

**MARUTA **

**PERSONAL DATA PROCESSING POLICY
(TRANSPARENCY POLICY)**

PERSONAL DATA PROCESSING POLICY

1. DEFINITIONS

- 1.1. **Controller** – TKT Engineering Sp. z o.o. with registered office in Warsaw, ul. Pryzmaty 4, 02-226 Warszawa.
- 1.2. **Personal data** – all information about an identified natural person or natural person identifiable through one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity, including image, voice recording, contact details, location data, information contained in correspondence, information collected through recording equipment or other similar technology.
- 1.3. **Policy** – this Personal Data Processing Policy.
- 1.4. **GDPR** – 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 repealing Directive 95/46/EC.
- 1.5. **Data subject** – each natural person whose personal data is processed by the Controller, e.g. a person visiting the premises of the Controller or submitting an inquiry to the Controller by email.

2. PROCESSING OF DATA BY THE CONTROLLER

- 2.1. In connection with the conducted business activity, the Controller collects and processes personal data according to the applicable regulations, including in particular the GDPR, and the data processing rules provided for therein.
- 2.2. The Controller ensures transparency of data processing, in particular always informs about the processing of data at the time of collection thereof, including about the purpose and legal basis for the processing – e.g. while concluding a contract for the purchase of goods and services. The Controller ensures that data is collected only to the extent necessary for the stated purpose and processed only for the period it is necessary.
- 2.3. While processing data, the Controller ensures their safety and confidentiality, and provides data subjects with access to information about the processing. If, despite applied safety measures, there is a data breach (e.g. data leakage or loss), the Controller will inform data subject about such an event in accordance with the regulations.

3. CONTACT WITH THE CONTROLLER

- 3.1. The Controller can be contacted by the email address kodo@tkt.pl or the correspondence address of TKT Engineering Sp. z o.o., ul. Pryzmaty 4, 02-226 Warszawa.

4. SAFETY OF PERSONAL DATA

- 4.1. In order to ensure data integrity and confidentiality, the Controller has implemented procedures which provide access to personal data only to authorised persons and only to the extent that is necessary due to the tasks they carry out. The Controller applies

organisational and technical solutions to make sure all operations on personal data are recorded and carried out by authorised persons only.

- 4.2. Furthermore, the Controller takes all necessary measures so that also their subcontractors and other cooperating entities guarantee to apply appropriate safety measures in each case they process personal data on behalf of the Controller.
- 4.3. The Controller conducts a risk analysis on an ongoing basis and monitors the adequacy of applied data security measures to identified threats. If necessary, the Controller implements additional measures to increase data security.

5. PURPOSES AND LEGAL BASIS FOR THE PROCESSING

EMAIL AND REGULAR MAIL CORRESPONDENCE

- 5.1. When sending correspondence that is not related to services provided to the sender or to any other contract concluded to the Controller via email or regular mail, personal data contained in such correspondence is processed only for the purpose of communication and resolution of the matter the correspondence relates to.
- 5.2. The legal basis for the processing is the legitimate interest of the Controller (art. 6 sec. 1 letter f) of the GDPR) consisting of the administration of correspondence addressed to the latter in connection with their business activity.
- 5.3. The Controller processes only personal data relevant to the matter the correspondence relates to. All the correspondence is stored in a way ensuring security of personal data contained therein (and other information) and is disclosed to authorised persons only.

CONTACT BY PHONE

- 5.4. If the Controller is contacted by phone, in matters not related to the concluded contract or services provided, the Controller may demand that personal data be provided only when it is necessary to handle the matter the contract relates to. In such a case the legal basis is the legitimate interest of the Controller (art. 6 sec. 1 letter f) of the GDPR) consisting of the necessity of resolving the reported matter related to the business activity conducted by the Controller.

