PERSONAL DATA PROCESSING POLICY (TRANSPARENCY POLICY)

DEFINITIONS

Data Controller: Agora S.A. with its registered office in Warsaw (00-732), ul. Czerska 8/10, entered in the register of entrepreneurs of the National Court Register maintained by the District Court for the capital city of Warsaw in Warsaw, 13th Commercial Division of the National Court Register, under KRS No 59944, NIP [tax identification number]: 526030-56-44.

Personal Data: any information about a natural person who is identified or identifiable through one or more specific facts that determine physical, physiological, genetic, psychological, economic, cultural or social identity of the natural person, including image, voice recording, contact data, location data, information contained in correspondence, information collected by means of recording equipment or any other similar technology.

Policy: this transparency Policy on Personal Data processing.

GDPR: Regulation (EU) 2016/679 of the European Parliament and of the Council of 7 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.

Data Subject: every natural person whose Personal Data are processed by the Data Controller, e.g. a person who visits the Data Controller's premises or sends the Data Controller an inquiry by e-mail.

DATA PROCESSING BY THE DATA CONTROLLER

In connection with its economic activity, the Data Controller collects and processes Personal Data in line with relevant regulations, in particular with GDPR and the data processing rules set out therein.

The Data Controller ensures the transparency of data-processing, in particular by always notifying, when collecting the data, that the data would be processed; this includes notification of the purpose and legal basis for the processing - e.g. when signing a contract of sale of goods or services. The Data Controller always pays attention to collecting data only in such scope as is necessary for the specified purpose, and to processing the data only for such time as is necessary.

When processing the data, the Data Controller ensures the data security and confidentiality and makes sure that Data Subjects have access to information about such processing. Should a Personal Data breach (e.g. a "leak" or loss of data) occur despite the security measures applied, the Data Controller shall notify this to the Data Subject in a manner compliant with regulations.

CONTACTING THE DATA CONTROLLER

The Data Controller can be contacted via e-mail at iod@agora.pl, or in writing to: Agora S.A., ul. Czerska 8/10, 00-732 Warsaw.

The Data Controller has appointed a Data Protection Officer who can be contacted via e-mail at iod@agora.pl in any matter pertaining to the processing of Personal Data.

SECURITY OF PERSONAL DATA

To ensure integrity and confidentiality of the data, the Data Controller implemented procedures, which allow access to Personal Data only to authorised persons and only within such scope as is

necessary because of their tasks. The Data Controller applies organisational and technical solutions to ensure that all operations on Personal Data are registered and performed only by authorised persons.

Furthermore, the Data Controller takes all necessary actions to cause its subcontractors and other associates to guarantee the application of appropriate security measures every time when they process Personal Data at the Data Controller's request.

The Data Controller performs risk analysis on a regular basis and monitors the adequacy of applied data safeguards to identified threats. If necessary, the Data Controller implements additional measures to increase data security.

PURPOSE AND LEGAL BASIS FOR DATA PROCESSING BY THE DATA CONTROLLER

E-mail and conventional correspondence

When an e-mail or conventional mail, unrelated to any services provided to the sender or another contract with the sender, is sent to the Data Controller, the Personal Data contained in such correspondence is processed only to communicate and deal with the matter, to which that correspondence pertains.

The legal basis for processing consists in the Data Controller's legitimate interest (Article 6(1)(f) GDPR), which involves exchanging correspondence addressed to the Data Controller in connection with the economic activity.

The Data Controller processes only such Personal Data as are relevant to the matter, to which the correspondence pertains. The entire correspondence is kept in a manner that ensures security of the Personal Data contained therein and other information, and is disclosed to authorised persons only.

Contact by phone

When the Data Controller is contacted by phone, in matters unrelated to a signed contract or provided services, Personal Data can be demanded only when this is necessary to deal with the matter, to which the contact pertains. The legal basis in this case is the Data Controller's legitimate interest (Article 6(1)(f) GDPR), which consists in the need to deal with the reported matter, connected to the economic activity.

Telephone calls can be also recorded — in such a case, the information about this is provided at the beginning of each call. Calls are recorded to verify the quality of provided service and verify the consultants' work, but also for statistical purposes. The recordings are available only to the Data Controller's staff and to the persons who handle the Data Controller's hotline.

