P-GDP-02 Etiya Privacy Policy for Personal Data Subject to GDPR

This Privacy Policy (this "Privacy Policy") only applies to processing of personal data subject to **EU General Data Protection Regulation No 2016/679 (the "GDPR").**

1. OUR PRIVACY POLICY

This Privacy Policy is an explanation by Etiya Bilgi Teknolojileri Yazılım Sanayi ve Ticaret Anonim Şirketi with its affiliates, which is an international software development company, located at 43 Çiftehavuzlar Mah., Eski Londra Asfaltı Caddesi, 151/1BYTÜ Davutpaşa Kampüsü Teknopark B1 Blok No.301, Davutpaşa, Esenler 34220, İstanbul, Turkey ("ETIYA" or "We"/"Us") to persons residing in the European Economic Area (the "EEA") protected under the GDPR (who may include our customers) (the "Data Subject") regarding how we collect and process personal data as the data controller if personal data is provided or disclosed by the Data Subject or if personal data is received or acquired through a third party. We process the personal data in accordance with the GDPR (and other applicable EU and Member State regulations on data protection, if such regulations exist).

Processing of personal data in this Privacy Policy means processing of personal data of persons who are in the EEA in any of the following cases:

- (i) if carried out in connection to activities of our establishment in the EEA,
- (ii) if related to the offering of goods or services to the Data Subjects, or
- (iii) if related to the monitoring of the Data Subject's behavior as far as their behavior takes place within the EEA.

2. COLLECTION AND PROCESSING OF PERSONAL DATA

We will always process the Data Subject's personal data based on the legal bases provided in the GDPR (Articles 6 and 7). In addition, if processing personal data that requires special care, we will do so in accordance with the special rules provided for in the GDPR (Articles 9 and 10).

Principles that dictate the data processing;

ETIYA, when processing your personal data, complies with the principles governing lawful data processing (No. 5 GDPR), namely:

-The principle of legality, objectivity and transparency, according to this particular principle, the data are submitted in a fair and lawful manner in a transparent manner.

-The purpose limitation principle that data is collected for specified, explicit, and legitimate purposes and is not further processed in a manner incompatible with those purposes.

-The principle of proportionality, "minimizing data", according to which the data processed are relevant and necessary for the purposes of processing.

-The principle of data accuracy, according to which the data is accurate and when necessary updated.

-The principle of integrity and confidentiality, according to which the data are processed in a way that guarantees their security and protection against unlawful processing, loss, destruction or deterioration.

-The principle of determining the length of the processing period, "storage period limitation", according to which data must be kept in a format that allows the identification of data subjects only for the time necessary to achieve the purposes of the processing.

-The accountability principle of the controller, according to which the controller is responsible and should be able to demonstrate compliance with the Regulation before the supervisory authorities and the courts.

We may collect and process the Data Subject's personal Data in the following cases :(i) if required in order to provide the Data Subject with adequate services and products and we otherwise have a legitimate interest; (ii) if required in order to perform an agreement with the Data Subject or carry out procedures before execution; or (iii) if we have obtained the Data Subject's express prior consent. In that case, we will give notification of the purpose of that collection and processing to the Data Subject through notification when obtaining consent, agreement, or other appropriate means.

The Data Subject is entitled to withdraw his or her consent to the collection and processing of the personal data at any time, but this withdrawal will not affect the lawfulness of processing based on the consent before withdrawal thereof.

We will process the Data Subject's personal data for the above specified, explicit and legitimate purposes, and will not further process the personal data in a way which is incompatible with those mentioned purposes. If we intend to process personal data originally collected in order to attain other objectives or purposes, we will ensure that the Data Subject is informed of this. We will keep personal data for as long as it is necessary for us to comply with our legal obligations, ensure that we provide an adequate service, and support our business activities (Articles 5 and 25(2) of the GDPR).

We ensure that the personal data processed shall be limited to what is adequate and necessary in relation to the purposes for which they are processed.

Sensitive Data

We do not generally seek to collect sensitive data (also known as special categories) through this site or otherwise. In the limited cases where we do seek to collect such data, we will do this in accordance with data privacy law requirements and/or ask for your consent.

The term "sensitive data" refers to the various categories of personal data identified by data privacy laws as requiring special treatment, including in some circumstances the need to obtain explicit consent from you. These categories include racial or ethnic origin, political opinions, religious, philosophical or other similar beliefs, membership of a trade union, physical or mental health, biometric or genetic data, sexual life or orientation, or criminal convictions and offences (including information about suspected criminal activities).

