POLICY ON PROCEDURES AND MEASURES FOR PERSONAL DATA PROTECTION

Version: 1

Revision: 1

Date of validity: from *25.5.2018* onwards

DONAU LAB svetovanje in servis, d.o.o., Tbilisijska ulica 85, 1000 Ljubljana, registered: 5590787000, (hereinafter referred to as: "Controller") on the basis of Articles 24 and 25 of the Slovenian Personal Data Protection Act (Official Journal of the Republic of Slovenia, No. 94/07, as amended, hereinafter referred to as: ”ZVOP-1”) and Articles 24, 25 and 32 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter referred to as: ”General Data Protection Regulation”)

adopts the following

Policy on procedures and measures for personal data protection

I. General provisions

Article 1

This Policy on Procedures and Measures for Personal Data Protection (hereinafter referred to as: ”Policy”) lays down the technical, organisational and HR procedures and measures for the protection of personal data of the Controller, in order to comply with the legal requirements for the protection of personal data and to protect the rights of data subjects.

These measures are a set of binding rules, recommendations and principles based on practice, internal procedures, organisational structures and IT security.

Article 2

The purpose of this Policy is to ensure confidentiality, integrity, availability and accuracy of personal data, in the interests of data subjects, at every stage of personal data processing. All employees must be familiar with the risks associated with technical and information systems and communication technology and thus process personal data with due diligence.

The measures laid out in this Policy are drawn up by taking into account the latest technological developments and costs, implementation and the nature, scope, circumstances and purposes of processing, as well as the risks to the rights and freedoms of individuals, and ensure adequate data security in relation to the potential risks posed by processing, in particular in the event of accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to personal data transmitted, stored or otherwise processed.

Article 3

The Controller shall comply with the established information security rules.

The Policy is based on the assumption that there is no such thing as absolute security and that information security is an ever-changing landscape that requires the Controller to continuously improve and adapt security to changing conditions. The measures are a compromise between technical and implementation capabilities, with the latter conditional upon HR and economic considerations on part of the Controller.

Article 4

When processing personal data, the Controller shall comply with the general principles related to personal data processing.

The Controller processes only personal data for which it has the appropriate legal basis in accordance with the provisions of the ZVOP-1 and the General Data Protection Regulation.

Personal data may only be collected for specified and legitimate purposes and may not be further processed in a manner that would render the processing incompatible with those purposes, unless permitted so by the relevant legislation.

When processing personal data, the Controller shall ensure that the personal data are:

- processed lawfully, fairly and in a transparent manner in relation to the data subject,
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes,
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed,
- accurate and, where necessary, kept up to date,
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed, unless otherwise provided by law,
- processed in a manner that ensures appropriate integrity and security of the personal data,
- subject to implementation of appropriate technical or organisational measures to safeguard them against unauthorised or unlawful processing and against accidental loss, destruction or damage.

Article 5

This Policy applies to all employees with the Operator, regardless of whether they are in an employment relationship with the Operator (hereinafter referred to as: "employees"). The Policy is particularly aimed at the employees directly or indirectly involved in the processing of personal data and in ensuring the security of IT technology.

Article 6

The terms used in this Policy shall have the meanings as defined in the applicable ZVOP-1 and the General Data Protection Regulation.

II. List of records of personal data processing activities

Article 7

For the purpose of identifying and keeping a record of all types of personal data processed by the Controller, the Controller shall keep a List of records of personal data processing activities (hereinafter referred to as: ”List of records”), which shall contain a record of all the personal data filing systems

processed, aimed at providing a complete overview of the flow of personal data. Thelist of records shall constitute the basis for adoption of technical, organisational and HR measures for the protection of personal data as laid out in this Policy.

The list of records shall be kept in manner so that the following is clearly stated for each record of personal data processing activities:

- what types of personal data are processed,
- categories of data subjects to which the personal data relate,
- purpose of personal data processing,
- legal basis for personal data processing,
- expected period of data retention or deletion and
- any persons or users to whom the personal data may be disclosed,
- whether the data are exported to a third country and/or an international organisation,
- technical, organisational and HR measures in place to ensure the protection of personal data.

