Information Notice for
Business Partners Shareholder/Employee/Authorized Personnel

Dear Business Partner Shareholder/Employee/Authorized Personnel,

As Usersdot Technology and Consultancy Inc. ("Usersdot" or "Company"), in our capacity as data controller, we hereby inform the Business Partner Shareholder/Employee/Authorized Personnel that we will record, store, maintain, and share, in accordance with the provisions of the Law on the Protection of Personal Data ("KVKK") and as detailed below, the personal data obtained from them, in a limited, proportionate, and accurate manner to ensure the accuracy and currency of personal data, within the framework of the purposes stated below and related to these purposes, and in accordance with the conditions envisaged by the KVKK, with third parties and companies authorized to request personal data by law.

1. DEFINITIONS RELATED TO THE LAW ON THE PROTECTION OF PERSONAL DATA

Data Controller	Data Controller refers to the natural or legal person who determines the purposes and means of processing personal data, and who is responsible for establishing and managing the data recording system.
The Company	The data controller refers to Usersdot Technology and Consultancy Inc.
Data Subject/Concerned Individual	The data subject is the individual whose personal data is being processed.
Data Processor	The natural or legal person who processes personal data on behalf of the data controller, based on the authority granted by the data controller.
Personal Data	It refers to any kind of information relating to an identified or identifiable natural person.
Sensitive Personal Data	It refers to data regarding individuals' race, ethnic origin, political opinions, philosophical beliefs, religion, sect or other beliefs, attire, association, foundation or union membership, health, sexual life, criminal record, and security measures, as well as biometric and genetic data.
Processing of Personal Data	It encompasses all kinds of processes carried out on data, whether fully or partially, by automatic or non-automatic means, including obtaining, recording, storing, preserving, altering, rearranging, disclosing, transferring, taking over, making data accessible, classifying, or preventing the use of data.
KVKK	It refers to the Law on the Protection of Personal Data No. 6698.
Board	It refers to the Personal Data Protection Board.
Authority	It refers to the Personal Data Protection Authority.
Data Registry System	It refers to the record system where personal data is processed in a structured manner according to specific criteria.

Explicit Consent	It expresses consent based on information provided on a specific subject and declared with free will.

2. PROCESSED PERSONAL DATA, DATA PROCESSING PURPOSES, AND LEGAL BASIS

In this context, as Usersdot, your personal data is processed for the purposes and legal reasons detailed below.

2.1. Personal Data Processed and Data Categories Regarding Business Partners, Shareholders, Employees, and Authorized Personnel of Usersdot Technology and Consultancy Inc.

As Usersdot Technology and Consultancy Inc., in our capacity as the Data Controller, the following Identity Data, Communication Data, Operational Security Data, and Physical Space Security Data of Business Partners, Shareholders, Employees, and Authorized Personnel are processed: Identity Data including ***"Name, Signature, Signature Circulars, Surname, TCKN (Turkish Republic Identification Number), Position, Title"; Communication Data including "Address, Company Address Information, Email Address, Phone Number"; Operational Security Data including "User Name, Password, IP Address, Website Log-in/Log-out Information, User Activities"; and Physical Space Security Data including "Camera Recordings".***

2.1.1. Processing of Identity Data

As Usersdot, Identity Data of esteemed Business Partners, Shareholders, Employees, Authorized Personnel such as Name, Signature, Signature Circulars, Surname, TCKN, Position, and Title are processed. The Data Controller company processes these personal data for the following purposes:

- Execution of Communication Activities, Execution of Information Security Processes,
- Execution of Purchase Processes for Goods/Services,
- Execution of Contract Processes,
- Execution of Product/Service Marketing Processes,
- Execution/Denomination of Business Activities,
- Compliance of Activities with Legislation,
- Execution of Financial,
- Accounting Processes,
- Pursuit and Execution of Legal Affairs.

These data are processed in compliance with the conditions specified in Article 5 of Law No. 6698, namely, **"Directly Related to the Establishment or Performance of a Contract, Mandatory for the Legitimate Interests of the Data Controller Provided that it Does not Harm the Fundamental Rights and Freedoms of the Data Subject, Fulfillment of Company's Legal Obligations,"** and they are stored both at the company headquarters and in electronic media.

