

Privacy Policy of FACEPLATE LLP

1. Personal Data Processing

1.1 Customer Data Processing and Ownership

Customer Data shall be used or processed only to provide the Customer with Web Services including purposes compatible with the provision of these services. FACEPLATE shall not use or otherwise process the Customer Data or derive information from it for any advertising or similar commercial purposes. In relations between the parties, the Customer shall retain all rights, ownership and property rights to the Customer Data. FACEPLATE shall not acquire the right to the Customer Data, with the exception of the rights that the Customer grants to FACEPLATE in order to provide Web services for the Customer. This clause shall not affect the rights of FACEPLATE to software or services that FACEPLATE licenses to the Customer.

1.2 Customer Data Disclosure

FACEPLATE shall not disclose the Customer Data outside FACEPLATE, unless with the instructions of the Customer (1) or required by law (2).

FACEPLATE shall not disclose the Customer data to law enforcement authorities, except as required by law. If law enforcement authorities contact FACEPLATE and request to provide the Customer data, FACEPLATE shall attempt to redirect them to request that data directly from the Customer. If FACEPLATE is compelled to disclose the Customer Data to law enforcement authorities, FACEPLATE shall promptly notify the Customer and provide a copy of the request, except where otherwise prohibited by law.

If any other third party requests provision of the Customer Data, FACEPLATE shall immediately notify the Customer of such a request, unless it is legally prohibited. FACEPLATE shall reject the request if its mandatory implementation is not required by law. If the third party's request for data is legal, FACEPLATE shall try to redirect the third party with this request directly to the Customer.

FACEPLATE shall not provide any third party with:

- a. direct, indirect, full or unhindered access to the Customer Data;
- b. platform encryption keys used to protect the Customer Data, or the ability to crack such encryption,
- c. access to the Customer Data, if FACEPLATE is aware that this data is used for purposes other than those specified in the third party request.

In support of the above, FACEPLATE may provide a third party with the Customer's basic contact details.

1.3 Personal Data Processing

The Personal Data provided to FACEPLATE by the Customer or on behalf of the Customer as part of the use of Web services also relates to the Customer Data.

When using the Web Services, the Customer may generate pseudonymizing identifiers that also relate to the Personal Data.

- 1.3.1 To the extent that FACEPLATE is the processor or additional processor of a Personal Data subject under the laws of the Russian Federation, the Conditions in Appendix 1 shall govern the processing of such data.
- 1.3.2 To the extent that FACEPLATE is the processor or additional processor of a Personal Data subject according to the General Data Protection Regulation (GDPR), the GDPR Conditions in Appendix 2 shall govern the processing of such data.
- 1.3.3 In addition, the parties shall agree to the following conditions in this subsection.

1.4 Roles and Responsibilities of the Processor and Controller

The Customer and FACEPLATE agree that the Customer acts as the Controller of the Customer's Personal Data, and FACEPLATE acts as the Processor of this data, unless

- (a) the Customer acts as the Processor of Personal Data, and FACEPLATE is additional processor, or
- (b) mentioned otherwise in the special terms of use of Web Services.

FACEPLATE shall process the Personal Data solely in accordance with the Customer's documented instructions. The Customer agrees that its corporate licensing agreement (including these Terms of Use of Web Services), including use of the Web Services functions and their configuration by the Customer, are complete and final written instructions issued by FACEPLATE for Personal Data processing. Any additional or alternative instructions shall be agreed upon in accordance with the procedure for amending the Customer's corporate licensing agreement.

In any case, when the GDPR is applied and the Customer is the Processor, the Customer guarantees FACEPLATE that instructions of the Customer, including appointment of FACEPLATE as the Processor or the additional Processor, have been authorized by the relevant Data Controller.

1.5 Processing Details

The Parties acknowledge and agree on the following:

The subject of processing is limited to Personal Data under the GDPR.

The processing duration shall correspond to the duration of the Customer's right to use the Web Service; Processing lasts until the Personal Data is deleted or returned in accordance with the instructions of the Customer or the Terms of Use of Web Services.

