DATA PROCESSING AGREEMENT

Last updated on 14 August 2026

This **DATA PROCESSING AGREEMENT** (hereinafter also "**Agreement**") is a binding legal agreement between AJAX SYSTEMS TRADING FZE (hereinafter "**Ajax**" or "**Processor**") and the Controller of Ajax Products and Software, as defined in Section 1 of this Agreement (hereinafter also the "**Controller**"), each individually referred to as a "Party" and jointly as the "Parties".

By using the Ajax Products and Software, the end user accepts and enters into this Agreement; the end user (and its signatory, if applicable) represents and warrants that the end user and its signatory have the legal capacity and authority to enter into this binding Agreement and adhere to its terms, and that the end user will act in accordance with this Agreement and all applicable laws.

BACKGROUND AND PURPOSE

A. Under this Agreement, the Processor, the Controller, and any relevant third parties (i.e., Sub-processors) specified in the Agreement and approved by both Parties are involved in the provision of the Services, which requires Personal Data (as defined below) to be processed by the Processor on behalf of the Controller. The Processor may process Personal Data on behalf of the Controller under the terms of this Agreement and all its integral parts, e.g., appendices, amendments, etc.

B. The Parties seek to implement this Agreement in compliance with the requirements of the applicable legal framework relating to data processing and with Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (hereinafter also the "General Data Protection Regulation" or "GDPR") on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

C. The purpose of this Agreement is to agree upon the privacy and data protection practices to be applied in the provision of the Services (as defined below). This Agreement and other related contractual materials constitute a data processing agreement as required by Article 28 of the GDPR. The Parties intend this Agreement to be interpreted in a manner consistent with this objective and with their obligations under the GDPR and other applicable data protection laws. Unless the context otherwise requires, terms used in this Agreement and the enclosures hereto shall have the same meaning as in the GDPR.

1. DEFINITIONS AND INTERPRETATION

Unless otherwise defined herein, capitalized terms and expressions used in this Agreement shall have the following meanings:

1.1 "**Agreement**" means this Data Processing Agreement and all the appendices, annexes, and supplementary documentation. References in this Agreement to the "End User Agreement" mean the Ajax End User Agreement at https://ajax.systems/end-user-agreement/;

1.2 "**Controller**" means the account holder who has registered an account to use the Ajax Products and Software as an end user and determines the purposes and means of the processing of Personal Data carried out by the Processor on its behalf. The Controller may be a natural or a legal person.

1.3 "**Data Protection Regulations**" means EU Data Protection Laws (including but not limited to the EU General Data Protection Regulation 2016/679 and laws implementing or supplementing the GDPR) and, to the extent applicable, the data protection or privacy laws of any other country relevant to the processing under this Agreement;

1.4 "**EEA**" means the European Economic Area;

1.5 "**Personal Data**" means any information that relates to an identified or identifiable natural person that the Processor processes on behalf of the Controller pursuant to or in connection with the End User Agreement at https://ajax.systems/end-user-agreement/ or any other agreement, if additionally agreed between the Parties.

1.6 "**Services**" means the services provided by the Processor to the Controller in connection with the Ajax Products and Software.

1.7 "**Instructions**" means any instruction given by the Controller to the Processor regarding the processing of Personal Data, whether provided (a) through the functionality of the Ajax Products and Software; (b) through technical agreements, annexes, or other documentation agreed upon with the Processor; or (c) in any other manner agreed between the Parties in writing. For the avoidance of doubt, the Processor is not required to verify the legal basis or appropriateness of Instructions unless they conflict with applicable Data Protection Regulations.

1.8 "**Sub-processor**" means any relevant third party appointed by or on behalf of the Processor to process Personal Data and any other related data on behalf of the Controller under the terms of the Agreement.

1.9 **"Ajax Products and Software"** means the hardware products and related software made available by Ajax under the End User Agreement at https://ajax.systems/end-user-agreement/.