The Controller shall ensure that the list of records is accurate and up to date. The Controller shall give the supervisory authority access to the list of records upon request.

Employees who process personal data in the course of working and carrying out tasks for the Controller must be familiar with the list of records; access to the list for consultation must also be provided to anyone who requests it and has a legitimate interest in consulting the list (e.g. data subject, supervisory authority, police on the basis of a legal authorisation).

Article 8

Taking into account the nature, scope, context and purpose of processing applicable to the Controller and evidenced by the list of records, the Controller concludes that data processing does not pose a significant risk to the rights and freedoms of natural persons and therefore no prior impact assessment in relation to data processing is necessary. If necessary, the impact assessment will be carried out as an Annex to this Policy.

The Controller shall undertake to review the risks and assess whether an impact assessment is necessary in relation to the processing whenever the risk posed by the processing operations changes, when processing new personal data, before applying new technologies, or when the nature, scope, circumstances and purposes of the processing of personal data change.

III. HR measures

Article 9

Conflicting tasks and responsibilities regarding personal data processing are assigned to different persons or departments in order to identify unauthorised or unintentional changes to data as soon as possible.
The roles and tasks are defined in accordance with the internal organisation of the Controller, with the CEO of the Controller as primarily responsible for determining the purposes for which personal data are

processed and authorized to determine the information technology means or operational processes, and ensure data security and the provision of technical, HR and organisational measures.

Access to personal data is defined in the list of records.

The CEO of Controller shall have final authority and responsibility for the proper implementation of this Policy.

Article 10

In relation to the Data Protection Officer, the Controller shall comply with Article 37 of the General Data Protection Regulation.

If the Controller appoints a Data Protection Officer, this shall be carried out by means of a Decision appointing the Data Protection Officer.

Article 11

All persons processing personal data within the Controller shall be obliged to process such data only with the Controller's authorisation and in line with the Controller's instructions, to implement the procedures and measures for personal data protection laid out in this Policy and to protect personal data they have been made aware of or that have been disclosed to them in the course of their work.

The data protection obligation does not cease upon termination of the employment relationship.

All persons processing personal data in the course of their work must be familiar with the legislation on personal data protection and the content of this Policy. To this end, the Controller shall ensure that such employees sign a special Personal Data Protection Declaration, indicating that they are familiar with the provisions of this Regulation and of the legislation on personal data protection.

In accordance with the principle of accountability, the Controller shall provide appropriate training on the protection of personal data to employees who handle personal data, if necessary.

Employees shall be subject to disciplinary action, damages and penalties for breach of provisions of this Article. A breach of the provisions of this Policy shall be considered a serious breach of the rights and obligations arising from the employment relationship, which shall constitute grounds for ordinary termination due to misconduct or, in case of serious breaches, for extraordinary termination.

IV. Physical security

Article 12

Personal data and IT systems must be adequately protected against theft, damage and adverse impacts from the environment.

The premises where personal data, copies thereof and IT systems are located must be protected against fire (fire extinguishers, fire detector), water leaks, flooding and electromagnetic interference, within the prescribed climatic conditions.

All IT systems that are critical to the Controller must be located in a secure environment. All premises containing personal data carriers, hardware and software must be physically secured (e.g. locked, placed in a drawer or cabinet protected with a lock or password etc.) to prevent unauthorised persons from accessing the data.

Such secure premises or the building where personal data is stored as a whole shall be secured by mechanical or technical means.

Article 13

Personal data must not be stored outside secure premises.

Secure premises must not be left unattended and are to be locked if the persons overseeing them are absent. Outside working hours, secure premises are to be locked and keys must be kept in accordance with the house rules. Keys are not to be left in door locks.

Article 14

Outside working hours, cabinets and desks with personal data carriers must be locked, while computers and other hardware must be switched off and locked physically or by means of a programme.

When absent from their work space, employees observe the "clean desk policy" and the "clean screen policy". Personal data carriers are not to be left on desks in the presence of persons who do not have the right to consult them, and computer screens must be locked physically or by means of a programme.

