AIGO BS, LTD

PERSONAL DATA PROTECTION POLICY

Belgrade, 2018

Change history

Version:	01
Date of version:	December 19, 2018
Created by:	Gojko Grubor
Verified by:	Vesna Vukobrat
Approved by:	Dragan Popovic
Confidentiality level:	Internal
Policy owner:	Data protection officer (DPO) or named person in charge of data protection matters
Policy stored:	On the Aigo BS web server in electronic form and in the main archive in printed form

Table of contents

1. PURPOSE, SCOPE AND USERS 4
2. REFERENCE DOCUMENTS 4
3. TERMS DEFINITIONS 4
4. BASIC PRINCIPLES REGARDING PERSONAL DATA PROCESSING 6
4.1. Lawfulness, Fairness and Transparency 6
4.2. Purpose Limitation 6
4.3. Data Minimization 6
4.4. Accuracy 7
4.5. Storage Period Limitation 7
4.6. Integrity, confidentiality and availability 7
4.7. Accountability 7
5. BUILDING DATA PROTECTION IN BUSINESS ACTIVITIES OF THE COMPANY 7
5.1. Notification to Data Subjects 7
5.2. Data Subject's Choice and Consent 7
5.3. Data Collection 8
5.4. Use, Retention, and Disposalof data 8
5.5. Data disclosure to Third Parties 8
5.6. Cross-border Transfer of Personal Data 9
5.7. Rights of Access by Data Subjects 10
5.8. Data Portability 10
5.9. Right to be Forgotten 11
5.10. Liability and damages 11
6. FAIR DATA PROCESSING GUIDELINES 11
6.1. Privacy Notices to Data Subjects 11
6.2. Obtaining Consents 12
7. ORGANIZATION AND RESPONSIBILITIES 12
8. GUIDELINES FOR ESTABLISHING THE LEAD SUPERVISORY AUTHORITY 14
8.1. Necessity to Establish the Lead Supervisory Authority 14
8.2. Main Establishment and the Lead Supervisory Authority 14
8.2.1. Main Establishment for the Data Controller 14
8.2.2. Main Establishment for the Data Processor 14
8.2.3. Main Establishment for Non-EU Companies for Data Controllers and Processors 15
9. RESPONSE TO PERSONAL DATA BREACH INCIDENTS 15
10. AUDIT AND ACCOUNTABILITY 15
11. CONFLICTS OF LAW 15
11.1. Obligations to inform, mandatory written form, choice of law. 15
11.2. Obligation of the Supplier to the Company 16
12. MANAGING RECORDS KEPT ON THE BASIS OF THIS DOCUMENT 17

13. VALIDITY AND DOCUMENT MANAGEMENT.....18

1. Purpose, Scope and Users

The **Aigo BS, LTD,** hereinafter referred to as "***The Company***", intents to comply with applicable Serbian laws and regulations related to personal data protection. This Policy sets forth the basic principles by which the Company processes the personal data of consumers, customers, suppliers, business partners, employees and other individuals or legal parties (hereinafter referred to as: "**The Clients**"), and indicates its responsibilities and employees while processing personal data.

This Policy applies to *the Company* and it's, directly or indirectly controlled, wholly-owned subsidiaries conducting business within the European Economic Area (EEA) or processing the personal data of data subjects within EEA.

The users of this document are all permanent or temporary employees, and all sub-contractors working on behalf of ***The Company***.

2. Reference Documents

- EU GDPR 2016/679 (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC)
- Data Protection Law of The Republic of Serbia (*"Sl. glasnik RS", br. 87/2018)*
- Information Security Management System of The Republic of Serbia, „Sl. Glasnik RS ", No. 6/2016)
- Obligation Relations Law of The Republic of Serbia *("Sl. list SFRJ", No. 29/78, 39/85, 45/89 - odluka USJ i 57/89, "Sl. list SRJ", br. 31/93 i "Sl. list SCG", br. 1/2003 - Ustavna povelja)*
- Information Security Policy of The Company

3. Terms definitions

The following definitions of terms used in this document are drawn from Article 4 of Data Protection Law of The Republic of Serbia (hereinafter referred to as: **The Law**).