Below is also a chart describing the categories of personal data we collect:

Additional personal details, contact details and identifiers.	In addition to the personal details listed above, ETIYA may collect additional personal details for recruitment/employment purposes, such as national identification number, social security number,

	insurance information, marital/civil partnership status, domestic partners, dependents, emergency contact information, and military history.
Education information and professional or employment-related information.	ETIYA may collect information about your education and professional or employment-related information, such as your employment history.
Sensitive data for recruitment purposes.	ETIYA may collect certain types of sensitive information when permitted by local law or with your consent, such as health/medical information (including disability status), trade union membership information, religion, race or ethnicity, minority flag, and information on criminal convictions and offences. ETIYA collects this information for specific purposes, such as health/medical information in order to accommodate a disability or illness (subject to legal limits on the timing of collection of such information and other applicable limitations) and to provide benefits; background checks and diversity-related personal information (such as race or ethnicity) in order to comply with legal obligations and internal policies relating to diversity and anti-discrimination.

Documentation required under immigration laws.	ETIYA may collect data on citizenship, passport data, and details of residency or work permit (a physical copy and/or an electronic copy).
Financial information for payroll/benefits purposes	Your banking and other relevant financial details we need for payroll/benefits purposes.
Talent management information.	Information necessary to complete a background check, details on performance decisions and outcomes, performance feedback and warnings, e-learning/training programs, performance and development reviews (including information you provide when asking for/providing feedback, creating priorities, updating your input in relevant tools), driver's license and car ownership information, and information used to populate biographies.
Requested recruitment information	Information requested to provide during the recruitment process, to the extent allowed by applicable law.
Recruitment information you submit	Information that you submit in résumés / CVs, letters, writing samples, or other written materials (including photographs).
Information generated by us during recruitment	Information generated by interviewers and recruiters related to

	you, based on their interactions with you or basic Internet searches where allowed under applicable law.
Recruitment information received from third parties	Information related to you provided by third-party placement firms, recruiters, or job-search websites, where applicable.
Recommendations	Recommendations related information provided on your behalf by others.
Immigration	Documentation and related information required under immigration laws.
Employment history and background checks	Information about your prior employment, education, and where applicable and allowed by applicable law, credit history, criminal records or other information revealed during background screenings.
Diversity related information	Information about race / ethnicity / religion / disability / gender and self-identified LGBT status, for purposes of government reporting where required by law, as well as to understand the diversity characteristics of the ETIYA workforce, subject to legal limits.
Assessment information	Information generated by your participation in psychological, technical or behavioral assessments. You will receive more information

	about the nature of such assessments before your participation in any of them.

Please view the table below for (i) a list of the purposes for which ETIYA uses your personal data and (ii) an overview of the legal basis for each such purpose.

Purpose	Legal basis
Managing our contractual and/or employment relationship with you.	Necessary for the performance of a contract to which you are a party.
Recruitment.	Justified on the basis of our legitimate interests for ensuring that we recruit the appropriate employees.
Facilitating communication with you (including in case of emergencies, and to provide you with requested information).	Justified on the basis of our legitimate interests for ensuring proper communication and emergency handling within the organization.
Operating and managing our business operations.	Justified on the basis of our legitimate interests for ensuring the proper functioning of our business operations.
Complying with legal requirements.	Necessary for the compliance with a legal obligation to which we are subject.
Monitoring your use of our systems (including monitoring the use of our website and any apps and tools you use).	Justified on the basis of our legitimate interests of avoiding non-compliance and protecting our reputation.

Social listening (Identifying and assessing what is being said about ETIYA and our clients on social media (only publicly accessible content) to understand sentiment, intent, mood and market trends and our stakeholders' needs and thereby improving our services. We do this through key-word searches and our goal is to gain insights in conversation trends over a specified period and not to identify an individual. To achieve this, we analyze and monitor conversation streams and monitor publicly available opinions, statements or other interactions on social media channels.)	Justified on the basis of our legitimate interest of protecting our assets and our brand on social media
Improving the security and functioning of our website, networks and information.	Justified on the basis of our legitimate interests for ensuring that you receive an excellent user experience and our networks and information are secure.
Undertaking data analytics, i.e. applying analytics to business operations and data to describe, predict and improve business performance within ETIYA and/or to provide a better user experience.	Justified on the basis of our legitimate interests for ensuring the proper functioning of our business operations.
Marketing our products and services to you	Justified on the basis of our legitimate interests for ensuring that