2. PURPOSES OF DATA PROCESSING

2.1 The subject matter of the processing under this Agreement is the Personal Data generated through or in connection with the Controller's use of the Ajax Products and Software, which the Processor processes on behalf of the Controller for the purposes set out in this Section 2.

2.2 The processing consists of the collection, storage, organization, transmission, retrieval, and deletion of Personal Data by means of the Processor's cloud infrastructure, and any other operation necessary to give effect to the purposes set out in clause 2.3 of this Agreement.

2.3 The Processor shall process Personal Data under the documented Instructions of the Controller as stipulated in clause 3.1 of this Agreement, for the following purposes:

(a) to operate the cloud infrastructure that receives, processes, and stores events, alerts, and other data generated by the Ajax Products and Software, and to transmit corresponding notifications to the Controller;

(b) to enable the Controller's remote access to and control of the Ajax Products and Software, including access to recordings and event history generated by the devices;

(c) to provide technical support to the Controller in connection with its use of the Ajax Products and Software;

(d) to enable the Controller, through documented Instructions, to share access to the Ajax Products and Software and related Personal Data with third parties authorized by the Controller, as further described in clause 3.3 of this Agreement.

2.4 The Processor processes Personal Data for the duration set out in Section 9 of this Agreement.

2.5 The categories of data subjects and the categories of Personal Data processed under this Agreement are set out in Annex 1.

3. GENERAL OBLIGATIONS REGARDING PROCESSING OF DATA

3.1 **Instructions**. The Processor shall process Personal Data solely:

(a) for the purposes set out in Section 2 of this Agreement;
(b) on the Controller's documented Instructions; and
(c) in compliance with applicable Data Protection Regulations.

The Controller shall not instruct the Processor to process Personal Data in violation of applicable law. The

Processor shall have no liability for any harm or damage resulting from its compliance with Instructions that the Controller was not lawfully entitled to give. If the Processor reasonably believes that an Instruction infringes applicable Data Protection Regulations, it shall, unless legally prohibited, promptly inform the Controller in writing and may suspend processing of the affected Personal Data (other than merely storing and maintaining the security of such data) until the Controller provides new Instructions with which the Processor is able to comply. During any such suspension, the Processor shall not be liable for any failure to perform obligations that depend on the suspended processing.

3.2 The Processor shall comply with applicable Data Protection Regulations and shall implement appropriate systems and procedures to ensure that any Personal Data processed under this Agreement is adequate, relevant, not excessive, accurate, and not retained for longer than necessary.

3.3 The Controller may, through documented Instructions, authorize the Processor to share Personal Data with the following categories of third parties, each acting as an independent data controller in respect of the Personal Data it receives:

(a) professional monitoring and alarm receiving centre (ARC) companies engaged by the Controller;

(b) security and guarding service companies engaged by the Controller;

(c) installation and maintenance engineers to whom the Controller has granted PRO account access rights.

The Processor shall transfer Personal Data to such third parties only on the Controller's documented Instructions and shall bear no responsibility for their subsequent processing.

3.4 The Processor is hereby authorized to respond directly to requests from data subjects relating to the exercise of their rights under applicable Data Protection Regulations in connection with the processing under this Agreement. The Processor shall notify the Controller of any such request and the substantive action taken no later than five (5) business days after acting on the request. The Processor's obligation to assist shall be limited to measures that are technically feasible, taking into account the nature of the processing.

3.5 The Processor shall further provide the Controller with commercially reasonable assistance in ensuring compliance with the Controller's obligations to perform security and data protection impact assessments, make breach notifications, and conduct prior consultations with the competent supervisory authority, as set out in the applicable data protection law, considering the nature of the processing and the information available to the Processor.

3.6 Taking into account the state of the art, the costs of implementation, and the nature, scope, context, and purposes of processing carried out by the Processor hereunder, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the Processor shall implement appropriate technical and organizational measures to safeguard the Personal Data against unauthorized and unlawful processing as well as accidental loss, alteration, or destruction.