Personal Data: Any information relating to an identified or identifiable natural person ("**Data Subject**") who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, 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.

Sensitive Personal Data: Personal data which are, by their nature, particularly sensitive in relation to fundamental rights and freedoms merit specific protection as the context of their processing could create significant risks to the fundamental rights and freedoms. Those personal data include personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union

membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

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

Data Processor: A natural or legal person, public authority, agency or any other body which processes personal data on behalf of a Data Controller.

Processing: An operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of the data.

Anonymization (Synonym**: Encryption):** Irreversibly de-identifying personal data such that the person cannot be identified by using reasonable time, cost, and technology either by the controller or by any other person to identify that individual. The personal data processing principles do not apply to anonymized data as it is no longer personal data.

Pseudonymisation (Synonym**: Coding):** The processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person. Pseudonymisation reduces, but does not completely eliminate, the ability to link personal data to a data subject. Because pseudonymised data is still personal data, the processing of pseudonymised data should comply with the Personal Data Processing principles.

Cross-border processing of personal data: Processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the European Union where the controller or processor is established in more than one Member State; or processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State;

Supervisory Authority: An independent public authority which is established by a Member State pursuant to Article 51 of the EU GDPR and by Republic of Serbia pursuant to Article 73 of The Law;

Lead supervisory authority: The supervisory authority in The Republic of Serbia is lead supervisor authority with the primary responsibility for dealing with a cross-border data processing activity, for example when a data subject makes a complaint about the processing of his or her personal data; it is responsible, among others, for receiving the data breach notifications, to be notified on risky processing activity and will have full authority as regards to its duties to ensure compliance with the provisions of The Law;

Local supervisory authority: Each *local supervisory authority* will still maintain in its own territory, and will monitor any local data processing that affects data subjects or that is carried out by an EU or non-EU controller or processor when their processing targets data subjects residing on its territory. Their tasks and powers includes conducting investigations and applying administrative measures and fines, promoting public awareness of the risks, rules, security, and rights in relation to the processing of personal data, as well as obtaining access to any premises of the controller and the processor, including any data processing equipment and means.

"Main establishment as regards a controller" with establishments in more than one Member State, the place of its central administration in the Union, unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the Union and the latter establishment has the power to have such decisions implemented, in which case the establishment having taken such decisions is to be considered to be the main establishment;

"Main establishment as regards a processor" with establishments in more than one Member State, the place of its central administration in the Union, or, if the processor has no central administration in the Union, the establishment of the processor in the Union where the main processing activities in the context of the activities of an establishment of the processor take place to the extent that the processor is subject to specific obligations under The Law;

Group Undertaking: Group of the companies connected according to the Law and any holding company together with its subsidiary. Company established in Serbia and its subsidiary in EU is a group undertaking.

4. Basic Principles Regarding Personal Data Processing

The data protection principles outline the basic responsibilities for organisations handling personal data. Article 4(8) of the Law stipulates that *"the controller shall be responsible for, and be able to demonstrate, compliance with the principles."*

4.1. Lawfulness, Fairness and Transparency

Personal data in **the Company** must be processed lawfully, fairly and in a transparent manner in relation to the data subject, according to The Law, Article 5(1).

4.2. Purpose Limitation

Personal data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (for example, profiling and marketing activities), without ***the Clients*** new explicit consents, according to The Law, Article 5(2)..

4.3. Data Minimization

Personal data collected, processed and stored in The Company must be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are collected, processed and stored. The Company must apply anonymization or pseudonymisation to personal data if there is high risk for the Clients' right and freedom and possibility to reduce the risks to the data subjects concerned.

