Security policy

1) **Introduction:** The Regional Association of Solid Waste Management Bodies of Central Macedonia (hereinafter: the Agency) pays special attention to safety and respects the private character and confidentiality of personal data. For this reason, we invest time and resources to protect your privacy. In this effort we are in an ongoing process of information and education, in order to fully comply with the applicable national, European and international legal framework and in particular with the General Regulation of Personal Data Protection 679/2016 of the European Union and its Greek implementing law L. 4624/2019.

2) **Purpose:** With this security policy (hereinafter: the policy), the Agency aims to inform about the way in which personal data is collected, stored, used and transmitted, the security measures we take to protect personal data, the reasons and the duration of their storage, and inform about the type of personal data collected. It concerns any transaction or series of transactions performed with or without the use of automated means, in personal data or in personal data sets, such as the collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or any other way of making them available, the alignment or combination, restriction, erasure or destruction.

   This Policy is updated from time to time and may be amended whenever necessary, without prior notice, always within the applicable legal framework and in accordance with any changes to current privacy legislation. Users of the Agency's services are advised to follow the current security policy for any modifications.

3) **What does personal data mean?**

   Personal data is any kind of information that concerns a specific natural person whose identity can be verified (e.g. name, identity number, address, etc.). Data related to health (physical or mental condition, reception of medical services, etc.) are included in the general term personal data, but consist a special category of data.

   The Agency applies the "principle of data minimization". In other words, it processes the absolutely necessary personal data required for the execution of the tasks assigned by the Articles of Association of the Agency (Government Gazette 1908 B / 2012).

4) **Collection:**

   4A) In what ways are the data collected:

   Documents containing personal data are received by the Protocol section in printed or digital form.

   4B) What kind of data are collected:

For the employees of the service all the personal data that are necessary for their recruitment, salary, regular employment in the Agency, and their retirement, are collected. More precisely, the data collected during the publication of this are (indicative and not restrictive) the following:

- Full name
- Father's name
- Mother's name
- Phone numbers
- Birth Certificate
- ID Card
- Tax Registration Number (TIN)
- Certificate of marital status
- Qualifications
- Extract from the criminal record
- Bank account number (I.B.A.N.)
- Social Security Registration Number (SSRN)
- Former insurance life
- Health certificate for professional competence
- Results of medical examinations when necessary

For contractors (or prospective contractors) of public procurement concluded by Agency, all the data that are necessary for the submission of a bid, the assignment of a project or procurement, the supervision of their completion stages, their receipt and repayment, are collected. More precisely, the following data are potentially collected:

- Full name
- Father's name
- Mother's name
- ID Card of a legal representative or other members of the company contracting or submitting a financial bid
- Natural person criminal record of the legal representative or other members of the company contracting or submitting a financial bid
- Articles of Association
- Tax Registration Number (TIN)
- Social Security Registration Number (SSRN)
- Bank account number (I.B.A.N.)
- E-mail account (e-mail)
- Phone number
- Business headquarters address
- Extract from the criminal record of members of the administrative and / or supervisory body, Chief Executive Officer, administrators, legal representatives
- Tax clearance certificate
- Insurance clearance certificate
- Certificate of registration in the Chamber (General Commercial Registry)
- Commencement of Business Activities at the Tax Office
- Qualifications
- Certificates of experience
- Certificate of non-suspension of business activities

- Certificates of non-inclusion in any bankruptcy and / or pre-bankruptcy proceedings
- Tax clearance certificate
- Insurance clearance certificate of employees
- Insurance clearance certificate of a natural person
- Annual turnover for a specific series of years
- Information on any insurance coverage of occupational risks
- Record and financial data of other contracts of the company with public bodies.
- Business vehicle registration number

In the event that the tendering agency, contractor or third party involved in the contract submits supporting documents containing other categories of simple or special categories of personal data, which are not provided in accordance with the above paragraph, they are provided freely and with their explicit consent and will be processed if required.

4C) For what reasons are the data collected / Legal basis

The operation of the Agency is based on the laws L. 3463/2006 and L. 4555/2018 as their amendments are in force today.
The technical projects, supplies and services implemented by the Agency are based on L. 4412/2016 as its amendments are in force today.
The Human Resources Department is based on the laws, L. 3528/2007, 3584/2007 code of civil servants (responsibilities and duties) as their amendments are in force today.

The following also apply:
L. 4305/2014 article 28, on the authenticity of documents and genuine copies.
L.4210/2013 article 7 and L. 3584/2007 article 14, which concern the physical and medical ability of employees in the Public Sector.
L. 4354 / 2015 regarding the salary issues of employees in the Public Sector.
Law 3584/2007, article 16 on the certificate of criminal record of employees in the Public Sector.