Personal data carriers located outside secure premises (i.e. in corridors, common areas) must be locked at all times.

Article 15

In customer-facing premises, data carriers and computer screens must be placed in such a manner that they cannot be viewed by customers.

Persons carrying out maintenance of premises, hardware and software, as well as visitors and business partners, are only allowed in the secured premises if the responsible employee of the Controller is informed thereof.

V. Protecting data integrity and confidentiality at the time of reception and transmission

Article 16

The employee responsible for receiving and registering mail:

1) must hand the postal item containing personal data over directly to the individual or the department to which the item is addressed,
2) shall open and inspect all postal items and items arriving to the Controller by other means, except for items referred to in items 3 and 4 of this Article,
3) shall not open postal items addressed to another authority or organisation and delivered in error, as well as items marked as personal data,
4) shall not open postal items addressed to an employee when the envelope features an indicates that it is to be delivered personally to the addressee; the same applies to items on which the employee's personal name is indicated first, without stating the employee's official position, followed by the address of the Controller.

Article 17

Personal data is to be sent by registered mail or in person by courier.

The envelope in which the personal data are transmitted must be made in such a way that the contents of the envelope cannot be read in daylight or when the envelopes are illuminated by a regular light. The envelope must also ensure that the envelope cannot be opened and its contents read without a visible sign of the envelope having been opened.

Article 18

Personal data may be transmitted by IT, telecommunication and other means only if appropriate procedures and measures are in place to prevent unauthorised persons from obtaining or destroying data or interfering with their integrity, and from gaining unauthorised access to the contents of the data.

If messages containing personal data are transmitted by electronic means, the controller shall ensure that there are technical procedures in place to prevent the transmitted information from being intercepted, copied, modified, altered, diverted or destroyed.

Article 19

The processing of special categories of personal data must be specifically marked and secured.

Special categories of personal data shall be sent to the addressees in sealed envelopes against signature in a delivery book or by means of a return receipt.

The data referred to in the preceding paragraph may be transmitted over telecommunications networks only if they are specifically secured by cryptographic methods and electronic signatures in such a manner as to guarantee that the data cannot be read during transmission.

VI. Ensuring confidentiality, integrity and resilience of data processing systems and services

Article 20

Access to highly sensitive information shall be regulated by the Controller by various technical means and by establishing security zones and restricting access.

Users and IT services and systems are to be separated in networks. Similarly, development, testing and operating environments shall also be separated.

Access controls shall be put in place to ensure that only authorised persons can access IT system functions, programmes and data.

Article 21

Access to the software is governed by an access rights policy. Access is restricted to pre-designated employees and external service providers.

Access to IT systems is limited to the rights necessary to perform specific tasks (e.g. right to read or edit, administrator access). When granting access rights, the Controller shall follow the "*need-to-know*" principle, which means that users should not receive more rights than necessary to perform their tasks or access the data.

Each user is assigned a unique (personal) user name (user ID). This also applies to privileged access rights (e.g. for administrators).

To prevent attacks and security risks, all critical access attempts, and in particular failed access attempts, are logged.

External maintenance access is only activated for the duration of the maintenance following an official and documented request. Once the maintenance work has been completed, the maintenance accesses granted are deactivated or disabled.

If an employee changes posts, access rights are reviewed and adjusted as necessary. In general, access rights are to be regularly checked and updated.

If an employee ceases to work for the Controller, all access authorisations granted shall be withdrawn no later than at the end of the last working day. The same applies to all external service providers.

Article 22

Hardware and system software, including input/output units, must be protected in a way that safeguards data integrity and confidentiality.

All personal computers allowing access to personal data are protected by a username and password.

Software installed on the computer that allows access to personal data is protected by a username and password.

The arrangements for storing and modifying passwords are determined by the authorized person.

Article 23

All passwords and procedures used to enter and administer a network of personal computers (control passwords), administer e-mails and administer application programmes shall be kept in sealed envelopes and protected from being accessed by unauthorised persons. They are to be used only in exceptional circumstances or emergencies.