2.1.2. Processing of Communication Data

As Usersdot, Communication Data of esteemed Business Partners, Shareholders, Employees, and Authorized Personnel such as Address, Company Address Information, Email Address, and Phone Number are processed. The Data Controller company processes these personal data for the following

purposes:

- Execution of Communication Activities,
- Execution of Information Security Processes,
- Execution of Purchase Processes for Goods/Services,
- Execution of Contract Processes,
- Execution of Product/Service Marketing Processes,
- Execution/Denomination of Business Activities,
- Compliance of Activities with Legislation,
- Execution of Financial and Accounting Processes,
- Pursuit and Execution of Legal Affairs.

These data are processed in compliance with the conditions specified in Article 5 of Law No. 6698, namely, **"Directly Related to the Establishment or Performance of a Contract, Mandatory for the Legitimate Interests of the Data Controller Provided that it Does not Harm the Fundamental Rights and Freedoms of the Data Subject,"** and they are stored both at the company headquarters and in electronic media.

2.1.3. Processing of Operational Security Data

As Usersdot, Operational Security Data of esteemed Business Partners, Shareholders, Employees, and Authorized Personnel such as User Name, Password, IP Address, Website Log-in/Log-out Information, and User Activities are processed. The Data Controller company processes these personal data for the following purposes:

- Execution of Communication Activities,
- Execution of Information Security Processes,
- Execution of Purchase Processes for Goods/Services,
- Execution of Contract Processes,
- Compliance of Activities with Legislation,
- Tracking Requests/Complaints,

These data are processed in compliance with the conditions specified in Article 5 of Law No. 6698, namely, **"Directly Related to the Establishment or Performance of a Contract, Mandatory for the Legitimate Interests of the Data Controller Provided that it Does not Harm the Fundamental Rights and Freedoms of the Data Subject, Explicit Consent of the Data Subject (in terms of User Activities)"** and they are stored both at the company headquarters and in electronic media.

2.1.4. Processing of Physical Space Security Data

As Usersdot, Physical Space Security Data of esteemed Business Partners, Shareholders, Employees, and Authorized Personnel such as Camera Recordings are processed. The Data Controller company processes these personal data for the following purposes:

- Ensuring Physical Space Security
- Execution of Information Security Processes

- Ensuring Security of Movable Property and Resources
- Pursuit and Execution of Legal Affairs
- Tracking Requests/Complaints

These data are processed in compliance with the conditions specified in Article 5 of Law No. 6698, namely, **"Mandatory for the Legitimate Interests of the Data Controller Provided that it Does not Harm the Fundamental Rights and Freedoms of the Data Subject"** and they are stored both at the company headquarters and in electronic media.

3. DATA COLLECTION METHOD AND LEGAL BASIS

Your personal data may be collected through various written, verbal, and electronic means, both automated and non-automated, for the purposes stated in the Privacy Notice for Processing of Personal Data. These methods include but are not limited to:

- Information entered and provided during the registration process in the business partners' admin panel.
- Information conveyed during the process of opening current accounts.
- Additional information provided during the completion of membership and contract acquisition processes.
- Data collected through cookies by Google.
- Information obtained from LinkedIn, business cards, and relevant individuals.
- Camera (CCTV) recordings.

4. TRANSFER OF PERSONAL DATA

Your personal data may be transferred, in accordance with Article 8 of the KVKK and other relevant legislation, for the following purposes:

- To authorized public institutions and organizations within the country, based on the legal basis of necessity of data processing for the legitimate interests of the data controller, provided that it does not harm the fundamental rights and freedoms of the data subject, for the purpose of providing information to authorized individuals, institutions, and organizations.
- To Cloud Service Providers abroad, based on your explicit consent, for the purpose of conducting information security processes and ensuring internal information and document management within the company.
- To third-party private organizations within the country, with whom contracts for external services are made, based on the legal basis of necessity of data processing for the legitimate interests of the data controller, provided that it does not harm the fundamental rights and freedoms of the data subject, for the purposes of conducting business activities in compliance with legislation/regulations, conducting legal affairs, and executing financial and accounting processes.

These transfers are limited to the realization of the above-mentioned purposes and the fulfillment of these purposes.

