POLICY OF PERSONAL DATA PROCESSING (TRANSPARENCY POLICY)

(Legal status as of May 25, 2018).

Key information in brief

- **Whose personal data we process and for what purpose?**
  In connection with our business activity, we collect and process personal data of our customers, contracting parties and business partners. As the Controller, we provide data security and confidentiality, as well as access to the data by persons to whom the information pertains. The collection and processing of data takes place only in accordance with the relevant regulations, in particular with the **EU GDPR** and the data processing regulations provided for in it. Detailed information about the purposes for which we collect and process personal data can be found further on in this document.
- **Do we protect personal data we process and how?**
  As a financial organisation we pay special attention to the security of our customers and all the data entrusted to us. We have implemented special procedures allowing access to personal data only to authorised persons and only to the extent that it is necessary due to the tasks performed by them. In addition, we use organisational and technical solutions to ensure that all operations on personal data are registered and made only by authorised persons. We also ensure that the entities cooperating with us guarantee the use of appropriate security measures for the personal data being processed.
- **Does this Policy comply with the regulations resulting from the EU GDPR?**
  Yes. This document fully takes into account the requirements imposed by the GDPR on entities processing personal data.
- **What is EU GDPR and what goals does is serve?**
  EU GDPR is the abbreviation of: The General Data Protection Regulation - Regulation (EU) 2016/679 of The European Parliament and of The Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and the repealing of Directive 95/46/EC. The goal of introducing the EU GDPR is primarily to increase the protection of personal data and to harmonise the rules for their processing by natural persons, businesses or organisations throughout the EU.
- **What does eService have to do with EU GDPR?**
  In the light of the applicable regulations, eService Sp. z o.o. is the **Controller** of the personal data entrusted to us. We are responsible for safe processing and storage, in accordance with the concluded agreements, consents and applicable regulations.
- **Is it necessary to contact eService with regard to EU GDPR?**
  There is no such need. It is sufficient to read the following document. It contains detailed information about our responsibilities and the ways in which we comply with them. You will also find information about the rights you are entitled to and the means of using them in eService Sp. z o.o.

DETAILED INFORMATION

Basic definitions

- Controller - Centrum Elektronicznych Usług Płatniczych eService Sp. z o. o. with its registered office in Warsaw (01-102) at ul. Jana Olbrachta 94.
- Personal data - any information relating to a natural person identified or identifiable by one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person, including image, voice recording, contact details, location data, information contained in correspondence, information collected via recording equipment or other similar technologies.
- Policy - this Policy for processing personal data.
- Data subject - every natural person whose personal data are processed by the Controller, for example a person visiting the Controller's premises or sending an e-mail inquiry.

Data processing by the Controller

1. In connection with the conducted business, the Controller collects and processes personal data in accordance with the relevant regulations, in particular with the EU GDPR, and the data processing rules provided for in them.
2. The Controller ensures transparency of data processing, in particular, by always informing the data subject about the processing of data at the time of collection, also informing about the purpose and legal basis of the processing - e.g. when concluding a contract for the sale of goods or services. The Controller makes sure that the data are collected only to the extent necessary for the indicated purpose and processed only for as long as it is necessary.
3. When processing data, the Controller ensures their security and confidentiality, as well as access to information on the processing to data subjects. If, despite the security measures applied, a personal data breach occurs (e.g. data 'leak' or loss), the Controller shall inform the persons to whom the data pertain of such an event in a manner consistent with the regulations.

Security of personal data

1. In order to ensure the integrity and confidentiality of data, the Controller has implemented procedures that allow access to personal data only to authorised persons and only to the extent that it is necessary due to the tasks performed by them. The Controller uses organisational and technical solutions to ensure that all operations on personal data are registered and made only by authorised persons.
2. In addition, the Controller undertakes all necessary actions to ensure that its subcontractors and other cooperating entities guarantee appropriate security measures whenever they process personal data on behalf of the Controller.
3. The Controller conducts an on-going risk analysis and monitors the adequacy of data security measures applied to the identified threats. If necessary, the Controller implements additional measures to increase data security.

Goals and legal grounds for processing

1. E-mail and traditional correspondence

a. In the event of correspondence sent to the Controller by e-mail or by regular mail, which is not related to the services provided to the sender or another contract concluded with him, personal data contained in this correspondence shall be processed solely for the purpose of communication and resolution of the matter addressed in the correspondence.

b. The legal basis of the processing is the legitimate interest of the Controller (Article 6.1.f of the EU GDPR) consisting in conducting correspondence addressed to the Controller in connection with his business activities.

c. The Controller processes only personal data relevant to the case to which the correspondence relates. All correspondence is stored in a manner ensuring the security of personal data (and other information) contained in it and is disclosed to authorised persons only.