Any use of the content of these sealed envelopes shall be documented. After each such use, new passwords are to be set up.

Article 24

Maintenance, repair, modification and additions to the system and application software may only be carried out with the approval of the CEO or a representative (administrator) duly authorized by the CEO, and performed exclusively by authorised computer service providers, organisations and individuals who have concluded relevant contracts with the Controller. Contractors must document any changes and additions to the system and application software.

Employees are prohibited from installing software without the knowledge of the person responsible for the operation of the computer IT system. Similarly, they are prohibited from removing software from the premises without the authorisation of the head of the organisational unit and the knowledge of the person responsible for the operation of the computer IT system.

Article 25

The content on network servers and local workstations storing personal data are checked for the presence of computer viruses on an ongoing basis.

All workstations, laptops and other equipment must be equipped with an activated and up-to-date anti-virus protection. All computers on the workstation must be equipped with a combination of a local firewall and a local system for intrusion detection and prevention. All laptops and other equipment must be equipped with a local firewall.

When a computer virus is detected, it is eliminated with as soon as possible by the relevant specialized department, at the same time identifying how the computer IT system was infected.

All personal data and software intended to be used in a computer IT system that the Controller receives on carriers for transmitting computer data or through telecommunication channels must be checked for the presence of computer viruses before use.

Article 26

If the user or administrator leaves the workstation or does not make any entries, a password-protected screen lock must be activated automatically after a certain time limit.

On systems where this is technically possible, the user is automatically logged off if no entries have been made within a certain time limit.

For laptops, appropriate hard disk encryption is used. Connection control can also be used to restrict or disable the use of external devices on clients.

Business information is generally stored locally on workstation computers or laptops only as long as necessary and is stored on centrally managed systems designed for this purpose.

Article 27

Office communication devices such as printers, copiers, fax machines, etc. must likewise be protected against unauthorised access and manipulation.

Controller must also take appropriate IT security measures in the case of remote access.

VII. Ensuring data availability in the event of a physical or technical incident

Article 28

All data operations are logged in the system log files. Logging must be carried out by an administrator in accordance with the requirements and capabilities of the operating systems and applications.

The audit trail must make it possible to establish when and by whom individual personal data have been entered into the database, used or otherwise processed or altered. All events must be time-stamped.

Article 29

Personal data is only disclosed to users who provide the relevant legal basis or written request or consent of the data subject.

For each transmission of personal data, the person entitled must submit a written application clearly indicating the legal basis authorising the user to obtain the personal data or the application must be accompanied by a written request or consent from the data subject.

Any disclosure of personal data is recorded in a record of disclosures showing which personal data have been disclosed, as well as where or to whom, when and on what basis. The traceability records of data transmissions shall be kept in chronological order.

Original documents are never transmitted, unless ordered so by a court in writing. During the absence, the original document must be replaced by a copy.

Article 30

To restore the computer system in the event of failures and other exceptional circumstances, regular copies of the content on the network server and local workstations, if the data is located there, shall be made (i.e. data backup).

For data subject to a high availability requirement, a backup is made on a regular basis so that the system as a whole can be restored to operational readiness if one or more components fail.

Article 31

In the event of a system failure, it must be ensured that no critical information is lost.

Backup data carriers must be stored in locations that meet the requirements of confidentiality, integrity and availability of the information concerned. This includes sufficient spatial distance between the backup data carriers and the source of data (e.g. storage in other premises).

It must be ensured that in an emergency, administrators have access to backup data carriers.

Time limits for storage and erasure of backup copies must be set.

Article 32

Information is archived in accordance with legal, contractual and commercial requirements.

The storage period for information that is critical for the business and archival copies must be specified.

Archival data must be stored or kept in locations that meet the requirements of availability, integrity and confidentiality.

VIII. Regular testing, assessment and evaluation of measures

Article 33

The Controller undertakes to regularly test, assess and evaluate the effectiveness of technical and organisational measures for ensuring secure processing.

To this end, the Controller shall check the lawfulness of the processing of personal data at least once a year. For the purpose of internal control, the Controller shall review the logs relating to the processing operations (log files) and consult the relevant information security experts.

