Introduction

AA AceNetworks Ltd (hereinafter referred to as "the Company", “we” "us", "our") takes the protection of your personal data and your privacy very seriously when collecting and processing your personal data. We ensure you that we fully respect the EU 679/2016 Regulation “on the protection of natural persons with regard to the processing of personal data and on the free movement of such data” as well as the National Law 125/I/2018 accordingly.

Definitions

Personal Data means any information relating to an identified or identifiable natural person (‘**data subject**’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such (indicatively) as a name, an identification number, age, address, occupation, contact details, education, work, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Processing means any operation or set of operations which is performed on personal data or on sets of personal data, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Personal data **breach** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

Controller means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

Processor means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

Third party means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

The Controller

Regarding the personal data in the cases where we determine the purposes and means of the processing, the Controller is the legal person **AA AceNetworks Ltd**, address 3 Omirou Av., Eleutherias Square, Nicosia, Cyprus, tel: +357 22516181, e-mail: info@acenetworks.eu.

Principles we comply

The personal data are:

- processed lawfully, fairly and in a transparent manner in relation to the data subject (principle of 'lawfulness, fairness and transparency');
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (principle of 'purpose limitation');
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (principle of 'data minimisation');
- accurate and, where necessary, kept up to date; we take every reasonable step to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (principle of 'accuracy');
- kept in a form which permits identification of data subjects for no longer than it is necessary or as required by relevant Laws (principle of 'storage limitation');
- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical and organisational measures (principle of 'integrity and confidentiality').

Finally, we are able to demonstrate compliance with the aforementioned principles (principle of 'accountability').

When we collect personal data

We, as the Controller, collect Personal Data from you in the following cases:

- When you contact us directly or through our collaborators, or when connecting to our website or social media accounts, or when emailing to us in order to be informed or to request information about our products and the services we offer, or when you visit our premises.
- If you purchase products and services from us or when you are involved in events related to the sale of our products and services.
- When participating in projects we bid for, either on our own or as consortium leaders.
- When you fill in any of our communication or other forms in paper or electronic format.
- When you cooperate with us, or if personal data of yours are legally disclosed to us by third parties or partners under contracts or agreements.
- During an evaluation process aiming to improve our services.
- When you contact us in any way as an employment candidate and sending your CV.

- When you are employed by us.

In addition, we process personal data, which third parties, usually legal entities, disclose to us in the case we are a Processor on their behalf.

We process your personal data for the purposes set out in detail below.

Minors' Personal Data

We do not collect minors' personal information without verifiable parental consent in cases where we are able to check it. For example, it is not possible to check information that is disclosed to us without physical presence (e.g., online). In any case, if we become aware having collected any minor's personal information without verifiable parental consent, we will directly erase such information (according Article 8 of the Regulation). If you believe that we may have collected minor's personal data, please contact us.

Personal data we collect and process

Data from the following categories of personal information about you, may be collected and processed by us as the Controller, **per case** in order to **serve** the **purpose** of the data collection and in accordance with the **relevant legal basis** as described in this Privacy Notice:

- Contact information such as full name, address, telephone /fax number and email address of yours or another individual you may indicate.
- Occupational status information (occupation, position, company).
- Information required for signing a contract such as your contact details or of people involved in signing the contract, the terms of agreement, amounts, bidding offer in co-financed projects that may include your CV, position in the project, time, amount, etc. in accordance with the application requirements.
- Payment details (IBAN or account number, tax identification number, desired payment method, payment terms, depositor's details).
- Customer's history (satisfaction rate, quotes received, market data, transaction data, complaints, product problems, terms of cooperation) and evaluation ratings.
- Apps / websites / social media data, like IP address, cookies, name under which you appear in the media, photo, any information that is public and comments or information included in any email attachments.

- Any information referred in your CV or any additional documents you send us, when you are interested in working with us.

It is noted that our employees are internally informed through policies and procedures and internal documents on the collection and processing of their personal data.

Purpose of the process and legal basis

The processing of personal data from us as the Controller, is based on one of the "legal bases" as referred to in Article 6 of the Regulation (or Article 9 in case of special categories of personal data). The legal bases on which the collection and processing of personal data is based (in most of the cases) are:

- your consent (Article 6.1.a) or explicit consent (Article 9.2.a);
- processing that is necessary for the performance of a contract to which you as the data subject is party, or in order to take steps at your request as the data subject prior to entering into a contract (Article 6.1.b);
- the compliance with our legal and statutory obligations (Article 6.1.c);
- the safeguarding of our legitimate interests, except where such interests are overridden by the interests or fundamental rights and freedoms of yours as the data subject (Article 6.1.f).

We do not collect and process other special categories of personal data (Article 9), with the exception of our employees; in this case they are internally informed.