VIDEO MONITORING AND ACCESS CONTROL

- 5.5. In order to ensure safety of persons and property, the Controller uses video monitoring and controls access to the premises and site managed by the same. Data collected in this manner is not used for any other purpose.
- 5.6. Personal data in the form of monitoring recordings and data collected in the visitor log book is processed in order to ensure safety and order of the facility, and to defend against claims or assert them. The basis for the data processing is the legitimate interest of the Controller (art. 6 sec. 1 letter f) of the GDPR) consisting of ensuring security of Controller's property and protecting their rights.

RECRUITMENT

- 5.7.** As part of the recruitment processes the Controller expects personal data to be provided (e.g. in a CV or resume) only to the extent specified in the labour law. Therefore, information must not be provided to a greater extent. If sent requests contain additional data, they will not be used or considered in the recruitment process.
- 5.8.** Personal data is processed:
- 5.8.1.** in order to fulfil the obligations under the law related to the employment process, including in particular the Labour Code – the legal basis of the processing is a legal obligation imposed on the Controller (art. 6 sec. 1 letter c) of the GDPR in connection with Labour Code regulations);
 - 5.8.2.** in order to carry out the recruitment process with regard to data not required by law, also for the purpose of further recruitment processes – the legal basis for the processing is consent (art. 6 sec. 1 letter a) of the GDPR);
 - 5.8.3.** in order to establish or assert any claims or defend against such claims – the legal basis for the data processing is the legitimate interest of the Controller (art. 6 sec. 1 letter f) of the GDPR).

COLLECTION OF DATA IN CONNECTION WITH THE PROVISION OF SERVICES OR IMPLEMENTATION OF OTHER CONTRACTS

- 5.9.** When collecting data for purposes related to the implementation of a specific contract, the Controller provides a data subject with detailed information regarding the processing of their personal data at the time of concluding the contract.

COLLECTION OF DATA IN OTHER CASES

- 5.10.** In connection with the conducted business activity, the Controller collects personal data also in other cases – e.g. at business meetings, trade events or through the exchange of business cards – for purposes related to initiating and maintaining business contacts. The legal basis for the processing in this case is the legitimate interest of the Controller (art. 6 sec. 1 letter f) of the GDPR) consisting of networking in relation to the business activity conducted.
- 5.11.** Personal data collected in such cases is processed only for the purpose for which it was collected, and the Controller ensures their adequate protection.

6. DATA RECIPIENTS

- 6.1.** In connection with activities requiring processing personal data is disclosed to third parties, including in particular to suppliers responsible for operating IT systems and equipment (e.g. CCTV equipment), entities providing legal or accounting services, couriers, marketing or recruitment agencies.
- 6.2.** The Controller reserves their right to disclose selected information concerning the data subject to relevant bodies or third parties applying for the provision of such information on the basis of an appropriate legal basis and in accordance with the applicable law.

7. TRANSFER OF DATA OUTSIDE THE EEA

- 7.1. The level of protection of personal data outside the European Economic Area (EEA) differs from that provided for by the European law. For this reason, the Controller transfers personal data outside the EEA only where necessary and with an appropriate degree of protection, in particular by:
- 7.1.1. cooperating with personal data processors in countries for which a relevant decision of the European Committee has been issued;
 - 7.1.2. applying standard contractual clauses issued by the European Committee;
 - 7.1.3. applying binding corporate rules approved by the competent supervisory body;
 - 7.1.4. in the event of transferring data to the USA – cooperating with entities participating in the Privacy Shield programme, approved by the decision of the European Committee.
- 7.2. The Controller always informs about the intention to transfer personal data outside the EEA at the stage of collection thereof.

8. PERSONAL DATA PROCESSING PERIOD

- 8.1. The period of data processing by the Controller depends on the type of a service provided and the purpose of the processing. The data processing period may also result from regulations when they constitute the basis for the processing. When processing data under the legitimate interest of the Controller – e.g. for safety reasons – data is processed for a period allowing that interest to be pursued or until an effective objection is made to the data processing. If the processing is carried out on the basis of consent, data is processed until such consent is withdrawn. When the necessity to conclude and implement a contract constitutes the basis for the processing, data is processed until its termination.
- 8.2. The data processing period may be extended in the event the processing is necessary to establish or assert claims or to defend against such claims, and after that period – only if and to the extent required by law. After the expiry of the processing period, data is irreversibly erased or anonymised.