	we can conduct and increase our business.
Specific Recruitment/Employment Purposes	Legal basis
Assess your suitability for employment for the role for which you are applying, as well as future roles that may become available.	Justified on the basis of ETIYA's legitimate interests of ensuring that it recruits the appropriate employees.
Manage your application.	Justified on the basis of ETIYA's legitimate interests of ensuring that it recruits the appropriate employees.
Facilitate communication with you.	Justified on the basis of ETIYA's legitimate interests of ensuring proper communication within the organization and with you.
Perform administrative functions (e.g. reimburse you for interview-related expenses).	Justified on the basis of ETIYA's legitimate interests of ensuring that it recruits the appropriate employees.
Perform data analytics, including analysis of our applicant pool in order to better understand who is applying to positions at ETIYA and how to attract and keep top talent.	Justified on the basis of ETIYA's legitimate interests of ensuring that it continually improves its recruitment processes.
In some cases, record your online interview for review by additional recruiters and hiring managers.	Justified on the basis of ETIYA's legitimate interests of ensuring that it recruits the appropriate employees.
If you register on our Careers website, we will enter you into a database to receive future mailings about ETIYA positions and events.	Justified on the basis of ETIYA's legitimate interests of ensuring that it recruits the appropriate employees.

You may also receive personalized job recommendations while browsing our Careers website.	
Transfer your contact information, education data, employment data, application information and the CV, all as supplied by you in our recruitment system, to the ETIYA System—a site that we maintain to notify you about new positions that may be of interest to you.	Justified on the basis of ETIYA's legitimate interests of ensuring that it recruits the appropriate employees.
Administration of employee benefits	Justified on the basis of ETIYA's legitimate interests of ensuring that our employees receive the applicable benefits.
Perform any legally required reporting and respond to legal process.	Compliance with a legal obligation.

3. SHARING PERSONAL DATA

We may share personal data with our group entities and with third-parties in accordance with the GDPR. When we share personal data with a data processor, we will put the appropriate legal framework in place in order to cover data transfer and processing (Articles 26, 28 and 29 of the GDPR).

Furthermore, when we share personal data with any entity outside the EEA, we will put appropriate legal frameworks in place, notably controller-to-controller (2004/915/EC) and controller-to-processor (2010/87/EU) Standard Contract Clauses approved by the European Commission, in order to cover such transfers (Chapter 5 of the GDPR).

Collaborative Partners

Subject to the Data Subject's prior consent, personal data may be transferred to, stored, and further processed by collaborative partners that work with us to provide our products and services or help us market to Data Subjects.

Outsourcing

（1）We may outsource all or part of the personal data processing in sales services, enquiry response services, equipment maintenance services, fee related services, marketing services, and other services.

（2）When executing an outsourcing agreement, the eligibility of the counterparty as an outsourcee is sufficiently investigated. Safety management measures, confidentiality, conditions for the outsourcee to outsource to another party, and other matters regarding the appropriate processing of personal data are prescribed in the outsourcing agreement, and our outsourcee are appropriately supervised by implementing periodic monitoring, etc. of the outsourcing conditions.

（3）The personal data provided (deposited) by the outsourcer in the services outsourcing is utilized within the scope necessary to perform the agreement with the outsourcer.

Corporate Affiliates and Corporate Reorganisations

We may share the personal data with all corporate affiliates. In the event of a merger, corporate reorganisation, civil rehabilitation, acquisition, joint venture, assignment, transfer, sale or disposition of all or any portion of our business (including in connection with any bankruptcy or similar proceedings), etc., we may transfer any and all personal data to the relevant third party.

Legal Compliance and Security

It may be necessary for us – by law, legal process, litigation, and/or requests from public and governmental authorities within or outside the Data Subject's country of residence – to disclose personal data. We may also disclose personal data if we determine that, for purposes of national security, law enforcement, or other issues concern of public importance, disclosure is necessary or appropriate.

We may also disclose personal data if we determine in good faith that disclosure is reasonably necessary to protect our rights and pursue available remedies, enforce our internal regulations, investigate fraud, or protect our operations or users.

Data Transfers

Disclosures or sharing of personal data as described above may involve transferring personal data out of the EEA. For each of these transfers we shall make sure that we provide an adequate level of protection to the data transferred, in particular by entering into Standard Contract Clauses as defined by the European Commission decisions 2001/497/EC, 2002/16/EC, 2004/915/EC and 2010/87/EU.

Mobile Information Sharing

No mobile information will be shared or sold with third parties/affiliates for marketing/promotional purposes. All the above categories exclude text messaging originator opt-in data and consent; this information will not be shared with any third parties.

4. OUR RECORDS OF DATA PROCESSES

We handle records of processing of personal data in accordance with the obligations established by the GDPR (Article 30), where we might process personal data. In these records, we reflect all the information necessary in order to comply with the GDPR and cooperate with the supervisory authorities in accordance with the GDPR (Article 31).

5. SECURITY MEASURES

We process personal data in a manner that ensure such data undergoes appropriate security (including protection against unauthorized or unlawful processing and against accidental loss, destruction damage, etc.) using appropriate technical or organizational measures to achieve this (Articles 25(1) and 32 of the GDPR).