The nature and purpose of processing shall be considered in the provisions of Web Services in accordance with the Customer's corporate licensing agreement. The types of Personal Data processed by Web Services include those explicitly specified in Article 4 of the GDPR.

Categories of data subjects: the Customer's representatives and end users, such as workers, contractors, employees, and customers.

1.6 Rights of Data Subjects and Assistance with Requests

FACEPLATE shall provide the Customer with access to the Personal Data of data subjects and the possibility to execute requests of data subjects in order to exercise the Customer's rights according to the GDPR. Access shall be provided according to Web Service functionality and FACEPLATE role as Data Processor. FACEPLATE shall execute the Customer's reasonable requests for assistance to the Customer to respond to such requests of data subjects. If FACEPLATE receives a request from the Customer's data subject, which is related to the exercise of one or more of its rights provided for in the GDPR, in connection with the Web service in which FACEPLATE is a processor or additional data processor, FACEPLATE shall redirect this data subject directly to the Customer. FACEPLATE shall execute the Customer's reasonable requests for assistance to the Customer to respond to such requests of data subjects.

1.7 Registration of Processing Operations

FACEPLATE shall maintain all records required by Article 30 (2) of the GDPR and, within the limits applicable to Personal Data processing of on behalf of the Customer, provide them to the Customer upon request.

2. Data Transfer and Location

2.1 Data Transfer

Except for the Terms of Use of Web Services described in other parts, the Customer Data and Personal Data which FACEPLATE processes on behalf of the Customer shall be stored and processed in the territory indicated when registering the account in the Web service.

2.2 Data Storage and Deletion

Throughout the term of the Customer's subscription, the Customer shall be able to retrieve, delete and access the Customer Data stored in each Web Service.

FACEPLATE shall store Customer Data stored on Web Service resources, on restricted account for 90 days from the expiration or early termination of the Customer's subscription so that the Customer can retrieve this data. Upon expiration of the 90-day storage period, FACEPLATE shall deactivate the Customer's account and delete the Customer Data and Personal Data within 90 days if the applicable law or agreement does not permit FACEPLATE to store such data or does not require FACEPLATE to do so.

The Web Service may not support software designed to store or retrieve data provided by the Customer. FACEPLATE shall not responsible for deletion of the Customer Data or Personal Data as described in this section.

2.3 Processor Confidentiality Obligations

FACEPLATE shall ensure that its personnel involved in the processing of the Customer Data and Personal Data fulfill the following conditions: (i) the processing of such data only in accordance with the instructions of the Customer; (ii) an obligation to ensure the confidentiality and security of such data even after the end of participation in its processing.

2.4 Notification of the Involvement of Additional Processor, and Controls

FACEPLATE may use the services of third parties to provide some limited or auxiliary services on its own behalf. The Customer agrees with the involvement of these third parties and affiliates of FACEPLATE as additional processors. The permissions listed above constitute the prior written consent of the Customer to engage a subcontractor of FACEPLATE in the processing of the Customer Data and Personal Data, if such consent is necessary under the Standard Terms of the Contract or the Terms of GDPR .

FACEPLATE shall be responsible for its additional Processors' compliance with the obligations of FACEPLATE set forth in the Terms of Use of Web Services. FACEPLATE shall provide information on additional Processors on the website of FACEPLATE. When interacting with any additional Processor, FACEPLATE, by concluding a written contract, guarantees that the additional Processor can access the Customer Data or Personal Data and use them solely to provide the services for the provision of which FACEPLATE has involved them, and that the additional Processor is prohibited to use the Customer Data or Personal Data for any other purposes. FACEPLATE shall ensure that additional Processors draw up written agreements that oblige them to provide a data protection level not lower than the level required from FACEPLATE in accordance with these Terms.

From time to time, FACEPLATE may involve new additional Processors. FACEPLATE shall notify the Customer (by updating the website and providing the Customer with a notification of such an update) of any new additional Processors at least 14 days before providing such additional Processors with an access to the Customer Data and Personal Data. As for the Basic Web Services, FACEPLATE shall notify the Customer (by updating the website and providing the Customer with an algorithm for receiving notification of such an update) of any new additional Processors at least 6 months before providing such additional Processor with an access to the Customer Data.