The legal basis, on which the processing of your personal data is based, is as follows for each processing purpose:

Consent: when you contact us physically or electronically either as interested in our products and services or as a potential corporate partner, when contacting us as candidates for employment, or when informing you during our promotion activities, when you make a complaint or when you evaluate us, or when you visit our website and social media accounts, or when you are connecting to our Wi-Fi, or when you give us your personal/ professional card.

Explicit Consent: when you agree to upload your photograph in our website or social media accounts.

Performance of a contract: when you are our customer for serving you and the fulfillment of our agreement, when you are one of our suppliers or collaborators for the compliance with the contractual terms of our agreement, when we cooperate with you in the framework of a project, or when we communicate with you prior or under the contract as well as for the payment of our liabilities.

Legal Obligations: for the compliance with our legal obligations towards authorities such as prosecuting authorities, police, labor law and regulatory authorities, tax and auditing authorities or judicial authorities.

Legitimate interests: to improve our services, or when investigating and managing any potential incident, to receive our payment, or for the assessment of persons and situations. In this specific legal basis is also based the video surveillance system (CCTV) in our premises that we legally operate for the protection of people and the property.

Our employees are internally informed through documents and procedures on the purpose and legal bases when collecting and processing their personal data.

Storage of personal data time limits

We store personal data we process as the Controller for as long as required by the respective processing purpose and any other lawful linked purpose.

Personal data that are collected under the legal basis of 'Performance of a contract' or the legal basis of 'Legal Obligations' (Article 6.1.b and 6.1.c), are maintained after the expiry of the contractual and legal obligations as long as the relevant institutional framework permits.

Data that may be needed for our legitimate interests as a Controller (Article 6.1.f) shall be kept until the reason for storing such data ceases. The recording of the video surveillance system is kept no longer than 15 days and then it is permanently deleted through overwrite.

Personal data included in an offer that does not lead to a cooperation agreement are kept for 12 months.

Employment candidates' personal data are kept for 12 months unless you prior withdraw your consent.

Specifically for personal data we process based on your consent, such data are kept from obtaining your consent and until it is revoked or the retention is no longer necessary.

Personal data that are no longer necessary are securely destroyed or anonymised. We restrict access to your personal data to those employees under a need-to-know basis.

Security of your personal data

We have implemented reasonable and appropriate organisational and technical measures to protect the personal data and the entire information we process, and in particular any specific categories of

personal data. We follow international standards and practices (as an example we follow the provisions of the ISO 27001:2013 International Standard) to ensure the security of the information we process. We ensure that your personal data is processed securely and legally, by adhering to policies and developing and implementing procedures.

For example, the following security measures have been implemented to protect personal data against unauthorised use or any other form of unauthorised processing:

- Access to personal data is restricted to a limited number of authorised employees under a need-to-know basis, and the necessary data transfer is done by secure procedures.
- Our employees are bound to confidentiality rules and agreements, with limited classified access to the necessary data only.
- We ensure that our employees are provided with the appropriate training in order to handle personal data promptly and in accordance with the legal framework.
- We select trusted collaborators who are committed in writing, in accordance with Article 28 of the Regulation, to the same obligations regarding the protection of personal data. We reserve the right to audit them in accordance with Article 28 (3) (h).
- In our ICT systems used for the processing of personal data, all technical measures are taken to prevent loss, unauthorised access or other illegal processing.

In addition, access to these ICT systems is monitored on a permanent basis in order to detect and prevent illegal use at an early stage. Although the transfer of data through the Internet or a web site cannot be guaranteed to be protected from cyberattacks, we work to maintain physical, electronic and procedural security measures to protect your data.
It is obvious that part of the security measures is not subject to public disclosure.

To whom the Data may be disclosed

We take measures to ensure that the recipients of personal data are kept to a minimum. The personal data we collect is disclosed to third parties, provided that the legality of such disclosure is fully justified. Specific personal data from those we lawfully process as the Controller, may be accessed (or disclosed) on a case-by-case basis by:

- Any supervisory or persecutory authority within its role.
- Any public or judicial authority where required by law or judicial decision.
- Company's auditor and legal advisor and only for the required amount of personal data to fulfil their role under a duty of confidentiality.
- Consortium partners in the bidding and implementation process, provided we act as the Controller or joint Controller, only for the data related to the specific project and for which they need to be aware.

- The Insurance cooperating company and only for the relevant part of the information.
- Partner banks (of the company, the staff or affiliates and suppliers), only for payment related data.
- The training or systems consultants, the trainer and HRDA (training Authority) for training or systems control issues and only for the necessary pieces of information and data.

Territorial Scope

The personal data we collect is processed within the European Economic Area (EEA) and/or an adequacy decision area according Article 45.