9. RIGHTS RELATED TO THE PROCESSING OF PERSONAL DATA

RIGHTS OF DATA SUBJECTS

- 9.1. Data subjects have the following rights:
- 9.1.1. **right to information about the processing of personal data** – based on this the person making a request is provided by the Controller with information about the processing of data, in particular about the purposes and legal bases of the processing, the scope of data possessed, entities to which it is disclosed and the scheduled date of data erasure;

- 9.1.2. **right to obtain a data copy** – based on this the Controller provides a copy of processed data of the person making a request;
- 9.1.3. **right to rectification** – the Controller is obliged to remedy any possible inconsistencies or errors of processed personal data and complement them if it is incomplete;
- 9.1.4. **right to erasure** – based on this one may request that data, whose processing is no longer necessary for any of the purposes for which it was collected, be erased;
- 9.1.5. **right to restriction of processing of personal data** – if such a request is made, the Controller ceases performing operations on personal data – except for operations to which the data subject has given their consent – and stops storing them, according to the applied retention rules or until the reasons for the restriction of data processing cease to exist (e.g. a decision is made by a supervisory body to authorise further data processing);
- 9.1.6. **right to data portability** – based on this – to the extent data is processed in connection with the concluded contract or consent – the Controller issues data provided by the data subject in a computer-readable format. It is also possible to demand that such data be sent to another entity – however, on condition that there are technical capacities in this regard both on the part of the Controller and on the part of that another entity;
- 9.1.7. **right to object to the processing of data for marketing purposes** – the data subject may at any time object to the processing of personal data for marketing purposes without having to justify such objection;
- 9.1.8. **right to object to other data processing purposes** – the data subject may at any time object to the processing of personal data which takes place under the legitimate interest of the Controller (e.g. for analytical or statistical purposes, or for reasons related to property protection); an objection in this regard should provide a justification;
- 9.1.9. **right to withdraw consent** – if data is processed on the basis of consent, the data subject is entitled to withdraw it at any time, which, however, does not affect the compliance with the right to processing carried out before the withdrawal of consent;
- 9.1.10. **right to complain** – if it is believed that the processing of personal data breaches the GDPR or other personal data protection regulations, the data subject may lodge a complaint with the President of the Personal Data Protection Office.

MAKING REQUESTS FOR EXERCISING RIGHTS

9.2. A request for exercising rights of data subjects may be submitted:

- 9.2.1. in writing to the address: TKT Engineering Sp. z o.o., ul. Pryzmaty 4, 02-226 Warszawa;

9.2.2. by email to the address: kodo@tkt.pl

- 9.3.** If the Controller is unable to identify the person making a request based on the request made, they will request additional information from the requestor.
- 9.4.** The request may be submitted in person or through an attorney (e.g. a family member). For the sake of security of data, the Controller encourages the use of a power of attorney in a form certified by a notary public or authorised solicitor or counsellor, which will significantly accelerate the verification of the authenticity of the request.
- 9.5.** A respond to the request should be given within one months of receipt thereof. If it is necessary to extend this date, the Controller will inform the requestor about the reasons for the delay.

FEE RULES

9.7. The request process is free of charge. Fees may be collected in the following cases only:

9.7.1. if a request is made that the second and each subsequent copy of data be issued (first data copy is given free of charge); in such a case the Controller may demand a fee of PLN 100.00.

The above fee includes administrative costs related to the fulfilment of the request.

9.1.9. when excessive (e.g. unusually frequent) or patently unreasonable requests are made by the same person; in such a case the Controller may demand a fee of PLN 200.00.

The above fee includes costs of communication and costs of taking requested action.

9.8. If a decision on imposing the fee is contested, the data subject may lodge a complaint with the President of the Personal Data Protection Office.

10. CHANGES IN THE PERSONAL DATA PROCESSING POLICY

10.1. The Policy is verified on an ongoing basis and updated, if necessary. The current version of the Policy was adopted on 24 May 2018.