If the Customer does not approve a new additional Processor, then the Customer may terminate any subscription of the corresponding Web Service without charge of a penalty by providing a written notice of termination before the end of the notification period indicating the grounds for refusal. If the linked Web Service is a part of a set (or a similar one-time purchase of services), then any

termination shall apply to the entire set. Upon termination, FACEPLATE shall remove the obligation to pay for all subscriptions to Web Services the validity of which has been terminated from all subsequent invoices issued to the Customer or its reseller.

3. Data Security

3.1. Security Practices and Policies

FACEPLATE shall take all necessary technical and organizational measures to protect the Customer Data and Personal Data. These measures are outlined in the FACEPLATE Privacy Policy. FACEPLATE provides the Customer with an access to such policy as well as descriptions of the security controls implemented for Web Services and other information about FACEPLATE security practices and policies reasonably requested by the Customer.

3.2. Customer's Duties

The Customer shall be solely responsible for independently determining whether the technical and organizational measures in relation to the Web Service comply with Customer's requirements, including any security obligations under the GDPR or other applicable data protection laws and regulations. The Customer acknowledges and agrees that (taking into account the state-of-the-art , the cost of implementation, the nature, scope, context and purpose of the Personal Data processing, as well as the associated risks for individuals) the security practices and policies implemented by FACEPLATE provide an adequate level of security and risk protection with respect to the Customer's Personal Data. The Customer shall be responsible for the implementation and observance of privacy and security measures regarding the components that the Customer provides or controls.

3.3. Information Security Breach Notification

If FACEPLATE becomes aware of any security breach resulted in accidental or unlawful destruction, loss, alteration, unauthorized disclosure of the Customer Data or Personal Data, or access to them during processing by FACEPLATE (in each case - "Information Security Breach"), FACEPLATE shall immediately (1) notify the Customer of an Information Security Breach; (2) investigate the Information Security Breach and provide the Customer with detailed information about this Information Security Breach and (3) take reasonable measures to mitigate the consequences and minimize any damage resulting from the Information Security Breach.

Information Security Breach Notification (Notifications), if any, shall be sent to one or more of the Customer's administrators by any mean chosen by

FACEPLATE, including e-mail. The Customer shall bear ultimate responsibility for exact contact details indicated by the Customer's administrators on each respective Web Services portal. The Customer shall bear ultimate responsibility for fulfilling its legal obligations to notify the Customer of any security breaches, and for fulfilling any obligations to notify third parties of any Information Security Breach.

The Customer shall immediately notify FACEPLATE of the possible illegal use of accounts or credentials for authentication, as well as any data breach associated with the Web service.

Appendix 1. Personal Data Processing Policy in the Russian Federation

1. General

1.1. This document defines the personal data processing policy of FACEPLATE (hereinafter referred to as the Company) and sets out the system of basic principles applicable to personal data processing in the Company.

1.2. This Policy applies to all operations performed in the Company in relation to personal data with or without automation tools.

1.3. This Policy is binding on all persons admitted to personal data processing in the Company and persons involved in the organization of processes of personal data processing and security in the Company.

1.4. This Policy is drawn up in accordance with Council of Europe Convention on Personal Protection in Connection with Automatic Processing of Personal Data No. 108 and Federal Law on Personal Data No. 152-FZ dated 27 July 2006 of the Russian Federation

1.5. This Policy shall be updated in case of changes to the personal data laws of the Russian Federation.

2. Introduction

2.1. The Company is a personal data operator.

2.2. An important condition for realization of the objectives of the Company's activity is protection of rights and freedoms of the personal data subject during processing of his personal data.

2.3. The Company has developed and implemented documents establishing the procedure for processing and ensuring the security of personal data, which ensure compliance with the requirements of Federal Law on Personal Data No. 152-FZ dated 27 July 2006 of the Russian Federation and the regulatory legal acts adopted in accordance with it.