3.7 Such measures shall include, where appropriate and relevant for each processing action:

i. the pseudonymization and encryption of the Personal Data;

ii. the ability to ensure the ongoing confidentiality, integrity, availability, and resilience of processing systems and services;

iii. the ability to restore the availability of and access to the Personal Data in a timely manner in the event of a physical or technical incident;

iv. a process for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

3.8 In addition, the Processor shall, and shall procure that its personnel shall:

i. promptly provide all such information to the Controller as the Controller may require to allow the Controller to comply with its obligations regarding the rights of data subjects, including access rights, or with notices and requests served by any data protection authorities;

ii. ensure that persons processing the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality; and

iii. promptly notify the Controller of any queries from data subjects, the data protection ombudsman, or any other law enforcement or regulatory authority.

4. TRANSFER OF PERSONAL DATA OUTSIDE THE EEA

4.1 Personal Data shall not be transferred outside the European Economic Area without the prior written consent of the Controller, unless the third party is or agrees to be bound by the SCC or the transfer falls within the cases specified in this Agreement, particularly in clause 4.2.

4.2 The Controller is also informed and grants authorisation for the Processor to transfer Personal Data outside the European Union or the European Economic Area in order to fulfill the terms and obligations of this Agreement. In such cases, the Processor hereby undertakes to ensure a high level of protection for transfers of Personal Data outside the EU/EEA by including, as appropriate, in the relevant agreements, the standard clauses for international data transfers set out in Commission Implementing Decision (EU) 2021/914, or by implementing another appropriate safeguard in accordance with the Data Protection Regulations.

4.3 Any term of this Agreement that would result in the standard clauses referred to in clause 4.2 above being deprived of their effect as adequate safeguards under Article 46 of the GDPR shall not apply to the extent that such term would have this effect.

5. AUDITS

5.1 Pursuant to Clause 8.9 of the SCC, the Parties agree to the following modalities for the exercise of audit rights under this Agreement:

i. to conduct an audit under this Agreement, the Parties shall engage only independent auditors who must sign a non-disclosure agreement with the Processor;

ii. the audit shall not involve access to the premises or information systems of the Processor and shall only be conducted in documentary form;

iii. the audit may be conducted no more than once a year upon written notification to the Processor at least thirty (30) calendar days prior to the scheduled start date of the audit;

iv. all costs of any such audit shall be paid by the Controller in full; and

v. any audit by the Controller shall in no way limit the Processor’s obligations and liability under this Agreement.

5.2 Nothing in this Section shall be construed as limiting or restricting the Controller's rights under Clause 8.9 of the SCC. The procedures set out in this Section constitute the practical modalities through which those rights will ordinarily be exercised.

6. BREACHES

6.1 The Processor shall notify the Controller without undue delay, but at the latest within seventy-two (72) hours after having become aware of any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data processed on behalf of the Controller (“**Breach**”). Where the Processor has reasonable grounds to believe that such a Breach has occurred, it shall inform the Controller accordingly. The Processor shall not notify a

supervisory authority or any data subject of a Breach on the Controller's behalf unless instructed by the Controller in writing or required to do so by applicable law.

6.2 The Processor shall provide the Controller with all relevant information as regards the Breach. The Processor's notification of the Breach to the Controller shall include at least the following:

i. a description of the nature of the Breach and the information affected by it;

ii. the name and contact details of the Processor's contact point where more information can be obtained;

iii. a description of the measures taken by the Processor to address the Breach, including, where appropriate, measures to mitigate its possible adverse effects.

6.3 The Processor shall document all Breaches, including the facts surrounding each Breach, its effects, and the remedial actions taken.