5) Data retention time

The Agency does not erase any personal data. In the event that you wish any of your personal data to be erased, you may exercise the right to erasure as described in Article 6 of this policy. The Agency will examine the legality of the request under current national and European law and will respond in writing either to confirm the erasure or to justify its refusal.

6) Rights

As long as the Agency retains your personal data, you have the following rights:

- **Right to disclose** your data. The disclosure of the data we maintain for the interested party will take place no later than thirty (30) working days from the receipt of the relevant request. They will be picked up for security reasons from the Agency's headquarters, only upon presentation of the ID card or other certificate of identity.

- **Right to correct** your data. The correction will concern any processing that may take place after its notification to the Agency. The request for correction can be made either by e-mail or in person. In any case, the presentation of a certificate of identity is required.
- **Right to erase** your data. Due to the fact that the Agency collects the absolutely necessary personal data, within thirty (30) working days from the receipt of the relevant request, you will be informed about which tasks the Agency will not be able to perform and whether this is legal according to with existing European and national legislation. If it is legal and feasible, then within thirty (30) working days the recording will be performed and you will be informed in writing about it.
- **Right to portability**. You can request the transfer of your personal data to another Data Controller at any time. Within thirty (30) working days the Agency will process the legality of the request and you will receive written notice of the fulfillment or not of your request. In case of non-compliance, you will receive a written reasoned refusal from the Agency.
- **Right to complain** to the supervisory authority in case of violation of the security of your data or their illegal processing. See Article 10 of this policy for more details.

In any case, the physical presence requirement is satisfied by the presence of a third party bearing a certificate of identity and a validated authorization from the person concerned.

7) Transmission of data to third parties

On a scheduled basis or when required, the Agency may transmit any required personal data which it maintains, to public administration structures including structures within the restricted or broader public sector. As the transmission is performed exclusively for the execution of the duties of the Agency (and the conditions of article 24 of L. 4624/2019 are met), neither the consent nor the information of the data subject is required according to article 26 of L. 4624/2019. The following are indicative and not restrictive:

- Single Social Security Entity – Social Security Institute.
- Manpower Employment Organization
- Labour Inspection
- Ministries of Justice, Interior and Finance and in the Services of these Ministries
- Court of Audit
- General Accounting Office of the State (Single Payment Authority and Pension Service)
- Potentially to all the bodies of the Central and General Government

8) Security measures

The Agency implements appropriate technical and organizational measures aimed at the secure processing of personal data and the prevention of their accidental loss or destruction and unauthorized and / or illegal access to them, their use, modification or publication. In particular, some of the measures implemented by the Agency to achieve the above objective are the following:

- Regarding the physical record:
  - ✓ Preservation of files in electronic form.
  - ✓ Limited staff access to the physical record
  - ✓ Premises security (office locking)
  - ✓ Surveillance of areas by security cameras
- Regarding digital record:
  - ✓ Firewall against external attacks
  - ✓ SSL encryption protocols between the user's browser and the Agency server. The same type of encryption protects the e-mail of the Agency.
  - ✓ Existence of a password on any computer connected to the Agency's network or processing personal data on a local basis. Access to personal data processing applications is also restricted by passwords.
  - ✓ Encryption of files on disks that store personal data.
  - ✓ Daily or weekly backup of files and databases maintained by the Agency. The frequency depends on the location and type of files.
  - ✓ The website of the Agency has been designed based on the latest technologies and with special care regarding its performance and effectiveness.

9) Conclusion of confidentiality agreements

The collaborations of the Agency with external partners who come in contact potentially or in a confirmed way with personal data, are governed by confidentiality agreements.

10) Details of the Data Protection Officer - Data Protection Authority

For any question regarding the data processed by the Agency and the exercise of the rights guaranteed by the European Regulation 679/2016 and the law L. 4624 / 2019, you can contact the office 212 by phone at 2310508800 (internal 1399) or by e -mail at dpo@fodsakm.gr. The Data Protection Officer of the Agency is Mr. Karakatsanis Polykarpos.

You have the right to file a complaint with the Personal Data Protection Authority (website:www.dpa.gr): Call Center: +30 210 6475600, Fax: +30 210 6475628, E-mail: contact@dpa.gr.

11) Contact

The head office of the Agency is located in the center of Thessaloniki, at Frangon 6-8 on the 2nd, 3rd and 4th floor. The contact phone is +30 2310 508800 and the call center is open daily (Monday to Friday) from 07:00 am until 15:00 pm. The email address is: ota@otenet.gr.