2. Telephone contact

a. In the event of contacting the Controller by phone, in matters not related to the contract or services provided, the Controller may request personal data only if it is necessary to handle the matter to which the contact relates. The legal basis of the processing is the legitimate interest of the Controller (Article 6.1.f of the EU GDPR) concerning the necessity to resolve the matter related to his business activity.

b. Telephone calls can also be recorded - in this case, appropriate information is provided at the beginning of the conversation. Calls are recorded in order to monitor the quality of the service provided and to verify the work of consultants, as well as for statistical purposes. The recordings are available only to the employees of the Controller and persons servicing the Controller's hotline.

c. Personal data in the form of a call recording are processed:

- for the purposes related to customer and client service via the hotline if the Controller provides such a service - the legal basis for data processing is the necessity of processing in order to provide a service (Article 6.1.b of the EU GDPR);
- in order to monitor the quality of service and verify consultants operating the hotline, as well as for analytical and statistical purposes - the legal basis for processing is the legitimate interest of the Controller (Article 6.1.f of the EU GDPR) aimed at ensuring the highest quality of customer and client service, as well as the work of consultants and statistical analysis of telephone communication.

3. Video monitoring and access control

a. In order to ensure the safety of persons and property, the Controller uses video monitoring and controls access to premises and the area he manages. Data collected in this manner shall not be used for any other purposes.

b. Personal data in the form of recordings from monitoring and data collected in the register of entries and exits are processed in order to ensure security and order on the premises and possibly to defend against claims or for the purpose of pursuing them. The basis of the

processing is the legitimate interest of the Controller (Article 6.1.f of the EU GDPR) concerning the ensuring of the security of the Controller's property and protection of his rights.

4. Recruitment

a. As part of recruitment processes, the Controller expects the provision of personal data (e.g. in a CV or cover letter) only to the extent specified in the labour law. Therefore, information beyond that should not be provided. In the event that the submitted applications contain additional data, they will not be used or taken into consideration in the recruitment process.

b. Personal data are processed:

- in order to comply with legal obligations related to the employment process, including in particular the Labour Code - the legal basis for processing is the legal obligation of the Controller (Article 6.1.c of the EU GDPR in relation to the provisions of the Labour Code);
- in order to conduct the recruitment process within the scope of data not required by law, as well as for the purposes of future recruitment processes - the legal basis for processing is consent (Article 6.1.a of the EU GDPR);
- in order to establish or assert any claims, or to defend against such claims in which case the legal basis of the processing is the legitimate interest of the Controller (Article 6.1.f of the EU GDPR).

5. Collection of data in connection with the provision of services or the performance of other contracts

In the event of data collection for purposes related to the performance of the contract, the Controller provides the data subject with detailed information regarding the processing of his personal data at the time of conclusion of the contract.

6. Collecting data in other cases

a. In connection with the conducted business activity, the Controller also collects personal data in other cases - e.g. during business meetings, at industry events or through the exchange of business cards - for purposes related to the initiation and maintenance of business contacts. The legal basis of the processing is the legitimate interest of the Controller (Article 6.1.f of the EU GDPR) concerning the creation of a network of contacts in connection with the conducted business activity.

b. Personal data collected in such cases are processed only for the purpose for which they were collected and the Controller ensures their adequate protection.

Data transfer and their recipients

1. Data transfer outside the EEA

a. The level of protection of personal data outside the European Economic Area (EEA) differs from that provided by European law. For this reason, the Controller shall transfer personal data outside the EEA only when it is necessary and with an adequate level of protection, primarily through:

- cooperation with personal data processing entities in countries for which an appropriate decision of the European Commission has been issued;
- the use of standard contractual clauses adopted by the European Commission;
- the use of binding corporate rules adopted by the supervisory authority;
- in the event of data transfer to the USA - cooperation with entities participating in the Privacy Shield programme, approved by the European Commission decision.

b. The Controller shall always inform the data subject about the intention to transfer personal data outside the EEA at the stage of data collection.

2. Recipients of data

a. In connection with conducting business that requires processing, personal data are disclosed to third parties, including in particular suppliers responsible for the operation of IT systems and equipment (e.g. CCTV equipment), entities providing legal or accounting services, couriers, marketing agencies or recruitment agencies. The data are also disclosed to entities affiliated with the Controller, including companies from its corporate group. More information on the Controller's corporate group can be found at: www.eservice.pl/o-nas/udzialowcy.

b. The Controller reserves the right to disclose selected information about the data subject to the competent authorities or third parties who submit a request for such information, based on an appropriate legal basis and in accordance with the applicable law.