3. Principles and conditions for personal data processing in the Company

3.1. The Company, as an operator, processes the following personal data:

3.1.1. applicants for filling vacant posts - in the composition and within the time necessary for the Company to make a decision on accepting or refusing to accept work, with the consent of the personal data subjects, as well as for the formation of a personnel reserve with the consent of the personal data subjects

3.1.2. employees who are or were in labor relations with the Company - in the composition and within the time necessary to achieve the goals stipulated by the legislation of the Russian Federation, to carry out and fulfill the functions, powers and duties assigned to the Company by the legislation of the Russian Federation, to form a personnel reserve with the consent of the subjects of personal data, as well as for the conclusion and execution of an agreement to which either the beneficiary or guarantor is a personal data subject, including for the purpose of providing insurance with the consent of the personal data subjects;

3.1.3. representatives of potential and existing customers - in the composition and within the time necessary for interaction with potential and existing customers, with the consent of the personal data subjects;

3.1.4. partners' representatives - in the composition and within the time necessary for interaction with partners, with the consent of the personal data subjects;

3.2. The terms for processing personal data are determined taking into account:

3.2.1. the established purposes of personal data processing;

3.2.2. the duration of contracts with the subjects of personal data and the consent of the subjects of personal data on the processing of their personal data;

3.3. The Company carries out the processing of personal data in a legal and fair manner.

3.4. When processing personal data, their accuracy, adequacy, and, if necessary, their relevance to the purposes of personal data processing are ensured.

3.5. The Company does not disclose personal data to third parties and does not distribute it without the consent of the subject of personal data (unless otherwise provided for by the Federal Law of the Russian Federation).

3.6. The Company does not process biometric personal data.

3.7. The Company provides cross-border transfer of personal data. In this case, the Company complies with the requirements for cross-border transfer of personal data provided for by Federal Law on Personal Data No. 152-FZ dated 27 July 2006 of the Russian Federation.

3.8. The Company does not make decisions resulted in legal consequences for the subject of personal data or otherwise affecting his rights and legitimate interests, based on exclusively automated processing of personal data.

3.9. The Company entrusts the processing of personal data to another person. In this case, the Company complies with the requirements for a personal data processing order provided for by Federal Law on Personal Data No. 152-FZ dated 27 July 2006 of the Russian Federation.

3.10. The Company processes personal data with or without automation tools. In this case, the Company fulfills the requirements for automated and non-automated processing of personal data provided for by Federal Law on Personal Data No. 152-FZ dated 27 July 2006 of the Russian Federation and regulatory legal acts adopted in accordance with it.

4. Rights of subjects of personal data processed in the Company

4.1. The subject of personal data has the right to receive information regarding the processing of his personal data. To obtain this information, the personal data subject can send a written request (the request can also be sent in the form of an electronic document and signed by electronic signature) to the address: 348a, Raymbek ave., Almaty, Kazakhstan, in the manner prescribed by Article 14 of Federal Law on Personal Data No. 152-FZ dated 27 July 2006 of the Russian Federation.

5. Fulfillment of operator duties by the Company

5.1. The Company receives personal data from subjects of personal data and from third parties (persons who are not subjects of personal data). At that, the Company fulfills the obligations stipulated by Federal Law on Personal Data No. 152-FZ dated 27 July 2006 of the Russian Federation and the Labor Code of the Russian Federation when collecting personal data.

5.2. The Company stops processing personal data in the following cases:

5.2.1. upon the occurrence of conditions for the termination of the processing of personal data or after the expiration of the established deadlines;

5.2.2. upon achieving the purposes of their processing or in case of loss of the need to achieve these purposes;

5.2.3. at the request of the personal data subject, if the personal data processed by the Company are incomplete, outdated, inaccurate, illegally obtained or are not necessary for the stated processing purpose;

5.2.4. in case of unlawful processing of personal data, if it is impossible to ensure the legitimacy of the processing of personal data;

5.2.5. in case of withdrawal by the subject of personal data of consent to the processing of his personal data or the expiration of such consent (if personal data is processed by the Company solely on the basis of the consent of the subject of personal data);

5.2.6. in case of liquidation of the Company.