4.4. Accuracy

Personal data collected in **the Company** must be accurate and, where necessary, kept up to date. The Company shall undertake reasonable steps to ensure that personal data that are inaccurate, having regard to the purposes for which they are collected and processed, are erased or rectified in a timely manner (The Law, Article 5(4)).

4.5. Storage Period Limitation

Personal data must be kept in the Company for no longer than is necessary for the purposes for which they are collected and processed (The Law, Article 5(5)).

4.6. Integrity, confidentiality and availability

Taking into account the state of technology and other available latest security measures, the implementation cost, and likelihood and severity of personal data risks, the Company must apply appropriate technical and procedural (administrative and organisational - operative) measures to process personal data in a manner that ensures appropriate security of personal data, including availability as they are needed and protection against accidental or unlawful destruction, loss, alternation, unauthorized access to, or disclosure (The Law, Article 5(6)).

4.7. Accountability

The Director of the Company as data controller must be responsible for and be able to demonstrate compliance with the Law principles outlined above.

5. Building Data Protection in Business Activities of the Company

In order to demonstrate compliance with the principles of data protection according to The Law, the Company shall build data protection into its business processes and activities.

5.1. Notification to Data Subjects

The Company must publish *Privacy Notice* on the company's web site and make link to this Policy. The *Privacy Notice* should contain all needed information regarding data collection, processing activities, data retention, data transfer, data protection measures and accountability and so on (See 6.1 section).

5.2. Data Subject's Choice and Consent

In the Company's business, data subjects give their consents for collecting and processing their personal data in legal mutually agreed and signed sale contracts for commercial wholesale purposes, or in Service Level Agreements (SLA) for the printers renting purposes (See 6.2 section).

5.3. Data collection

The Company must strive to collect the least amount of personal data possible. If personal data is collected from a third party DPO or named person in charge of data protection matters must ensure that the personal data is collected lawfully.

5.4. Use, Retention, and Disposal of data

The purposes, methods, storage limitation and retention period of personal data must be consistent with the information contained in the *Privacy Notice*. The Company must maintain the accuracy, integrity, confidentiality, availability and relevance of personal data based on the processing purpose. Adequate security mechanisms designed to protect personal data must be used to prevent personal data from being stolen, misused, or abused, and prevent personal data breaches. Director of the Company is responsible for compliance with the requirements listed in this section:

(1) Copies or duplicates of the data shall never be created without the knowledge of the Company's Director, with the exception of back-up copies as far as they are necessary to ensure orderly data processing, as well as data required to meet regulatory requirements to retain data.
(2) After conclusion of the contracted work, or earlier upon request by the Company, at the latest upon termination of the sale contracts or SLA, the Company shall, against prior consent of the Client, erase or encrypt (anonymise) personal data and archive together with contracts and SLA in order to retain them according to The Law (up to 10 years) or longer if necessary.
(3) Documentation which is used to demonstrate orderly data processing in accordance with the contracts and SLA shall be stored beyond the contract and SLA duration by the Company in accordance with the respective retention periods and relevant laws.

5.5. Data disclosure to the Third Parties

Whenever the Company uses a third-party supplier or business partner to process personal data on its behalf, DPO or named person in charge of data protection matters must ensure that this processor will provide security measures to safeguard personal data that are appropriate to the associated security risks. For this purpose, the *Processor GDPR Compliance Questionnaire* and *Supplier Security Policy* must be used.

The Company must contractually require the supplier or business partner to provide the same level of data protection and security measures to safeguard personal data. The supplier or business partner must only process personal data to carry out its contractual obligations towards the Company or upon the instructions of the Company and not for any other purposes. When the Company processes personal data jointly with an independent third party, the Company must explicitly specify its

respective responsibilities of and the third party in the relevant contract, SLA or any other legal binding document, such as the Supplier Data Processing Agreement.