5. STORAGE PERIOD OF PERSONAL DATA

The company will retain your personal data for the duration of the Service Agreement and for 10 years after the termination of the service agreement. For operational security data, in accordance with Law No. 5651 on the Regulation of Internet Publications, the data will be retained for a maximum of 2 years. For transfers abroad, the data will be retained for the duration of explicit consent. Visual and auditory data in the form of camera recordings will be retained for 90 days from the date of processing.

6. MEASURES AND COMMITMENTS REGARDING DATA SECURITY

The company undertakes to take necessary technical and administrative measures to ensure an adequate level of security in order to:

- Prevent the unlawful processing of personal data,
- Prevent unauthorized access to personal data,
- Ensure the confidentiality, integrity, and availability of personal data.

The measures taken by the company include but are not limited to:

Technical Measures:

- Network security and application security are ensured.
- Closed system networks are used for transferring personal data over the network
- Key management is implemented.
- Security measures are taken in the procurement, development, and maintenance of information technology systems.
- Security of personal data stored in the cloud is ensured.
- An authorization matrix is created for employees.
- Access logs are regularly maintained.
- Corporate policies on access, information security, usage, storage, and disposal have been developed and implemented.
- Data masking measures are implemented when necessary.
- Current anti-virus systems are utilized.
- Firewalls are employed.
- Signed contracts include data security provisions.
- Personal data is backed up, and the security of backed-up personal data is ensured.
- Log records are maintained in a manner that prevents user intervention.
- Secure encryption/cryptographic keys are used for sensitive personal data and managed by different units.
- Intrusion detection and prevention systems are used.
- Penetration testing is conducted.
- Cybersecurity measures are implemented and continuously monitored for compliance.
- Encryption is applied.
- Data loss prevention software is used.

Administrative Measures:

- Discipline regulations containing data security provisions are in place for employees.
- Regular training and awareness programs on data security are conducted for employees.
- Privacy commitments are made.
- The permissions of employees undergoing role changes or leaving the company in this field are revoked.
- Policies and procedures for personal data security are established.
- Personal data security issues are promptly reported.
- Monitoring of personal data security is conducted.
- Necessary security measures are taken for access to physical environments containing personal data.
- Security against external risks (fire, flood, etc.) is ensured for physical environments containing personal data.
- Security of environments containing personal data is maintained.
- Personal data is minimized whenever possible.
- Internal periodic and/or random audits are conducted.
- Existing risks and threats are identified.
- Protocols and procedures for the security of special category personal data are established and implemented.
- Data processing service providers undergo regular audits regarding data security.
- Data processing service providers are made aware of data security practices.

7. YOUR RIGHTS UNDER THE LAW

According to Article 11 of the Law, data subjects have the following rights:

- To learn whether personal data is being processed,
- To request information if personal data has been processed,
- To learn the purpose of processing personal data and whether they are used for their intended purpose,
- To know the third parties to whom personal data is transferred domestically or abroad,
- To request correction of personal data if it is incomplete or inaccurate and to request notification of the correction to third parties to whom the personal data has been transferred,
- To request the deletion or destruction of personal data in accordance with the Law No. 6698 and other relevant legislation, despite being processed in compliance with the law, if the reasons requiring processing have ceased, and to request notification of this process to third parties to whom the personal data has been transferred,
- To object to a decision made against them based solely on automated processing of data,
- To demand compensation for damages suffered due to unlawful processing of personal data.

Your requests regarding these rights will be evaluated and concluded within 30 (thirty) days if delivered

in writing to USERSDOT TECHNOLOGY AND CONSULTING INC.'s address "Barbaros Mahallesi Kardelen Sokak Palladium Tower No:2/10 Ataşehir/İstanbul" by hand delivery, post, or cargo, or through a notary, or via secure electronic signature and mobile signature to our electronic mail (KEP) address usersdotteknoloji@hs01.kep.tr or to the company's email address kvkk@usersdot.com. Requests submitted by the data subject must include the following information: name, surname, signature if the application is in writing, TR identity number, nationality if the data subject is a foreigner, passport number or, if any, identity number, and the address of residence or workplace, email address for notification, telephone and fax numbers, and the subject of the request.

You can access and download the request form from the "Personal Data Protection" section on www.usersdot.com