We update and test our security technology on an ongoing basis. We restrict access to your personal data to those employees who need to know that information to provide benefits or services to you. In addition, we train our employees about the importance of confidentiality and maintaining the privacy and security of your information.

If any personal data leak occurs we will do everything to eliminate it and to assess a level of risk connected with the leak according to our Personal data breach policy. If it turns out the leak may

lead to physical, material or non-material damage for you (e.g. discrimination, identity theft, fraud or financial loss) we will contact you without undue delay unless the law provides otherwise. All our steps will be taken in full cooperation with competent supervising authority.

6. NOTIFICATION OF DATA BREACHES TO THE COMPETENT SUPERVISORY AUTHORITIES

In case of breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed, we have the mechanisms and policies in place in order to identify it and assess the details of the breach promptly. Depending on the outcome of our assessment, we will make the necessary notifications to the supervisory authorities and communications to the affected data subjects (Articles 33 and 34 of the GDPR).

7. PROCESSING LIKELY TO RESULT IN HIGH RISK TO THE DATA SUBJECT'S RIGHTS AND FREEDOMS

We have mechanisms and policies in place in order to identify data processing activities that may result in high risk to the data subject's rights and freedoms (Article 35 of the GDPR). If any such data processing activity is identified, we will assess it internally and either stop it or ensure that the processing is compliant with the GDPR or that appropriate technical and organizational protective measures are in place in order to proceed with it.

In case of doubt, we will contact the competent Data Protection Supervisory Authority in order to obtain their advice and recommendations (Article 36 of the GDPR).

8. DATA SUBJECT'S RIGHTS

We will notify the Data Subject of the details of the rights granted to the Data Subject under the GDPR when notifying the Data Subject of the purpose of processing personal data.

If the Data Subject will exercise such rights, please contact us at the address set forth section 13 below.

If the Data Subject is not satisfied with the way in which we have proceeded with any request, or if the Data Subject has any complaint regarding the way in which we process personal data, the Data Subject may lodge a complaint with a Data Protection Supervisory Authority.

- Request access to the personal data we process about you: this right entitles you to know whether we hold personal data about you and, if we do, to obtain information on and a copy of that personal data. Download related form.
- Request a rectification of your personal data: this right entitles you to have your personal data be corrected if it is inaccurate or incomplete. Download related form.
- Object to the processing of your personal data: this right entitles you to request that ETIYA no longer processes your personal data. Download related form.
- Request the erasure of your personal data: this right entitles you to request the erasure of your personal data, including where such personal data would no longer be necessary to achieve the purposes. Download related form.
- Request the restriction of the processing of your personal data: this right entitles you to request that ETIYA only processes your personal data in limited circumstances, including with your consent. Download related form.
- Request portability of your personal data: this right entitles you to receive a copy (in a structured, commonly used and machine-readable format) of personal data that you have provided to ETIYA, or request ETIYA to transmit such personal data to another data controller. Download related form.

9. CHILDREN

If we collect and process personal data from a child who is under 16 years of age or who has not reached the age limits under the laws of a Member State, we will process that data appropriately (Article 8 of the GDPR).

10. ABOUT COOKIES

As is true of most other websites, this website collects certain information automatically and stores it in log files. This includes Internet Protocol (IP) addresses, geographic location of your computer or device, browser type, operating system and other information about visiting this website, for example, pages viewed. This information is used to improve this website and, thanks to this constant improvement, to better serve to our users. Your IP address may also be used to diagnose problems with our server, administer this website, analyze trends, track a user's movement on the

site, and collect demographic information to help us understand visitor preferences and their needs. This website also uses cookies and web beacons.

11. PERSONAL DATA RETENTION

We will retain your personal data only for as long as is necessary. We maintain specific records management and retention policies and procedures, so that personal data are deleted after a reasonable time according to the following retention criteria:

We retain your data as long as we have an ongoing relationship with you (in particular, if you have an account with us).

We will only keep the data while your account is active or for as long as needed to provide services to you.

We retain your data for as long as needed in order to comply with our global legal and contractual obligations.

12. UPDATES TO PRIVACY POLICY

We may change this Privacy Policy from time to time. Any changes to this Privacy Policy will become effective upon posting of the revised Privacy Policy via the Website. If we make changes which we believe are significant, we will inform the Data Subject through the Website to the extent possible and seek for the Data Subject's consent where applicable.

This policy was reviewed on November 10, 2023.

13. CONTACT AND DATA PROTECTION OFFICER (DPO)

The Etiya is headquartered in Istanbul, Turkey. The ETIYA has appointed an internal data protection officer for you to contact if you have any questions or concerns about our personal data policies or practices. The email of ETIYA data protection officer is dpo@etiya.com

For any questions or requests relating to this Privacy Policy, please contact us as follows:

E-mail: dpo@etiya.com

Website: Exceed Everyday