7. USE OF THIRD PARTIES IN DATA PROCESSING

7.1 **General authorization.** The Controller gives its general authorization for the Processor to involve the Processor's affiliated companies and other subcontractors as sub-processors to process Personal Data in connection with the Services ("**Sub-processors**"), provided that such appointment does not lead to non-compliance with any applicable law or the Processor's obligations under this Agreement. The Processor shall maintain a list of the Sub-processors used by the Processor in the Ajax GDPR White Paper (FAQ) at https://ajax.systems/gdpr-white-paper/. The Processor shall ensure that the engaged Sub-processors are properly qualified and are contractually bound by data protection obligations no less protective than those stipulated under this Agreement, whether by way of a data processing agreement or other binding contractual documentation.

7.2 **Change of Sub-processor.** Pursuant to Clause 9 of the SCC set out in Appendix 1, the Processor's obligation to inform the Controller of the addition or replacement of a Sub-processor is fulfilled by updating the list of Sub-processors published in the Ajax GDPR White Paper (FAQ) at https://ajax.systems/gdpr-white-paper/, and by notifying the Controller by email to the address registered in the Controller's account and/or by a notification within the Ajax Products and Software. Such notification shall be sent at least five (5) business days before the new or replacement Sub-processor begins processing Personal Data under this Agreement. The Controller may object to such change within that period by notifying the Processor in writing. If no objection is received before the end of that period, the change shall be deemed accepted.

8. DELETION AND RETURN OF PERSONAL DATA

8.1 Upon termination or expiry of the End User Agreement, closure of the Controller's account, or upon the Controller's request, the Processor shall, at the choice of the Controller, delete or return to the Controller all Personal Data processed on the Controller's behalf and delete existing copies, unless applicable law requires further storage. The Controller may change its choice at any time before the end of the provision of the Services by notifying the Processor in writing.

8.2 Where the Controller has not communicated its choice under clause 8.1 within thirty (30) calendar days of the relevant event, the Processor shall delete the Personal Data.

8.3 Deletion from the Processor's live production systems shall be completed within thirty (30) calendar days of the date of the relevant request or the event referred to in clause 8.1, as applicable.

8.4 Personal Data may remain in encrypted backup copies after deletion under clause 8.3 for the duration of the Processor's backup retention cycle, which does not exceed twelve (12) months. During that

period, such Personal Data is not processed for any other purpose, access to it is restricted, and it is permanently deleted upon expiry of the applicable backup cycle. In the event of restoration from a backup, the Processor shall remove the Personal Data of Controllers whose data was previously deleted before the restored data is used in production.

8.5 Until deletion or return is completed, the Processor shall continue to ensure compliance with this Agreement in respect of the Personal Data concerned.

8.6 The Processor shall, upon the Controller's request, confirm to the Controller in writing that deletion has been completed.

8.7 Where applicable law requires the Processor to retain Personal Data beyond the periods set out in this Section, the Processor shall inform the Controller of that requirement, unless prohibited from doing so by law, and shall process the retained Personal Data only to the extent and for as long as required.

9. TERMINATION AND MISCELLANEOUS

9.1 This Agreement enters into force simultaneously with the End User Agreement and forms an integral part thereof from the date the Controller accepts the End User Agreement at https://ajax.systems/end-user-agreement/. This Agreement shall continue to be in force until the Processor has ceased to process Personal Data on the basis of the Services or any agreement between the Parties and fulfilled the obligations relating to the completion of processing, unless otherwise agreed in writing between the Parties.

9.2 Termination or expiry of this Agreement does not release the Parties from any obligation of confidentiality or any other responsibilities under this Agreement.

9.3 Ajax may amend this Agreement by publishing an updated version on the Ajax website, by email notification, or via notification within the Products and/or mobile applications. Continued use of the Products or Software after such notice constitutes acceptance of the amended Agreement. This right to amend does not extend to the Standard Contractual Clauses in Appendix 1, which may be updated only as permitted under those Clauses.

10. GOVERNING LAW AND DISPUTE RESOLUTION

10.1 This Agreement, including all schedules, annexes, and other integral parts hereof, shall be governed by and construed in accordance with the laws of the Republic of Poland.

10.2 The Parties also agree to comply with the Applicable data protection law relating to the processing of Personal Data.