Personal Data the in form of call recording is processed:

- for the purposes related to the client and customer service through hotline when the Data Controller provides such service — the legal basis for the processing is the necessity to process in order to provide the service (Article 6(1)(b) GDPR);
- to monitor the service quality and verify the work of consultants who operate the hotline — the legal basis for the processing is the Data Controller's legitimate interest (Article 6(1)(f) GDPR), which involves paying attention to the highest quality of service to clients and customers.

Visual monitoring and access control

To ensure the safety of people and property, the Data Controller uses visual monitoring and controls access to the premises and area managed by the Data Controller. The data collected in this way are not used for any other purposes.

Personal Data in the form of monitoring recordings and data collected in the register of entries and exists are processed to ensure security and order in the facility area and, possibly, to defend against or seek claims. The legal basis for processing consists in the Data Controller's legitimate interest (Article 6(1)(f) GDPR), which involves ensuring safety of the Data Controller's property and protecting the Data Controller's rights.

Recruitment

As a part of recruitment processes, the Data Controller expects to be provided with Personal Data (e.g. in CV) only to the extent set out in employment law. Therefore, information in any broader scope should not be provided. When the received applications contain this kind of additional data, such data will not be used or taken into consideration in the recruitment process.

Personal Data are processed:

- to perform the legal obligations related to the employment process, first of all the Labour Code — the legal basis for processing is the Data Controller's legal obligation (Article 6(1)(c) GDPR in conjunction with the Labour Code);
- to carry out the recruitment process with respect to the data, which are not required by law, and for the purpose of future recruitment processes — the legal basis for the processing is the consent (Article 6(1)(a) GPDR);
- to determine or seek possible claims or defend against such claims — the legal basis for the processing is the Data Controller's legitimate interest (Article 6(1)(f) GDPR).

Collecting data in connection with the provision of services or performance of other contracts

If Personal Data are collected for the purposes connected with performance of a specific contract, upon the execution of such contract the Data Controller provides the Data Subject with detailed information concerning the processing of that Subject's Personal Data.

Collecting data in other situations

In connection with its business, the Data Controller collects Personal Data also in other situations — e.g. during business meetings, at industry events or by business card exchange — for purposes related to the establishment and maintenance of business contacts. The legal basis for processing in this case consists in the Data Controller's legitimate interest (Article 6(1)(f) GDPR), which involves creation of a network of contacts in connection with the conducted business.

The Personal Data collected in such situations are processed solely for the purpose, for which they were collected, and the Data Controller provides appropriate protection for such Data.

DATA RECIPIENTS

In connection with the pursued business, which requires the processing of Personal Data, such Data are disclosed to third parties, in particular to suppliers in charge of IT system service and equipment (e.g. CCTV equipment), legal or accounting service providers, courier services , marketing or recruitment agencies. The Data are also disclosed to the Data Controller's related parties, including the other entities of company . More information about the Data Controller's group of companies can be found at https://www.agora.pl/en/about-agora.

The Data Controller reserves the right to disclose selected information concerning the Data Subject to the competent authorities or to third parties, who submit the demand to be provided with such information, on the basis of appropriate legal basis and in line with applicable laws.

TRANSMITTING THE DATA OUTSIDE THE EUROPEAN ECONOMIC AREA

The level of Personal Data protection outside the European Economic Area (EEA) differs from the level provided by European laws. For this reason, the Data Controller transfers the Personal Data

outside the EEA only when this is necessary, with appropriate protection level provided, primarily through:

- co-operation with Personal Data processors in those countries, for which the relevant decision of the European Commission was issued;
- application of standard contractual clauses issued by the European Commission;
- application of binding corporate rules, approved by the competent supervisory authority;

The Data Controller always notifies the intention to transmit Personal Data outside the EEA, at the stage of data collection.

TIME LIMIT FOR THE PROCESSING OF PERSONAL DATA

The time limit for the processing of data by the Data Controller depends on the type of service provided and the purpose of processing. The time limit for data processing may also result from legal regulations, when such regulations form the basis for the processing. If the data are processed on the basis of the Data Controller's legitimate interest — e.g. for security reasons — the data are processed for a period required to accomplish that interest or until an effective objection is filed with respect to the data processing. If the processing is based on a consent, the data are processed until the consent is withdrawn. When the processing is based on the data being needed to execute and perform a contract, such data will be processed until the termination thereof.

The time limit for data processing can be extended, if the processing is necessary to determine, seek or defend against possible claims, and after that time limit — only if and to the extent that this would be required by law. After the end of the time limit for processing, data must be irrevocably removed or anonymised.