(1) The Supplier shall ensure that the Company is able to verify compliance with the obligations of the Supplier in accordance with Article 26 of The Law. The Supplier undertakes (for example from EU country) to give the Company the necessary information on request and, in particular, to demonstrate the execution of the technical and organizational measures. Evidence of such measures may be provided by Compliance with approved Codes of Conduct pursuant to Article 59 of The Law;
(2) Certification according to an approved certification procedure in accordance with Article 61 of The Law;
(3) Current auditor's certificates, reports or excerpts from reports provided by independent bodies (e.g. auditor, Data Protection Officer, IT security department, data privacy auditor, quality auditor);
(4) A suitable certification by IT security or data protection auditing (e.g. ISO/IEC 27001).
(5) Where, in individual cases, audits and inspections by the Company or an auditor appointed by the Company are necessary, such audits and inspections will be conducted during regular business hours, and without interfering with the Supplier's operations, upon prior notice, and observing an appropriate notice period. The Supplier may also determine that such audits and inspections are subject to prior notice, the observation of an appropriate notice period, and the execution of a confidentiality undertaking protecting the data of other customers and the confidentiality of the technical and organisational measures and safeguards implemented. The Supplier shall be entitled to rejecting auditors which are competitors of the Supplier.
(6) Where a data protection supervisory authority or another supervisory authority with statutory competence for the Company conducts an inspection, para. 3 above shall apply mutatis mutandis. The execution of a confidentiality undertaking shall not be required if such supervisory authority is subject to professional or statutory confidentiality obligations whose breach is subjected to sanctions under the applicable criminal code.

5.6. Cross-border Transfer of Personal Data

Before transferring personal data out of the European Economic Area (EEA) adequate safeguards provided into Standard Contractual Clauses must be used including the signing of a Data Transfer Agreement, as required by the European Union and The Law, if required, authorization from the relevant Data Protection Authority must be obtained. The entity receiving the personal data must comply with the principles of personal data processing set forth in Cross Border Data Transfer Procedure.

General principle for transfers (Article 63 of The Law)

Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation shall take place only if, subject to the other provisions of this Regulation, the conditions laid down in this Chapter are complied with by the controller and processor, including for onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation. All

provisions in this Chapter shall be applied in order to ensure that the level of protection of natural persons guaranteed by The Law is not undermined. The controller is responsible to create and maintain evidence about data transfers to the third countries or international organizations (Article 47(5) of The Law), including name of the state or international organization, and document on the adequate technical and organisation measures if data transfer in accordance with Article 69 para. 2.

Transfers subject to appropriate safeguards (Article 64 of The Law)

(1) In the absence of a decision pursuant to Article 64(3) of The Law, a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has provided appropriate safeguards (Article 65 of The Law), and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.
(2) The appropriate safeguards referred to in paragraph 1 may be provided for, without requiring any specific authorisation from a supervisory authority, by:

(a) A legally binding and enforceable instrument between public authorities or bodies;
(b) Binding corporate rules for registering of the processing activities in accordance with Article 47 of The Law;
(c) Standard data protection clauses adopted by the Commission in accordance with the examination procedure referred to GDPR in Article 93(2) and Article 50 of The Law;
(d) Standard data protection clauses adopted by a supervisory authority and approved by the Commission pursuant to the examination procedure referred to GDPR in Article 93(2) and Article 51 of The Law;
(e) An approved code of conduct pursuant to Article 59 of The Law together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights; or
(f) an approved certification mechanism pursuant to Article 61 of The Law together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights.

5.7. Rights of Access by Data Subjects

When acting as a data controller, the Company's Director is responsible to provide data subjects with a reasonable access mechanism to enable them to access their personal data, and must allow them to update, rectify, erase, or transmit their Personal Data, if appropriate or required by law. The access mechanism will be further detailed in the *Data Subject Access Request Procedure* (prescribed by *Supervisor Authority),* and provide by manual help of the Company's administrators.

5.8. Data Portability

Data Subjects have the right to receive, upon request, a copy of the data they provided to the Company, in a structured format and to transmit those data to another controller, for free. DPO or named person in charge of data protection matters is responsible to ensure that such requests are

processed within one month, are not excessive (For example, if data subject sends requests to a company every day) and do not affect the rights to personal data of other individuals.