10.3 “Applicable data protection law” means the legislation on the processing of personal data in force from time to time, including the General Data Protection Regulation (EU) 2016/679; the UK Data Protection Act 2018; the Privacy and Electronic Communications Directive 2002/58/EC (as updated by Directive 2009/136/EC); the Privacy and Electronic Communications Regulations 2003 (SI 2003/2426), as amended; and any other EEA legislation relating to personal data and all other legislation and regulatory requirements in force from time to time that apply to the Parties in relation to the use of Personal Data (including, without limitation, the privacy of electronic communications), depending on the territory in which the Products and Software are provided.

10.4 Any dispute, controversy, or claim arising out hereof or relating in any way hereto, as well as to the interpretation, enforceability, performance, breach, termination, or validity hereof shall be settled in the courts of Poland (Warsaw), unless otherwise provided by the Applicable data protection law. The

language of the proceedings shall be English.

10.5 The Parties irrevocably agree that the courts of the Republic of Poland shall have exclusive jurisdiction to settle any disputes which may arise out of or in connection with the Agreement, including, but not limited to, disputes regarding its performance, existence, validity, interpretation, termination, or consequences thereof. Accordingly, any legal action or proceeding arising out of or in connection with the Agreement, whether based on contractual or extracontractual liability, shall be brought exclusively before the courts of the Republic of Poland. Where the Controller is a natural person acting as an Individual End User (as defined in the End User Agreement), the Controller may also bring proceedings before the courts of its country of habitual residence.

Appendix 1. STANDARD CONTRACTUAL CLAUSES (hereinafter also "**SCC**")

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) 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 1 (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 SCC, as listed in Annex 1 (hereinafter each "data importer") have agreed to these standard contractual clauses.

(c) These SCC apply with respect to the transfer of personal data as specified in Annex 1.

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

Clause 2

Effect and invariability of the SCC

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

(b) These SCC 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 SCC, 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 the rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

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

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

(c) These SCC 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 SCC and the provisions of related agreements between the Parties, existing at the time these SCC are agreed or entered into thereafter, these SCC 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 1.

Clause 7

Docking clause

In Clause 7, the optional docking clause does not apply.

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 organizational measures, to satisfy its obligations under these SCC.

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 1, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these SCC, 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 2 and personal data, the data exporter may redact part of the text of the Appendix to these SCC prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand 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 1. 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 SCC. 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 SCC 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 organizational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorized 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 organizational measures specified in Annex 2. 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 authorized 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 SCC, 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 offenses (hereinafter "sensitive data"), the data importer shall

apply the specific restrictions and/or additional safeguards described in Annex 1.

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 (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 SCC, under the appropriate Module, or if:

(i) the onward transfer is to a country benefiting 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 of Regulation (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise, or defense 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 SCC, 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 SCC.

(b) The Parties shall be able to demonstrate compliance with these SCC. 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 SCC and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these SCC at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may consider 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 five (5) business 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 SCC, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfills its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these SCC.

(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 fulfill its obligations under that contract.

(e) The data importer shall agree on 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 authorized 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 2 the appropriate technical and organizational 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 authorized 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 SCC, 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, organization, 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 SCC.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these SCC.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these SCC. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these SCC, 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.

(f) The Parties agree that if one Party is held liable under paragraph (e), 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.

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

Clause 13

Supervision

(a) 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 1, shall act as the 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 SCC. In particular, the data importer agrees to respond to inquiries, 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 SCC

(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 authorizing access by public authorities, prevent the data importer from fulfilling its obligations under these SCC. 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 SCC.

(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 authorizing access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards[1];

(iii) any relevant contractual, technical, or organizational safeguards put in place to supplement the safeguards under these SCC, 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 SCC.

---

[1] As regards the impact of such laws and practices on compliance with these SCC, 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 SCC, 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.

(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 SCC 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).

(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 fulfill its obligations under these SCC, the data exporter shall promptly identify appropriate measures (e.g., technical or organizational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. 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 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 SCC. 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.

