**WEBSITE PRIVACY AND PERSONAL DATA PROTECTION POLICY**

**1. PURPOSE AND SCOPE**

This Website Privacy and Personal Data Protection Policy (hereinafter referred to as the ‘Policy’), Atlantis Mühendislik Golf Peyzaj Tarımsal Sulama Sistemleri İnşaat Taahhüt Sanayi Ve Ticaret A.Ş. (hereinafter referred to as the ‘Company’) aims to inform the relevant persons in accordance with the Law No. 6698 on the Protection of Personal Data (hereinafter referred to as the ‘KVKK’).

**2. BASIC PRINCIPLES FOR THE PROCESSING OF PERSONAL DATA**

The Company, as the data controller, processes your data in accordance with the following principles:

* **Compliance with the Law and the Principle of Honesty**

In data processing activities, legal regulations and honesty rules are adhered to. When processing personal data, only legitimate purposes are pursued, transparency is ensured, and the interests of individuals are not violated.

* **Keeping Personal Data Accurate and Up-to-Date When Necessary**

It is essential to keep the data accurate and up-to-date when necessary, regular checks and updates are carried out in this context, and necessary measures are taken for the effective management of this process.

* **Processing for Specific, Explicit, and Legitimate Purposes**

Personal data is processed only for specific, explicit, and legally legitimate reasons. These purposes are clearly stated in the relevant sections of the Policy.

* **Being Relevant, Limited and Proportionate to the Purpose of Processing**

Data are collected only to the extent and within the limits required by the specified purpose; unnecessary or excessive data processing practices are avoided.

* **Retention for the period stipulated in the relevant legislation or required for the purpose for which they are processed.**

Personal data is stored for the period stipulated in the relevant legislation or required by the purpose of processing. When the period expires or the reason for processing disappears, the data is deleted, destroyed, or anonymised.

**3. PERSONAL DATA PROCESSING CONDITIONS**

According to the KVKK, personal data may be processed depending on the following legal grounds:

* **Explicitly Stipulated in Laws**

In cases where a legal provision explicitly requires data processing, processing may be carried out without seeking the consent of the data subject.

* **Inability to Obtain Explicit Consent Due to Factual Impossibility**

If a person is unable to express their consent due to a factual impossibility, or if the processing of data is necessary to protect someone else’s life or physical integrity, the data may be processed without explicit consent.

* **Establishment or Performance of a Contract**

Data processing may be carried out without consent if it is directly related to the establishment or performance of a contract.

* **Fulfillment of Legal Obligations**

Personal data may be processed if it is necessary for the Company to fulfill its legal obligations.

* **Public Disclosure of Personal Data**

If the data subject has made their personal data public on their initiative, such data may be processed in accordance with the purpose of its disclosure.

* **Establishment or Protection of a Right**

If the processing of personal data is necessary for the establishment, exercise, or protection of a legal right, it may be processed.

* **Legitimate Interest**

If processing is necessary for the legitimate interests of the Company, the data may be processed provided that the fundamental rights and freedoms of the data subject are not violated.

* **Explicit Consent**

In cases not covered by the exceptions listed above, personal data is processed based solely on your explicit consent.

* **Processing of Special Categories of Personal Data**

Special categories of personal data are processed with appropriate security measures in place, only in cases permitted under Article 6 of the Personal Data Protection Law (KVKK).

**4. TRANSFER OF PERSONAL DATA**

Your collected personal data may be transferred to business partners located within or outside the country in accordance with the relevant provisions of this Policy and Articles 8 and 9 of the Personal Data Protection Law (KVKK). These transfers are carried out in compliance with legal requirements and with necessary data security measures in place.

**5. SECURITY OF PERSONAL DATA**
The Company takes all reasonable administrative and technical measures to ensure the secure storage of personal data and to prevent unlawful processing, access, or loss of such data. These measures are designed to prevent unauthorized access, intentional deletion, alteration, or damage to the data.

Technical and physical security precautions are implemented to ensure that only authorized personnel can access personal data. Authorization processes are carefully planned to prevent individuals or systems from accessing more data than is necessary.