5.9. Right to be forgotten

Upon request, Data Subjects have the right to obtain from the Company the erasure of its personal data (Article 30 of The Law). When the Company is acting as a Controller, DPO or named person in charge of data protection matters must take necessary actions (including technical measures) to inform the third-parties who use or process that data to comply with the request in reasonable period of time (8 to 16 days).

5.10. Liability and damages

The Company and the Supplier shall be liable to data subject in accordance with Article 82 to 86 of the Law.

6. Fair Data Processing Guidelines

Personal data in Company must only be processed when explicitly authorised by DPO or named person in charge of data protection matters and approved by the Company's Director as data controller.

The Company must decide whether to perform the *Data Protection Impact Assessment* for each data processing activity according to the *Data Protection Impact Assessment (DPIA) Guidelines* (Article 54 of The Law).

6.1. Privacy Notices to Data Subjects

At the time of collection or before collecting personal data for any kind of processing activities including but not limited to buying and selling goods, services, or marketing activities, DPO or named person in charge of data protection matters is responsible to properly inform data subjects of the following: *the types of personal data collected, the purposes of the processing, processing methods, the data subjects' rights with respect to their personal data, the retention period, potential international data transfers, if data will be shared with third parties and the Company's security measures to protect personal data*. This information is provided through *Privacy Notice*.

If the Company has multiple data processing activities, it will need to develop different notices which will differ depending on the processing activity and the categories of personal data collected – for example, one Notice might be written for mailing purposes, and a different one for shipping purposes.

Where personal data is being shared with a third party, DPO or named person must ensure that data subjects have been notified of this through a Privacy Notice.

Where personal data is being transferred to a third country according to Cross Border Data Transfer Policy, the *Privacy Notice* should reflect this and clearly state to where, and to which entity personal data is being transferred.

Where sensitive personal data is being collected, the DPO or named person in charge of data protection matters must make sure that the *Privacy Notice* explicitly states the purpose for which this sensitive personal data is being collected.

6.2. Obtaining Consents

Whenever personal data processing is based on the data subject's consent, or other lawful grounds, DPO or named person in charge of data protection matters is responsible for retaining a record of such consent. DPO or named person in charge of data protection matters is responsible for providing data subjects with options to provide the consent and must inform and ensure that their consent (whenever consent is used as the lawful ground for processing) can be withdrawn at any time.

Where collection of personal data relates to a child under the age of 16, DPO or named person in charge of data protection matters must ensure that parental consent is given prior to the collection using the *Parental Consent Form* prescribed by Supervisor Authority (Article 16, para. 2 of the Law). The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology.

When requests to correct, amend or destroy personal data records, DPO or named person in charge of data protection matters must ensure that these requests are handled within a reasonable time frame. DPO or named person in charge of data protection matters must also record the requests and keep a log of these.

Personal data must only be processed for the purpose for which they were originally collected. In the event that the Company wants to process collected personal data for another purpose, the Company must seek the consent of its data subjects in clear and concise writing. Any such request should include the original purpose for which data was collected, and also the new, or additional, purpose(s). The request must also include the reason for the change in purpose(s). The DPO or named person in charge of data protection matters is responsible for complying with the rules in this paragraph.

Now and in the future, The Company must ensure that collection methods are compliant with relevant law, good practices and industry standards.

DPO or named person in charge of data protection is responsible for creating and maintaining a Register of the *Privacy Notices*.

7. Organization and Responsibilities

The responsibility for ensuring appropriate personal data processing lies with everyone who works for or with the Company and has access to personal data processed by the Company.

The key areas of responsibilities for processing personal data lie with the following organisational roles:

The Director of the Company makes decisions about, and approves the Company's general strategies on personal data protection and acting as controller of the processing activities.