Your rights as a data subject and exercising such rights

You have the right to be informed, the right of consent when this is the legal basis of data collection and processing, the right of access to your personal data, the rights of rectification and erasure (in cases it is permitted), the right to restriction of processing, the right to data portability, the right to object. If processing is based on your consent, you may withdraw it at any time.

The right to be informed is exercised through this privacy and personal data protection notification. In some cases, it is also mentioned on documents – forms we are using.

We inform you that we are not using software of decision making solely based on automated processing including profiling.

The right of **consent** is provided by design as we have reviewed all processing activities and ask your consent when the case.

Right of access: you have the right to obtain from us confirmation as to whether or not your personal data are being processed as well as other relevant information, and, where that is the case, access to your personal data.

Right of rectification: you have the right of rectification of your inaccurate personal data as well as to have incomplete personal data completed by providing a supplementary statement.

Note: Since it is not possible for us to be aware of any changes to your personal data if you do not inform us, please help us keep your information accurate by informing us of any changes to your personal information we do process.

Right to erasure ('right to be forgotten'): we have to answer such right when:

- your personal data are no longer necessary in relation to the purposes for which we collected it
- withdraw your consent on which the processing is based and where there is no other legal basis for the processing
- your personal data have been unlawfully processed
- personal data have to be erased for compliance with a legal obligation we are subject to
- personal data have been collected in relation to the offer of information society services.

We reserve the right to refuse this right if the processing is necessary for compliance with any legal obligation, we are subject to, or for reasons of public interest, or for the foundation and exercise or support of our legal claims (according Article 17 § 3).

Right to restriction of processing: you have the right to restriction of processing when:

- you contest the accuracy of your personal data for a period enabling us to verify the accuracy of the personal data
- the processing is unlawful and you oppose the erasure of the personal data and request the restriction of their use instead
- we no longer need your personal data for the purposes of the processing, but they are required by you for the establishment, exercise or defence of legal claims
- you objected to processing pending the verification whether our legitimate grounds override those of yours.

Right to data portability: You have the right to receive your data in a structured, commonly used and machine-readable format and under an explicit request such data to be transferred to both you and another natural or legal person who will process it when:

- the processing is based on consent or the data were processed for the performance of a contract to which you were a party; and
- the processing is carried out by automated means.

Right to object: you have the right to object to the processing of your data at any time when the reason for the processing relates to direct marketing.

In the event that you make such request in a written or electronic form regarding any of the above rights, will assess your request and respond within one month of its receipt, either for its satisfaction or to provide you with objective reasons preventing it from being satisfied, or, given the complexity of the request and the number of requests at the given time, request an extension of response for a further two months period (Article 12.3).

The exercise of your rights is free of charge. Where requests from you are manifestly unfounded or excessive, in particular because of their repetitive character, we may refuse to answer or charge you an administrative fee.

Please note that we are not allowed to respond requests when we are the Processor. In this case you should contact the Controller.

If you are dissatisfied with the use of your data by us, or our response after exercising your rights, you have the right to lodge a complaint with a supervisory authority. Before such complaint, you may contact us if you wise so we can provide you with complete information and support.

Data Breach

In the event of a breach of the security and integrity of the personal data processed, we will take the following measures (in accordance with Article 33 and 34 of the Regulation) and we will:

- assess it in order to implement the appropriate procedures needed to limit the breach
- examine the extent of the breach and the sensitivity of the data included
- evaluate the risk and its impact on your rights and freedoms
- endeavour to reduce as much as possible the damage that is or may be caused
- notify within a time limit of 72 hours of becoming aware of the breach, the National Personal Data Protection Authority, if required
- assess the impact on your privacy and take appropriate measures to prevent the repeating of the incident

In the event we are the processor, we will inform the Controller as soon as possible.

Links with other sites

Our website may be linked to other websites that are not operated or controlled by us. If you click on a third-party link, you will be directed to that third-party site. We recommend you to review the Privacy Policy in each site you visit. We have no control over and assume no responsibility for the content, privacy policies, or practices of any third-party sites or services.

Communication with the National Authority on the protection of Personal Data

If you wish to contact with the Supervisory Authority, the contact details are: Jason 1 str., 1082 Nicosia, CYPRUS, telephone +357.22818456, e-mail: commissioner@dataprotection.gov.cy.

Additional information and the Regulation in European languages can be found on the website https://eur-lex.europa.eu/eli/reg/2016/679/oj.

Contacting with us

For any questions or other issue regarding the processing of your personal data and the exercise of your rights mentioned above, you may contact us in the address 3 Omirou Av., Eleutherias Square, Nicosia, Cyprus, tel: +357 22516181, email: info@acenetworks.eu.

Update of the present Policy

This policy was updated at July 1, 2021 and will be reviewed when there is a significant change. This review will be available on the same website. Printed form of this policy is available at our offices or it may be sent to you upon request.