IX. Data storage period and erasure

Article 34

The Controller shall ensure that the personal data storage period is limited to the shortest possible period. To this end, the Controller shall lay down time limits for the erasure of personal data in the list of records.

After the expiry of the storage period, personal data shall be erased or permanently destroyed or anonymised, unless otherwise provided by law or another act.

Article 35

To erase data from computer media, a method that makes it impossible to restore all or part of the erased data shall be used. The erasure must be complete and irreversible. Inaddition to such data carriers, data in the "Deleted" or "Recycle Bin" folders or other appropriate folders/directories must also be erased so that the content can no longer be restored.

Data on traditional carriers (documents, files, registers, lists etc.) shall be destroyed in a manner that prevents all or part of the destroyed data from being read. Accompanying material (e.g. matrices, calculations and graphs, sketches, test or failed print-outs etc.) is destroyed in the same manner.

It is forbidden to dispose of waste data carriers containing personal data in the rubbish bins.

When personal data media are transported to the destruction site, it is necessary to ensure that they are adequately secured during transport.

X. Services provided by external legal or natural persons

Article 36

Controller may entrust individual data processing operations to an external legal or natural person (hereinafter referred to as: "Processor") providing sufficient guarantees to implement appropriate technical and organisational measures for the protection of personal data. A processor providing agreed services off the Controller's premises must have in place at least the same level of personal data protection as is provided for in this Policy.

In such cases, Controller and Processor shall conclude appropriate written contractual arrangements for the processing of personal data, setting out the rights and obligations of both parties. Such an agreement must lay down the conditions and measures to ensure that personal data are protected and secured, as well as the obligations of the Processor vis-à-vis the Controller. This also applies to processors who maintain hardware and software or build and install new hardware or software.

Under such an agreement, the Processor may only carry out, on behalf and for the account of the Controller, the agreed tasks relating to the processing of the Controller's personal data. The Processor may not process the personal data or use them for any other purpose.

XI. Reporting security incidents

Article 37

The Controller shall ensure a consistent and effective system for handling security incidents, including documenting and reporting security incidents.

For this purpose, the Controller shall have in place an IT system capable of surveillance to detect events (e.g. firewall, intrusion detection, surveillance system). IT systems further enable the recording of all events relevant in terms of security or critical for the system. The person responsible for monitoring these records is the authorised person (administrator) of the IT system, who must report any incidents relevant to the security to the management of the Controller.

All employees are obliged to immediately inform the management of the Controller about any activity involving the discovery or unauthorised destruction of confidential data, malicious or unauthorised use, misuse, appropriation, inaccessibility, alteration or corruption of data, and to attempt to prevent such activities themselves.

Controller shall record any personal data breaches in a security incident log, indicating the facts related to the personal data breach, the impact of the personal data breach and the corrective measures taken.

Security incidents shall be entered in the security incident log in chronological order, regardless of the level and type of risk to the rights and freedoms of individuals. In particular, the Controller shall record breaches of data confidentiality (e.g. unauthorised data disclosure), breaches of data accessibility and breaches of data integrity (e.g. unauthorised data alteration).

Article 38

If a personal data breach is likely to result in a risk to the rights and freedoms of natural persons, the Controller must notify the competent supervisory authority without undue delay and at the latest within 72 hours of becoming aware of the breach, in accordance with Article 33 of the General Data Protection Regulation.

When a personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the Controller shall, in accordance with Article 34 of the General Data Protection Regulation, also communicate the personal data breach to the data subjects without undue delay.

XII. Final provisions

Article 39

Any amendments and supplementations to this Policy shall be adopted in writing and in the same manner as the Policy.

Article 40

The Policy shall enter into force on the day it is published.

The Policy shall be published in the manner usual with the Controller, enabling all employees of the Controller to become acquainted with the Policy content.

Article 41

This Policy shall be made available and accessible to all employees in the HR department of the Controller during working hours. The employees shall be allowed to acquaint themselves with the content of this Policy without supervision.

In _____, on _____

Aleš Boškin, CEO

_____