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 SCC; 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 SCC 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 at the 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 SCC.

15.2 Review of legality and data minimization

(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.

(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 SCC and termination

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

(b) In the event that the data importer is in breach of these SCC or unable to comply with these SCC, 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 SCC, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these SCC 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 SCC; or

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

In these cases, it shall inform the competent supervisory authority 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) 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. 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 SCC. 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 SCC 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 SCC 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 SCC 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 SCC shall be governed by the law of one of the EU Member States, provided such law allows 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 SCC 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 1. DATA PROCESSING DESCRIPTION

A. LIST OF PARTIES

Data exporter

Role: Controller

Identity and contact details: The Controller, as identified by the account information (name or company name, address, and contact email) registered by the Controller in the Ajax Products and Software at the time of account creation.

Activities relevant to the data transferred: Use of the Ajax Products and Software to secure premises or property under the Controller's control.

Data importer

Role: Processor

Name: AJAX SYSTEMS TRADING FZE

Address: S3B2SR06, Jebel Ali Freezone, Dubai, United Arab Emirates

Contact details: privacy@ajax.systems

Activities relevant to the data transferred: Provision of Services enabling the Controller's use of the Ajax Products and Software in accordance with the End User Agreement.

B. CATEGORIES OF DATA SUBJECTS

The Personal Data transferred under these SCC concern the following categories of data subjects:

- the Controller (account holder) and any persons the Controller grants account access to;

- household members, employees, visitors, or other natural persons present at premises or property secured by the Controller's Ajax Products and Software, whose Personal Data (including images and video recordings) may be captured depending on the configuration set by the Controller.

C. FREQUENCY OF THE TRANSFER

Continuous for the duration of the Controller's use of the Ajax Products and Software.

D. SUBJECT MATTER, NATURE, AND PURPOSE OF THE PROCESSING

The subject matter, nature, and purposes of the processing are set out in Section 2 of the Agreement.

E. CATEGORIES OF PERSONAL DATA

For the provision of the Services specified in this Agreement, the Processor may process:

- Unique identifiers (username);
- Information about the use of Ajax Products and Software (such as requests from the app);
- IP address;
- Name, surname, and contact information as specified during the initial registration;
- The content of SMS messages with access codes sent to end users during registration or account changes;
- Information about end users' mobile devices, including their type, operating system, and interface language;
- Images, audio, and video recordings captured by Ajax Products and Software;
- Other data and information being processed where necessary.

Special Categories of Personal Data

Not intentionally collected. Images and video recordings captured by the Controller's devices may incidentally include biometric data (e.g., images of faces). The Processor applies the additional safeguards described in Annex 2 to any such data. Special category data may only be processed where such processing is compatible with applicable Data Protection Regulations and where initiated by the data subject or the Controller.

F. DURATION OF PROCESSING / RETENTION

For the duration of the Controller's use of the Ajax Products and Software. Upon termination, deletion is completed within the period set out in Section 8 of the Agreement.

G. COMPETENT SUPERVISORY AUTHORITY

Where the EU GDPR applies, the competent supervisory authority is that of the EU Member State in which the Controller (or, if the Controller does not have an establishment in the EU, its representative) is established. Where the Controller has neither an establishment nor a representative in the EU, the competent supervisory authority is the Irish Data Protection Commission.

Where the UK GDPR applies, the competent supervisory authority is the UK Information Commissioner's Office.

ANNEX 2. TECHNICAL AND ORGANIZATIONAL MEASURES

This Annex sets out **Technical and Organizational Measures** (hereinafter also "TOM") and supplements Section 3 of the Data Processing Agreement between the Processor and the Controller pursuant to Article 28 of the GDPR (EU General Data Protection Regulation No. 2016/679).