5.3. The Company has taken the following measures to ensure fulfillment of obligations stipulated by Federal Law on Personal Data No. 152-FZ dated 27 July 2006 of the Russian Federation and the regulatory legal acts adopted in accordance with it:

5.3.1. The person responsible for organizing the processing of personal data has been appointed;

5.3.2. The local acts on the processing and ensuring the security of personal data, as well as local acts establishing procedures aimed at preventing and detecting breach of the legislation of the Russian Federation, eliminating the consequences of such breach, have been issued:

5.3.2.1. Personal Data Processing Regulation;

5.3.2.2. This Policy;

5.3.2.3. Other local acts on the processing and ensuring the security of personal data;

5.3.3. Legal, organizational and technical measures have been applied to ensure the security of personal data;

5.3.4. The internal control of compliance of personal data processing with the requirements of Federal Law On Personal Data No. 152-FZ dated 27 July 2006 of the Russian Federation and regulatory legal acts adopted in accordance with it, this Policy, local acts of the Company has been carried out;

5.3.5. The damage that may be caused to personal data subjects in case of breach of the requirements of federal legislation on personal data has been assessed, this damage and the measures taken by the Company aimed at ensuring the fulfillment of obligations stipulated by the requirements of Federal Law on Personal Data No. 152-FZ dated 27 July 2006 of the Russian Federation and regulatory legal acts adopted in accordance with it have been correlated;

5.3.6. The Company employees who directly process personal data have been familiarized with the provisions of Federal Law on Personal Data No. 152-FZ dated 27 July 2006 of the Russian Federation and the regulatory legal acts adopted in accordance with it, this Policy and local acts of the Company on personal data processing.

5.4. The Company implements the following requirements for the protection of personal data:

5.4.1. A security regime has been established for the premises in which information systems are located that impede the possibility of uncontrolled entry or stay in these premises of persons who do not have access to these premises;

5.4.2. The safety of personal data storage media has been ensured;

5.4.3. The Head of the Company has approved a document defining a list of persons whose access to personal data processed in the information system is required to perform official (labor) duties by them;

5.4.4. The information protection means that have passed the procedure for assessing compliance with the requirements of the information security laws of the Russian Federation have been used;

5.4.5. The requirements established by Decree No. 687 on Approval of Regulation for Peculiarities of Non-Automated Personal Data Processing dated 15 September 2008 of the Russian Federation Government have been implemented;

FACEPLATE assumes the obligations set forth in these Terms of the GDPR to all its customers. FACEPLATE shall fulfill these obligations to the Customer regardless of (1) the version of the Terms of Use of Web Services, which would otherwise apply to any specified subscription to Web Services, and (2) any other agreement containing a reference to this Appendix.

In order to comply with these Terms of the GDPR, the Customer and FACEPLATE agree that the Customer acts as the Controller of Personal Data, and FACEPLATE acts as the Processor of this data, unless the Customer acts as the processor of Personal Data, and FACEPLATE, respectively, as an additional processor. These Terms of the GDPR are applied by FACEPLATE in the interests of the Customer to the processing of Personal Data within the scope of the GDPR. These Terms of the GDPR do not limit or reduce any obligations regarding data protection

undertaken by FACEPLATE to the Customer under the Terms of Use of Web Services or other agreement between FACEPLATE and the Customer. These Terms of GDPR do not apply if FACEPLATE is the Controller of Personal Data.