* **Some of the security measures implemented include:**
* **Network and application security are ensured.**
* **A closed network system is used for personal data transfers over networks.**
* **Security measures are taken during the procurement, development, and maintenance of IT systems.**
* **The security of personal data stored in the cloud is ensured.**
* **Disciplinary regulations, including data security provisions, are in place for employees.**
* **Regular training and awareness programs on data security are conducted for employees.**
* **An authorization matrix has been established for employees.**
* **Access logs are maintained regularly.**
* **Corporate policies on access, information security, usage, storage, and destruction have been developed and implemented.**
* **Data masking measures are applied when necessary.**
* **Confidentiality agreements are signed.**
* **Data access rights of employees who change roles or leave the company are revoked.**
* **Up-to-date antivirus systems are used.**
* **Firewalls are in place.**
* **Contracts include data security clauses.**
* **Additional security measures are taken for personal data transferred via paper, and such documents are sent in a classified document format.**
* **Policies and procedures for personal data security have been established.**
* **Personal data security incidents are reported promptly.**
* **Monitoring of personal data security is conducted.**
* **Security measures are taken for entry and exit to physical environments containing personal data.**
* **Physical environments containing personal data are protected against external risks (such as fire, flood, etc.).**
* **Security of environments where personal data is stored is ensured.**
* **Personal data is minimized as much as possible.**
* **Personal data is backed up, and the security of backups is also ensured.**
* **A user account management and authorization control system is in place and monitored.**
* **Internal periodic and/or random audits are conducted or commissioned.**
* **Log records are kept in a manner that prevents user intervention.**
* **Existing risks and threats are identified.**
* **Protocols and procedures for the protection of special categories of personal data have been established and are enforced.**
* **If special categories of personal data are sent via email, they are encrypted and sent via KEP (Registered Electronic Mail) or a corporate email account.**
* **Secure encryption/cryptographic keys are used for special categories of personal data and managed by separate units.**
* **Intrusion detection and prevention systems are used.**
* **Cybersecurity measures are in place and their implementation is continuously monitored.**
* **Data encryption is performed.**
* **Data processors are audited periodically for data security compliance.**
* **Data processors are provided with awareness training on data security.**

**EXPLANATION ANNEX 1: These measures are the template precautions listed in the data protection registry (VERBIS) to which we are subject. You may delete any of the measures that you have not adopted.**

**6. DATA SUBJECT RIGHTS**

If you are a citizen of a European Union member state, you have the following rights under the General Data Protection Regulation (GDPR): the right to withdraw your explicit consent, to access and obtain information about your personal data, to correct, delete, or restrict the processing of your personal data under certain circumstances, to data portability under specific conditions, and to object to the processing of your personal data.

In addition, you have the following rights under Article 11 of the Turkish Personal Data Protection Law (KVKK):

a) To learn whether your personal data is being processed,
b) To request information if your personal data has been processed,
c) To learn the purpose of processing your personal data and whether they are used in accordance with that purpose,
d) To know the third parties to whom your personal data is transferred, domestically or abroad,
e) To request the correction of personal data if it is incomplete or incorrectly processed,
f) To request the deletion or destruction of personal data within the framework of the conditions outlined in Article 7 of the KVKK,
g) To request notification of the transactions carried out pursuant to subparagraphs (d) and (e) to third parties to whom the personal data has been transferred,
h) To object to a result that is detrimental to you arising from the analysis of processed data exclusively through automated systems,
i) To request compensation for the damage incurred due to the unlawful processing of personal data.

**7. EXERCISING DATA SUBJECT RIGHTS**

You may submit your requests to exercise your data subject rights using the Data Subject Request Form available on our website, or by submitting a written application prepared in accordance with the Communiqué on the Principles and Procedures for the Request to the Data Controller, via one of the methods listed below.

Your application will be processed as soon as possible and no later than thirty (30) days from the date of receipt, free of charge. However, if the process requires an additional cost, the fee schedule determined by the Personal Data Protection Board may be applied.

If your request is denied, if you find the response insufficient, or if you do not receive a response within the legal time frame, you may contact us again. Additionally, you have the right to file a complaint with the relevant data protection authority in your country within 30 days of receiving our response, and in any case, within 60 days of the date on which you submitted your request in due form.

|  |  |
| --- | --- |
| **Application Method** | **Application Adress** |
| E-mail | info@atlantis.com.tr |
| Registered e-mail (KEP) | atlantismuhendislik@hs03.kep.tr |
| Physical mail address | Şerifali Mah. Açıkyüz Sok. No:35 Ümraniye/İSTANBUL |