RIGHTS RELATED TO PERSONAL DATA PROCESSING

Data Subjects' rights

Data Subjects have the following rights:

- **Right to information about personal data processing** — on this basis, any person who makes such a demand is provided by the Data Controller with information about: data processing, including purposes and legal basis for the processing; the scope of possessed data; the entities to whom the data are disclosed; and the planned date of data removal;
- **Right to receive a copy of the data** — on this basis, the Data Controller provides a copy of the processed data concerning the data subject who made the demand;
- **Right to correction** — the Data Controller must remove any possible inconsistencies or errors in the personal data processed, and supplement the data if incomplete;
- **Right to erasure** — on this basis, a demand to erase data can be made, when the processing of such data is not required any longer for any of the purposes, for which the data were collected;
- **Right to restriction of processing** — if such a demand is made, the Data Controller ceases any operations on the personal data, except for operations consented to by the data subject, and stops storing such data in line with the adopted retention rules or until the reasons for restriction on data processing expire (e.g. a decision of supervisory authority is issued, permitting further processing of the data);
- **Right to data portability** — on this basis, within such scope as the data are processed in connection with a signed contract or a received consent, the Data Controller shall release the

data provided by the data subject, in a machine-readable format. It is also possible to demand that such data be sent to another entity — provided, however, that both the Data Controller and that other entity have technical capability in this respect;

- **Right to object against processing of data for marketing purposes** — the data subject can at any time object to the processing of personal data for marketing purposes, with no need to provide any rationale for such an objection;
- **Right to object against processing of data for other purposes** — the data subject can any time object to the processing of personal data on the basis of the Data Controller's legitimate interest (e.g. for analytical or statistical purposes or for reasons related to property protection). An objection in this respect should contain a rationale;
- **Right to withdraw consent** — if data are processed on the basis of the received consent, the data subject can withdraw such consent any time; however, this will not affect the lawfulness of any processing done before the consent was withdraw.
- **Right to complain** — if the data subject decides that the processing of personal data violated the GDPR or other regulations concerning personal data protection, he/she can file a complaint to the President of the Personal Data Protection Office *(Prezes Urzędu Ochrony Danych Osobowych)*.

Submitting demands related to the exercise of rights

An application concerning the exercise of data subjects' rights can be submitted:

- in writing to the address: Agora S.A., ul. Czerska 8/10, 00-732 Warsaw;
- by e-mail to the address: iod@agora.pl.

The application should specify as precisely as possible what the demand is about i.e. in particular:

- what right the applicant wishes to exercise (e.g. right to receive a copy of the data, right to erasure, etc.);
- what processing process the demand pertains to (e.g. use of a specific service, activity on a specific Internet site, newsletter with commercial information sent to a specific e-mail address, etc.);
- what processing purposes the demand pertains to (e.g. marketing purposes, analytical purposes, etc.).

If the Data Controller is unable to determine the content of the demand or identify the applicant on the basis of the received application, the Data Controller will request additional information from the applicant.

The application can be submitted in person or through an attorney-in-fact (e.g. family member). For data security reasons, the Data Controller recommends that the power of attorney be given in a form certified by a notary or authorised legal counsellor or advocate (attorney-at-law), as this will help verify the instrument's authenticity much faster.

A reply to the application should be given within one month of receipt of the same. If this time limit needs to be extended, the Data Controller will notify the reasons for such extension to the applicant.

The reply is given in writing, unless the application was submitted by e-mail or it contained a demand to give the reply in an electronic form.

Principles of charging

The procedure concerning the submitted applications is free of charge. Charges can be collected **only** when:

- a demand to release a second and every next copy of the data is made (the first copy of the data is free of charge); in such a case, the Data Controller may request a fee of PLN 30 to be paid.

  This fee covers the administration costs related to the fulfilment of the demand.

- the same person makes excessive demands (e.g. unusually frequent) or obviously unfounded demands; in such a case, the Data Controller may request a fee of PLN 30 to be paid.

  This fee includes the costs of communications and costs related to the demanded actions.

If the data subject wishes to challenge the decision to charge a fee, he/she can file a complaint to the President of the Personal Data Protection Office (Prezes Urzędu Ochrony Danych Osobowych).

CHANGES TO THE PERSONAL DATA PROCESSING POLICY

This Policy is reviewed on a regular basis and updated as needed.