The **Data Protection Officer (DPO) or any other relevant employee** in charge of data protection, is responsible for managing the personal data protection program and is responsible for the development and promotion of end-to-end personal data protection policies, and other activities as defined in *Data Protection Officer Job Description* (Articles 56, 57 and 58 of The Law);

The **lawyer of the Company,** monitors and analyses personal data laws and changes to regulations, develops compliance requirements, and assists business departments in achieving their Personal data Policy goals.

The **IT manager of the Company,** is responsible for:

- Ensuring all systems, services and equipment used for processing and storing data meet acceptable security standards.
- Performing regular checks and scans to ensure security hardware and software, and procedural measures are functioning properly.

The **Marketing manager**, is responsible for:

- Approving any data protection statements attached to communications such as emails and letters.
- Addressing any data protection queries from journalists or media outlets like newspapers.
- Where necessary, working with the Data Protection Officer or named person in charge of data protection, to ensure marketing and Company's promotion initiatives abide by data protection principles.

The **Human Resources Manager** is responsible for:

- Improving all employees' awareness of user personal data protection.
- Organizing *Personal data protection* expertise and awareness training for employees working with personal data.
- Ensuring end-to-end employee personal data protection. He/she must ensure that employees' personal data is processed based on the employer's legitimate business purposes and necessity.

The **Procurement Manager** is responsible for passing on personal data protection responsibilities to suppliers, and improving suppliers' awareness levels of personal data protection as well as flow down personal data requirements to any third party a supplier they are using. The Procurement Department must ensure that the Company reserves a right to audit supplier's security capacity.

The **Sales Manager** is responsible for passing on Company's personal data protection responsibilities to buyers, and improving buyers' awareness levels of personal data protection as well as flow down personal data requirements to any third party in wholesale chain of supply they are using.

8. Guidelines for Establishing the Lead Supervisory Authority

8.1. Necessity to Establish the Lead Supervisory Authority

Identifying a Lead supervisory authority for data protection is only relevant if the Company carries out the cross-border processing of personal data.

Cross border of personal data is carried out if:

a) *Processing of personal data is carried out by subsidiaries of the Company which are based in other Member States; or*
b) *Processing of personal data which takes place in a single establishment of the Company in the European Union, but which substantially affects or is likely to substantially affect data subjects in more than one Member State.*

If the Company only has establishments in one Member State and its processing activities are affecting only data subjects in that Member State than there is no need to establish a lead supervisory authority. If Company's subsidiary in EU (Croatia) processes data only online on server located in Company's main establishment (Serbia) then responsible Supervisor Authority shall be The Supervisor Authority of The Republic of Serbia (Trustee). The only competent authority will be the Supervisory Authority in the country where Company has main establishment and is lawfully established.

8.2. Main Establishment and the Lead Supervisory Authority

8.2.1. Main Establishment for the Data Controller

The Director of the Company needs to identify the main establishment (This is usually the headquarters of the company where the strategic decisions are made) so that the lead supervisory authority can be determined.

If the Company (**controller**) is based in an EU Member State and it makes decisions related to cross-border processing activities in the place of its central administration, there will be a single lead supervisory authority for the data processing activities carried out by the **Company**.

If Company has an subsidiary in EU that act independently and make decisions about the purposes and means of the processing of personal data on its server located at its establishment, and independently making decisions on cross-border data transfer to the main establishment of The Company (Serbia) only then there is need to have one lead supervisory authority in that EU state.

8.2.2. Main Establishment for the Data Processor

When the Company is acting as a data processor, then the main establishment (This means that it doesn't have the headquarters in the European Union) will be the place of central administration. In case the place of central administration is not located in the EU, the main establishment will be the establishment in the Serbia where the main processing activities take place.

8.2.3. Main Establishment for Non-EU Companies for Data Controllers and Processors

If the Company does not have a main establishment in the EU, and it has subsidiaries(s) in the EU that processing data on its own server located in EU, then the competent supervisory authority is the local supervisor authority from the EU member state where the subsidiary has main establishment. If the Company's subsidiary located in EU processes data online on the server located at the Company's main establishment, then the national Supervisor Authority from Serbia (Trustee) shall be responsible.