Period of personal data processing

1. The period of data processing by the Controller depends on the type of service provided and the purpose of the processing. The period of data processing can also result from the regulations when they form the basis for processing. In the case of data processing based on the legitimate interest of the Controller - for example for security reasons - the data are processed for a period of time enabling this interest to be realised or until effective opposition to data processing has been submitted. If processing is based on consent, the data are processed until such consent is withdrawn. When the processing basis is the necessity to enter into and perform the contract, the data are processed until it is terminated.
2. The processing period may be extended should the processing of personal data be necessary to establish or assert claims or to defend against such claims, after which time it is only possible in the case of and to the extent required by law. After the end of the processing period, the data are irreversibly deleted or anonymised.

Rights related to the processing of personal data

Your rights

Data subjects have the following rights:

1. the right to information about the processing of personal data - on this basis, the Controller provides the person making the request with information about data processing, primarily including the purposes and legal grounds for processing, the scope of data in the Controller's possession, entities to which the data are disclosed and the planned date of deletion;

2. the right to obtain a copy of the data - on this basis, the Controller provides a copy of the data processed concerning the person making the request;
3. the right to rectification - the Controller is obliged to remove any incompatibilities or errors of personal data being processed and to supplement them if incomplete;
4. the right to erasure - on this basis, you can request the erasure of data, the processing of which is no longer necessary to pursue any of the goals for which they were collected;
5. the right to restriction of processing - in the event of such a request, the Controller ceases to perform operations on personal data - except for operations agreed to by the data subject - and to store them, in accordance with accepted retention rules or until the reasons for restricting data processing have ceased to exist (e.g. a decision of the supervisory body will be issued allowing further processing of data);
6. the right to data portability - on this basis - to the extent that the data are processed in relation to the concluded agreement or expressed consent - the Controller shall issue data provided by the data subject in a format that facilitates their reading on computer. It is also possible to request that data be sent to another entity - provided, however, that there are technical possibilities in this regard both on the part of the Controller and the other entity;
7. the right to object to processing of personal data for marketing purposes - the data subject may at any time object to the processing of personal data for marketing purposes, without the need to justify such objection;
8. the right to object to other purposes of data processing - the data subject may at any time object to the processing of personal data resulting from the legitimate interest of the Controller (e.g. for analytical or statistical purposes or for reasons related to the protection of property); such objection should contain justification;
9. the right to withdraw consent - if the data are processed based upon consent, the data subject has the right to withdraw it at any time, but withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal.
10. the right to lodge a complaint - if it is decided that the processing of personal data violates the provisions of the GDPR or other provisions on the protection of personal data, the data subject may lodge a complaint to the President of the Office of Personal Data Protection.

Submitting requests related to exercising rights

1. A request to exercise the rights of data subjects can be submitted:
   a. by regular mail at the following address: Centrum Elektronicznych Usług Płatniczych eService Sp. z o. o. with its registered office in Warsaw (01-102) at ul. Jana Olbrachta 94;
   b. by e-mail at: gdpr@eservice.com.pl.
2. Should the Controller be unable to identify the applicant on the basis of the submitted application, he will ask the applicant for additional information.
3. The application may be submitted in person or through a proxy (e.g. a family member). For reasons of data security, the Controller encourages the use of a power of attorney in the form certified by a notary public or an authorised legal advisor or attorney, which will significantly speed up verification of the authenticity of the application.

4. A response should be given within one month of its receipt. If this deadline needs to be extended, the Controller shall inform the applicant of the reasons for the delay.
5. The response is provided via regular mail, unless the application was submitted by e-mail or a response was requested in electronic form.

Rules for collecting fees

1. Proceedings regarding the applications submitted are free of charge. Fees can only be charged:
   a. In the case when the data subject requests a second or subsequent copy of the data (the first copy of the data is free of charge); in this case, the Controller is entitled to charge a fee covering the costs of preparation, handling and sending of the requested information. The abovementioned fee includes administrative costs related to the processing of the request.
   b. in the case of reporting excessive demands by the same person (e.g. extremely frequent) or clearly unjustified; in this case, the Controller is entitled to charge a fee covering the costs of preparation, handling and sending of the requested information.

      The abovementioned fee includes the costs of communication and the costs associated with taking the required actions.
2. If the decision to impose the charge is challenged, the data subject may file a complaint to the President of the Office for Personal Data Protection.

Contact with the Controller

1. The Controller can be contacted by e-mail at gdpr@eservice.com.pl or by regular mail at the following address: Centrum Elektronicznych Usług Płatniczych Spółka z ograniczoną odpowiedzialnością, 01-102 Warszawa, ul. Jana Olbrachta 94.
2. The Controller has appointed a Data Protection Officer who can be contacted by e-mail at iod@eservice.com.pl on any matter regarding personal data processing.

Changes to the Personal Data Processing Policy

The policy is verified on a regular basis and updated if necessary. The current version of the Policy was adopted on May 24, 2018.