Applicable obligations under Articles 28,32 and 33 of the General Data Protection Regulation (GDPR)

1. FACEPLATE shall not engage another processor without prior specific or general written approval of the Customer. In case of general written approval, FACEPLATE shall inform the Customer of any intended changes concerning addition or replacement of other processors, thus giving the Customer the opportunity to object to such changes. (Article 28 (2))

2. Processing performed by FACEPLATE is governed by these Terms of the GDPR in accordance with the laws of the European Union (hereinafter referred to as the EU) or a Member State of the EU, and FACEPLATE shall comply with them in relation to the Customer. The subject and duration of the processing, the nature and purpose of the processing, the type of Personal Data, the categories of data subjects, as well as the obligations and rights of the Customer are set forth in the Customer's licensing agreement, including these Terms of the GDPR. In particular, FACEPLATE undertakes to:

(a) Process Personal Data only in accordance with the documented instructions of the Customer, including instructions for transfer of personal data to any third country or international organisation, unless otherwise required by the laws of the EU or a Member State of the EU applicable to FACEPLATE; in such cases, FACEPLATE undertakes to inform the Customer of the relevant legal requirements before processing, unless the law prohibits the provision of such information on the basis of important public interest;

(b) Ensure that persons authorised to process the personal data have undertaken to ensure confidentiality, and ensure that the obligation of confidentiality established by law is properly documented;

(c) Take all measures required pursuant to Article 32;

(d) Comply with the conditions referred to in paragraphs 2 and 4 in case of involvement of another processor;

(e) Taking into account the nature of the processing, assist the Customer with appropriate technical and organisational measures to the extent possible, to ensure the Customer's fulfilment of obligation to respond to requests for exercising the data subject's rights set out in Chapter III of the GDPR;

(f) assist the Customer in ensuring compliance with the obligations pursuant to Articles 32 -36 of the GDPR, taking into account the nature of processing and the information available to FACEPLATE;

(g) at the request of the Customer, delete or return all Personal Data to the Customer upon provision of processing services, and delete existing copies if the laws of the EU or a Member State of the EU does not provide for the storage of Personal Data;

(h) Provide the Customer with access to all information necessary to demonstrate fulfillment of the obligations under Article 28 of the GDPR , as well as allow for and contribute to audits, including inspections, conducted by the Customer or another auditor authorized by the Customer.

FACEPLATE undertakes to inform the Customer immediately, if, in its opinion, any instruction contradicts the requirements of the GDPR or other data protection provisions of the laws of the EU or a Member State of the EU. (Article 28 (3))

3. If FACEPLATE engages other processors to perform specific processing operations in the interests of the Customer, the corresponding other processor shall be subject to the same data protection obligations set forth in these Terms of the GDPR by entering into an agreement or drawing up another legal act in accordance with the laws of the EU or a Member State of the EU, in particular providing sufficient guarantees for the adoption of appropriate technical and organizational measures in such a way to ensure compliance of processing with the GDPR. If corresponding other processor fails to fulfil its data protection obligations, FACEPLATE shall bear full responsibility to the Customer for the performance of that other processor's obligations. (Article 28 (4))

4. Taking into account the state-of-the-art, the costs of implementation, the nature, scope, context and purposes of processing as well as the risk of varying probability and severity for the rights and freedoms of individuals, the Customer and FACEPLATE shall take appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including but not limited to:

- (a) Pseudonymisation and encryption of Personal Data;
- (b) Ability to ensure ongoing confidentiality, integrity, availability and fault tolerance of data processing systems and services;
- (c) Ability to ensure timely recovery of Personal Data and access to them in case of a physical or technical incident;
- (d) A process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of data processing. (Article 32 (1))

5. In assessing the appropriate level of security, the risks posed by processing shall be taken into account. In particular, the risks associated with accidental or unlawful destruction, loss, alteration, unauthorized disclosure of Personal Data, or access to Personal Data being transferred, stored or otherwise processed. (Article 32 (2))

6. The Customer and FACEPLATE shall take measures to ensure that each individual acting on behalf of the Customer or FACEPLATE who obtains an access to Personal Data processes them only in accordance with the instructions of the Customer, unless otherwise required from this person under the law of the EU or a Member State of the EU. (Article 32 (4))

7. FACPLATE shall notify the Customer without undue delay, if it becomes aware of any breach of personal data security. (Article 33 (2)). Such notice shall include information that the processor is to provide to the controller in accordance with Article 33 (3) to the extent that this information is available to FACEPLATE.