technical and organizational support services to the **Processor**;
   b) other entities to whom the **Processor** or Krzysztof Gustalik - PROGUS entrusts the data in connection with the provision of necessary services to the **Processor** for the proper performance of the Main Agreement,

   which entities will have the status of another processor within the meaning of Article 28(2) of the RODO ("**Sub-Processor**"). The Controller shall be informed by the Processor about the change of the list of sub-processors (possible in electronic form, including as part of information on the website).
4. The Processor shall process data primarily within the European Economic Area (EEA). If it is necessary to process data outside the EEA (e.g. due to the use of sub-processors) in a country for which no adequacy decision has been issued by the European Commission, the Processor undertakes that the transfer will take place on the basis of one of the mechanisms set forth in Chapter V of the GDPR, in particular the conclusion of the Standard Contractual Clauses with the identification of appropriate technical or organizational measures.
5. The **Processor** is located in third country. **The Parties** agree to implement the Standard Contractual Clauses, attached as Schedule nr 1 to the DPA, as the legal basis for the transfer of data to the third country under this Agreement.

§ 9. RESPONSIBILITY OF THE PROCESSING PARTY

1. The **Processor** undertakes not to transfer or use personal data in a manner that could result in a breach of the Agreement, such as, in particular, entrusting access to personal data to unauthorized persons.
2. **Each Party** shall immediately inform the **other Party** of any proceedings, in particular, administrative or judicial, relating to the processing by either **Party** of the personal data specified in the Agreement, any administrative decision or ruling regarding the processing of such data addressed to the **Party**, as well as any planned, if known, or carried out audits and inspections relating to the processing of such personal data, in particular those carried out by the supervisory authority.

3. The contractual and tort liability of the **Processor** is limited to the direct losses incurred by the **Controller**. The **Processor** shall not be liable for lost profits, regardless of their source, except in the case of willful misconduct or gross negligence.
4. The **Processor'** total liability, regardless of the number and basis of the **Controller's** claims, is limited to the equivalent of the fixed subscription fee for a period of 3 (three) months, paid by the **Controller** for the Services during the billing period immediately preceding the date of the event causing the damage, excluding amounts comprising installation fees or additional charges of any kind. The **Controller** shall indemnify the **Processor** for liabilities in excess of the above limitation.
5. The **Processor** shall not be liable for improper performance or non-performance of the Services as a result of Force Majeure.
6. The **Parties** agree that the **Controller** shall be responsible for indemnifying the claims of data subjects caused as a result of incorrect processing of Personal Data under the DPA, unless **Controller** proves that the damage resulted from the sole fault of the **Processor** or its subcontractors. If the above is not proven, the **Controller** shall unconditionally release the **Processor** from any claims made by entities whose Personal Data is processed by the **Processor** under the Terms and Conditions. In the event of initiating court proceedings against **Processor**, the Controller shall be obliged, on the **Processor's** request, to intervene as a party to such proceedings and assume responsibility for the asserted claim.

§ 10. PRINCIPLES OF CONFIDENTIALITY

1. **Each Party** undertakes to keep confidential all information, data, materials, documents and personal data received from the **other Party** and from the persons cooperating with it, as well as data obtained in any other way, deliberate or accidental in verbal, written or electronic form ('data confidential').
2. **Each Party** declares that due to the obligation to keep confidential data secret, it will not be used, disclosed or made available without the written consent of the **other Party** for any purpose other than the performance of the Agreement, unless the necessity to disclose the information is required by applicable law or the Agreement.

§ 11. FINAL PROVISIONS

1. The **Parties** declare that there are no other arrangements in this Agreement that would modify or supplement its provisions.
2. Any issues not regulated by the provisions of this Agreement shall be governed by appropriate Polish Law Regulations.
3. Matters arising out of the implementation of the provisions of this Agreement will be settled by the common court of competent jurisdiction of the **Processor**.
4. The contract was drawn up in two identical copies, one for each **Party**.

Schedules:

1. Standard Contractual Clauses (SCC) – Modul Two: Controller to Processor.

Schedule 1 to DPA

STANDARD CONTRACTUAL CLAUSES

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)[1] for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter "entity/ies") transferring the personal data, as listed in Annex I.A. (hereinafter each "data exporter"), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A. (hereinafter each "data importer")

have agreed to these standard contractual clauses (hereinafter: "Clauses").