9. Response to Personal Data Breach Incidents

When the Company learns of a suspected or actual personal data breach, [e.g. DPO or named person in charge of data protection matters] must perform an internal investigation and take appropriate remedial measures in a timely manner, according to the *Data Breach Policy*. Where there is any risk to the rights and freedoms of data subjects, the Company must notify the relevant data protection authorities (Trustee) and national CERT, without undue delay and, when possible, within 72 hours.

10. Audit and Accountability

The Company shall use Audit Department or other relevant department (This could be legal department, or similar) responsible for auditing to audit how well business departments of The Company implement this Policy and to improve technical and organisational measures for data protection.

Any employee who processes data has to be trained on data collection, data processing and protection, law regulation and responsibilities that resulting from The Law, if violates rights and freedom of data subjects in accordance with this Policy and The Law, will be subject to disciplinary action and the employee may also be subject to civil or criminal liabilities if his or her conduct violates laws or regulations.

11. Conflicts of Law

This Policy is intended to comply with the laws and regulations in the place of establishment and of the countries in which the Company operates. In the event of any conflict between this Policy and applicable laws and regulations, the latter shall prevail.

11.1. *Obligations to inform, mandatory written form, choice of law*

(1) Where the data becomes subject to search and seizure, confiscation during bankruptcy or insolvency proceedings, or similar events or measures by third parties while in the Supplier's control, The Company shall notify the Client of such action without undue delay.
(2) The Company shall, without undue delay, notify to all pertinent parties in such action, that any data affected thereby is in the Company's sole property and area of responsibility, that data is at the Company's sole disposition, and that the Company is the responsible body in the sense of The Law.
(3) The duration of this Policy statement corresponds to the duration of the sale contracts, SLA and other contracts that The Company concludes outside its regular activities, if is necessary for regular business activities.
(4) No modification of this Policy section and/or any of its components – including, but not limited to the Supplier's (client's) representations and warranties, if any – shall be valid and binding unless made in writing or in a machine-readable format (in text form).
(5) In case of any conflict, the Law shall take precedence over the regulations of this Policy. Where individual regulations of this Policy section are invalid or unenforceable, the validity and enforceability of the other regulations of this Policy section shall not be affected.
(6) This Policy shall be governed by Serbian law. The competent Serbia courts shall have sole jurisdiction with respect to any dispute, controversy or claim arising under, out of or relating to the data subject right and any subsequent amendments of the contracts or SLA, including, without limitation, its formation, validity, binding effect, interpretation, performance, breach or termination as well as non-contractual claims.

11.2. *Obligation of the Supplier to the Company*

Technical and organizational measure (Attachment 1) that The Company applies in order to protect data subjects' personal data. These measures are subject to technical progress and development, so The Company is allowed to implement some alternative technical and organizational measures for personal data protection, but the security level has to be maintained and critical changes must be documented.

The Company shall request the Clients (Suppliers and Partners) to apply the same adequate technical and organizational measures to protect personal data that they obtained in the contracts and SLAs from the Company, including:

(1) The clients shall suport the Company/Controller in performing clients' rights and freedom according to the Law and this Policy.
(2) The clients shall farther support the Company/Controller to comply with obligations in data protection, data violence notification, DPIA and previous consultation with Supervisor Authority, including:

a) Securing appropriate data security level applying adequate technical and organizational measures for data protection given by the Company, taking in consideration technology state of art, circumstances and purposes of data processing, assessment of data protection risks due to ICT system vulnerabilities, violation of the Law, and capacity to detect and prevent data security events;

b) Obligation to notify Company on data protection violation in due time;
c) Help the Company regarding subjects' data protection and immediately send related information to the Company;
d) Support the Company in DPIA activities:
e) Support the Company with previous Supervisor Authority consultation.