Information Security

Data Encryption: Use of AES-256 for data at rest and TLS 1.2+ for data in transit.
Pseudonymization: Use of SHA-256 hashing for applicable data sets.
Firewalls: Implementation of Web Application Firewalls (WAF) and network-level firewalls.
Authorization Control: Strict logic for accessing information based on roles.
Resilience: Protection against unauthorized processing, loss, or destruction.
Backup and Restoration: Key systems are backed up as complete system images to enable rapid recovery. Backups are encrypted both at rest and in transit, including remote and cloud-based backups. Backup and restoration procedures are tested regularly to confirm that recovery is fully functional.
In the event of restoration from a backup, previously deleted Personal Data is removed from the restored data without undue delay, and in any event within 24 hours of the restoration.
DDoS Protection: Use of specialized traffic filtering services and automated mitigation tools provided by the infrastructure vendor to protect against infrastructure (Layer 3/4) and application-layer (Layer 7) attacks.
Patch Management: Automated monitoring and deployment of security patches for all cloud resources and operating systems.

1. Confidentiality

1.1. Physical Access Control

Measures suitable for preventing unauthorized persons from gaining access to data processing systems with which Personal Data are processed or used.

1.2. Technical Measures

Alarm System: Use of Ajax's own advanced security systems (hubs, motion detectors, and sirens) with 24/7 monitoring and instant alerting.
Electronic Access Control: Secure RFID key card/fob system for office entry; access logs are maintained and reviewed regularly.
Video Surveillance: High-definition IP cameras monitoring entry/exit points and internal critical zones.
Cloud Infrastructure Security: Physical access to servers is managed by AWS in accordance with its compliance certifications (SOC 2, ISO 27001).

1.3. Organizational Measures

Information Security Policy: Comprehensive internal rules governing physical security and asset protection.
Work Instructions for Operational Safety: Documented procedures for securing the office environment and handling hardware.
Work Instruction Access Control: Strict protocols for issuing, revoking, and auditing physical access rights for employees and contractors.
Visitor Management Policy: Requirements for logging, identifying, and escorting all visitors within the office premises.

2. Logical Access Control

Measures to prevent unauthorized use of data processing systems.

Multi-Factor Authentication (MFA): Mandatory for all administrative access, cloud console management, and remote logins.
Identity and Access Management (IAM): Centralized management of user permissions with regular access reviews.
VPN Access: Requirement for encrypted VPN tunnels for any remote connection to the production environment or internal management tools.

3. Data Access Control

Measures to ensure that persons entitled to use a data processing system can access only the data within their competence.

Role-Based Access Control (RBAC): Permissions are granted strictly according to specific job functions and on a "need-to-know" basis.
Audit Logging: Comprehensive logging of all access activities, changes, and deletions within systems containing Personal Data.

4. Integrity, Availability, and Resilience

Transfer Control: Measures to ensure that Personal Data cannot be read, copied, modified, or removed without authorisation during electronic transmission.
Input Control: Measures to ensure that it is possible to check and establish whether and by whom Personal Data have been entered into, modified, or removed from data processing systems.
Availability Control: Measures to ensure that Personal Data are protected against accidental destruction or loss (e.g., uninterruptible power supply (UPS) in data centers, redundant storage).
Business Continuity and Disaster Recovery: Documented business continuity and disaster recovery plans are maintained, tested, and verified at least annually.

5. Procedures for Regular Testing and Evaluation

Incident Management: Documented process for detecting, reporting, and responding to security incidents and potential data breaches.
Vulnerability Management: Regular automated vulnerability scanning and periodic professional penetration testing of the infrastructure and applications.
Employee Awareness: Regular training sessions for staff regarding data protection, GDPR compliance, and phishing threats.
Personnel Security: Background checks are performed in line with good hiring practices, and all personnel and contractors sign confidentiality agreements before accessing Personal Data.

ANNEX 3. THE LIST OF APPROVED SUB-PROCESSORS

The current and up-to-date list of sub-processors engaged by the Processor is maintained and published at: https://ajax.systems/gdpr-white-paper/

The Processor shall update this list prior to engaging any new sub-processor according to the procedure set out in Section 7 of this Agreement.