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46 (2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down

---

[1] Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295 of 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision […].

in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8.1(b), 8.9(a), (c), (d) and (e);

(iii) Clause 9(a), (c), (d) and (e);

(iv) Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18(a) and (b);

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7 - Optional

Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the

extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter "personal data breach"). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter "sensitive data"), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union[2] (in the same country as the data importer or in another third country, hereinafter "onward transfer") if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

---

2 The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

(a) The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least 3 days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects.[3] The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure

[3] This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby - in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent - the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) Each Party shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages that the Party causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter under Regulation (EU) 2016/679.

(c) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(d) The Parties agree that if one Party is held liable under paragraph (c), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.

(e) The data importer may not invoke the conduct of a processor or sub-processor to avoid its own liability.

Clause 13

Supervision

(a) [Where the data exporter is established in an EU Member State:] The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679:] The supervisory authority of the Member State in which the

representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679:] The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by

such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards[4];

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a). [For Module Three: The data exporter shall forward the notification to the controller.]

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation [for Module Three: , if appropriate in consultation with the controller]. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by [for Module Three: the controller or] the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

---

4 As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

Clause 15

Obligations of the data importer in case of access by public authorities

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request. [For Module Three: The data exporter shall make the assessment available to the controller.]

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority [for Module Three: and the controller] of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) [For Modules One, Two and Three: Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data.] [For Module Four: Personal data collected by the data exporter in the EU that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall immediately be deleted in its entirety, including any copy thereof.] The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data

importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

These Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of Poland.

Clause 18

Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of Poland.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

ANNEX I

A. LIST OF PARTIES

Data exporter(s): [*Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]*

Entity who is party to the DPA with the Processor
Role (controller/processor): CONTROLER

Data importer(s): [*Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]*

Name:
Krzysztof
Gustalik -
PROGUS
Address:
Sklepowa 27 Radomsko 97-500, Poland
Contact person's name and contact details:
Krzysztof Gustalik, mail: contact@proguscommerce.com
Activities relevant to the data transferred under these Clauses:
As described in the DPA to which these SCCs are annexed
Signature and date:
In accordance with the DPA
Role (controller/processor): PROCESSOR

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

As described in the DPA to which these SCCs are annexed

Categories of personal data transferred

As described in the DPA to which these SCCs are annexed

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

As described in the DPA to which these SCCs are annexed

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

As described in the DPA to which these SCCs are annexed

Nature of the processing

As described in the DPA to which these SCCs are annexed.

Purpose(s) of the data transfer and further processing

As described in the DPA to which these SCCs are annexed;

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

As described in the DPA to which these SCCs are annexed.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

As described in the DPA to which these SCCs are annexed

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13

The competent supervisory authority is authority of the registered office of the main establishment or of the single establishment of the data exporter.

ANNEX II - TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Description of the technical and organizational measures implemented by the data importer(s)

- *Measures of pseudonymization and encryption of personal data.*
  PROGUS applies safeguards in the form of pseudonymization of personal data by implementing appropriate IT systems and introducing guidelines in the Organization for pseudonymization.

  PROGUS applies encryption to personal data. All documents contain personal data sent within the organization and to third parties are encrypted through software that provides an adequate degree of protection.

- *Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident.*
  PROGUS's infrastructure is designed to meet the scalability and continuous availability requirements of our service. Systems are monitored 24/7 to respond to potential operational issues.

  For personal data processed electronically, PROGUS provides permanent network monitoring to enable incident detection and prompt response. In addition, PROGUS performs data back-up, which enables prompt restoration if access is lost due to e.g. an incident.

- *Processes for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures in order to ensure the security of the processing.*
  The main activity of the PROGUS is to provide services related to the offered application. The application is constantly subjected to security tests focused on system penetration (with particular attention to personal data) in order to identify potential errors. These activities are implemented in the software development cycle and constitute its inherent part. The bugs found are fixed immediately and the system is tested again after the corrections are made. PROGUS also runs a non-public bug bounty program under a "responsible disclosure" model. Reports submitted by researchers are evaluated by the security team and further steps are taken based on the evaluation.

  The controller also conducts regular testing, assessing and evaluating the analysis of technical measures used internally to ensure that appropriate technical and organizational measures are implemented and that the necessary safeguards are put in place to meet the requirements under the RODO and the need to protect the rights of data subjects.

  To ensure practical application, the organization's employees are trained on secure practices and processes through cyber security awareness. Each employee must meet a series of security requirements for their digital accounts and physical devices. Only employees who need to work with data have access to it. Physical access to employee premises is restricted through electronic access cards or security available in the building. Access to the organization's network is restricted through a VPN that only employees of the organization have access to.