(3) The clients shall guarantee, in scope of their responsibilities, that all employees included and another person that can be included in data protection contracts with the Company, will be prohibited to process data outside of purposes given in the Company's instructions;

(4) The Clients (suppliers, partners) shall notify in due time contact person in the Company regarding any question that is related to data protection, originated from the contracts and SLAs with the Company;

(5) If data subjects applies any objection or request against the Company in accordance with the Law, Article 82, clients (suppliers, partners) shall support the Company in defense from those requests, if it is possible and justified.

12. Managing records kept on the basis of this document

Record name	Storage location	Person responsible for storage	Controls for record protection	Retention time
Data Subject Consent Forms	[specify folder on the company Intranet or the database in your information system]	DPO or named person in charge of data protection	Only authorized persons may access the forms	10 years
Data Subject Consent Withdrawal Form	[specify folder on the company Intranet or the database in your information system]	DPO or named person in charge of data protection	Only authorized persons may access the forms	10 years
Parental Consent Form	[specify folder on the company Intranet or the database in your information system]	DPO or named person in charge of data protection	Only authorized persons may access the forms	10 years
Parental Consent Withdrawal Form	[specify folder on the company Intranet or the database in your information system]	DPO or named person in charge of data protection	Only authorized persons may access the forms	10 years
Supplier Data Processing Agreements	[specify folder on the company Intranet]	DPO or named person in	Only authorized persons may access the folder	5 years after the agreement has expired

		charge of data protection		
Register of Privacy Notices	[specify folder on the company Intranet]	DPO or named person in charge of data protection	Only authorized persons may access the folder	Permanently

13. Validity and document management

13.1. The owner of this document is DPO or named person in charge of data protection, CISO or named person in charge of security measures, who must check and, if necessary, update the document at least once per year.

13.2. This document is valid as of January 1st, 2019

General Manager
Dragan Popovic

Attachment 1 - Technical and Organisational Measures

1. **Confidentiality**
   - **Physical Access Control**
     No unauthorised access to Data Processing Facilities, e.g.: magnetic or chip cards, keys, electronic door openers, facility security services and/or entrance security staff, alarm systems, video/CCTV Systems
   - **Electronic Access Control**
     No unauthorised use of the Data Processing and Data Storage Systems, e.g.: (secure) passwords, automatic blocking/locking mechanisms, two-factor authentication, and encryption of data carriers/storage media
   - **Internal Access Control** (permissions for user rights of access to and amendment of data)
   - No unauthorised reading, copying, changes or deletions of Data within the system, e.g. rights authorisation concept, need-based rights of access, logging of system access events
   - **Isolation Control**
     The isolated processing of Data, which is collected for differing purposes, e.g. multiple client support, sandboxing;
   - **Pseudonymisation**
     The processing of personal data in such a method/way, that the data cannot be associated with a specific data subject without the assistance of additional Information, provided that this additional information is stored separately, and is subject to appropriate technical and organisational measures.

2. **Integrity**
   - **Data Transfer Control**
     No unauthorised reading, copying, changes or deletions of Data with electronic transfer or transport, e.g.: encryption, Virtual Private Networks (VPN), electronic signature;
   - **Data Entry Control**
     Verification, whether and by whom personal data is entered into a Data Processing System, is changed or deleted, e.g.: logging, document management

3. **Availability and Resilience**
- **Availability Control**
  Prevention of accidental or wilful destruction or loss, e.g.: Backup Strategy (online/offline; on-site/off-site), Uninterruptible Power Supply (UPS), virus protection, firewall, reporting procedures and contingency planning
- **Rapid Recovery** from backup system and recovery erased data using digital forensic tool and techniques.

4. **Procedures for regular testing, assessment and evaluation**
   - Data Protection Management;
   - Incident Response Management;
   - Data Protection by Design and Default;
   - **Order or Contract Control**
     No third party data processing without corresponding instructions from the Company, e.g.: clear and unambiguous contractual arrangements, formalised order management, strict

controls on the selection of the service provider, duty of pre-evaluation, and supervisory follow-up checks.