- *Measures for user identification and authorization.*
  Each user authenticates in the application using e-mail address and password (password-based authentication), which established during the registration process;

- ✓ The password established by the user must have a minimum of 8 characters
- ✓ The password can be changed by the user at any time after providing the current password
- ✓ The password is sent to the application via a secure communication channel and is stored as a strong irreversible hash in a protected database.

Additionally, while setting the password, the user has the possibility to check how strong the password is in order to establish its proper length and complexity. The authentication process is protected against brute force attacks that attempt to guess the user's password.

Each correctly authenticated user receives a long, random, unique token with high entropy, which authorizes him to perform authorized actions in the application. This token loses its value when the user logs out of the application and cannot be used again to authorize his/her requests. Access control in the application is implemented based on the RBAC (role-based access control) model, which is configurable by the project owner.

- *Measures for the protection of data during transmission.*
  All traffic exchanged between the user and the application is encrypted using TLS protocol with strong cryptographic algorithms. This provides protection against attacks trying to eavesdrop the communication between the user and the application. What is more, the communication with the application over the encrypted channel is forced by the application itself.

- *Measures for the protection of data during storage.*
  Access is granted only to employees who need it to perform their duties. The access list is reviewed on an ongoing basis.

- *Measures for ensuring physical security of locations at which personal data are processed.*
  Personal information is held on servers provided by our third-party service provider, which ensures that only authorized employees have physical access to the servers. Additionally, the data centers where the servers are located are continuously monitored and protected by guards. The server rooms are equipped with fire suppression systems.

- *Measures for ensuring events logging.*
  Applications and services offered by PROGUS log detailed information about: successful and unsuccessful login attempts, created accounts, password recovery processes, data access, changes in account settings and other relevant events.

  All logs go to a centralized system, which allows for analysis and detection of potential attacks. Depending on the type of logged events, the monitoring system is ready to signal an alarm in case of anomalies.

- *Measures for ensuring system configuration, including default configuration*
  PROGUS uses standard system configurations. The systems are continuously monitored and maintained in vulnerability-free versions.

  Ensure that critical or significant security updates/patches are installed in accordance in application programs (including browsers), application programs (including browser, plug-ins, PDF reader, etc.), security infrastructure (scanner d. in security infrastructure (virus scanner, firewall, IDS systems, content filters, routers, etc. internal server operating systems.

· *Measures for internal IT and IT security governance and management.*
PROGUS has a security and risk management program that includes the following aspects:

- ✓ Employee accounts are assigned privileges according to the principle of least privilege - meaning that an individual has the minimum level of privilege that is necessary for them to perform the duties of their position.
- ✓ Employees are trained on security and privacy best practices.
- ✓ Access to resources by an employee is closely tied to their employment status. Upon termination, all access to resources is immediately revoked.
- ✓ Employees are required to use multi-step authentication using secure components such as TOTP tokens or U2F hardware keys.
- ✓ Access to the internal network infrastructure is only possible via VPN from the employee's device.
- ✓ Employee access privileges are periodically verified.
- ✓ Employee email addresses are regularly searched in a public data leak database.

· *Measures for ensuring accountability.*

- ✓ PROGUS conducts company-internal audits of the application and maintenance of an adequate level of personal data protection and security, in particular IT;
- ✓ PROGUS has implemented the documentation necessary for the proper processing of personal data in accordance with the law, in particular as required by the GDPR regulation;
- ✓ Based on the risk analysis conducted and related to cyber security, procedures and policies have been developed and implemented to ensure an appropriate level of protection;
- ✓ All documentation related to the protection of personal data as well as the safeguards applied, especially IT safeguards, is kept in electronic or physical form;
- ✓ PROGUS also introduced various factual solutions, among others:
  - limiting accessibility to data by employees;
  - employee training, including access to employee training materials to raise and ensure an appropriate level of awareness in Ogranization.

· *Measures for allowing data portability and ensuring erasure.*
PROGUS has functionality that allows you to delete your account along with its associated data at the request of the account owner

ANNEX III – LIST OF SUB-PROCESSORS

The controller has authorised the use of the following sub-processors:

1. *Name:* Krzysztof Gustalik - PROGUS

Address: Sklepowa 27 Radomsko, Poland

Contact person's name and contact details:

Krzysztof Gustalik, e-mail: contact@proguscommerce.com

Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorised): ...

As described in the DPA to which these SCCs are annexed

2. *Name: .....*

Address: ....

Contact person's name, position and contact details: ....

Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorised): ...