PRIVACY POLICY
in the company Metis Polska Sp. z o. o.

This Privacy Policy, hereinafter referred to as the Policy, has been prepared in order to demonstrate that personal data is processed and secured in accordance with the legal requirements regarding the principles of data processing and security in the Company, including Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46 / EC (hereinafter GDPR).

I. Personal data administrator

1. The personal data Administrator is Metis Polska Sp. z o. o. with headquarters in Warsaw, ul. Twarda 18, 00-105 Warsaw, entered by the District Court for the Capital City of Warsaw, XIV Commercial Division of the National Court Register to the Register of Entrepreneurs under the KRS number: 0000346294, NIP number 5242697220, REGON 142213792, hereinafter referred to as the "Administrator".
2. For purposes related to the protection of personal data, contact with the Administrator is possible in writing at the following address: ul. Twarda 18, 00-105 Warsaw, as well as in the form of electronic correspondence at the following e-mail address: rodo@metispolska.pl, as well as by phone at: +48 519 580 547.

II. General provisions

1. This Policy covers all personal data processed by the Administrator.
2. The policy is stored in electronic and paper form and is made available for inspection at the request of persons authorized to process personal data, as well as persons to be authorized to process personal data, in order to read its content.
3. In order to effectively implement this Policy, the Administrator provides appropriate technical measures to protect personal data and organizational solutions that prevent violation of this protection, their monitoring, as well as control and supervision over the processing of personal data.
4. Administrator ensures that the activities performed in connection with the processing and protection of personal data are in accordance with this Policy and the relevant legal provisions.

III. Personal data processed by the Administrator

1. Personal data processed by the Administrator are collected in data sets.
2. The administrator does not undertake processing activities that could be associated with a serious probability of a high risk for the rights and freedoms of individuals. If such an action is planned, the Administrator will perform the activities specified in art. 35 and next of GDPR.
3. The Administrator keeps a register of processing activities.
4. Personal data may be processed in paper and electronic form.

IV. The area of personal data processing

1. Personal data are processed by the Administrator in the territory of the Republic of Poland.
2. Periodically, personal data may be processed by the Administrator outside the territory of the Republic of Poland, for example during business trips.

V. Responsibilities in the field of personal data security management

1. All persons authorized to process personal data referred to in this Policy are obliged to process them in accordance with applicable regulations and the Privacy Policy established by the Administrator.
2. All personal data are processed in compliance with the rules of processing provided for by law:
a. In each case, there is at least one of the grounds for data processing provided for by law.
b. The data is processed fairly and transparently.
c. Personal data is collected for specific, explicit and legitimate purposes and not further processed in a manner inconsistent with these purposes.
d. Personal data is processed only to the extent necessary to achieve the purpose of data processing.
e. Personal data is correct and, when necessary, kept up to date.
f. Data storage is limited to the period of its usefulness for the purposes for which it was collected, and after this period it is deleted.
g. The information obligation is fulfilled towards the data subject in accordance with Art. 13 and 14 of GDPR.
3. The Administrator is obliged to ensure:
a. appropriate preparation of employees for the performance of their duties;
b. a written authorization for each employee who processes personal data.
4. Each employee of the Administrator processing personal data is obliged to:
a. comply with the authorization granted to process personal data;
b. processing of personal data in accordance with the law, including in accordance with the GDPR;
c. reporting incidents related to data security breaches;
d. keep personal data secret, as well as the methods of securing it.

VI. Violation of the security of personal data

1. A breach of the security of personal data shall in particular include:
a. Making data available or making it possible to disclose data to unauthorized persons or entities;
b. processing of personal data inconsistently with the intended purpose of their collection;
c. causing damage, loss, uncontrolled alteration or unauthorized copying of personal data;
d. loss of the personal data carrier.
2. In the event of a breach of personal data security, the Administrator's employee takes all necessary steps to limit the effects of the breach and immediately notifies the Administrator about finding these circumstances, as well as about the steps taken to limit the effects of the breach.

3. The Administrator assesses each time whether the breach of personal data protection could cause a risk of violating the rights or freedoms of natural persons. If there is a likelihood of violation of the rights or freedoms of natural persons, the Administrator shall, without undue delay - no later than 72 hours after finding the violation - report it to the supervisory authority.
4. If the risk of violation of rights and freedoms is high, the Administrator also notifies the data subject.

VII. Defining technical and organizational measures necessary to ensure confidentiality, integrity and accountability of the data processed

Technical and organizational measures necessary to ensure confidentiality, integrity and accountability of data processing include:
a. preventing third party access to the room;
b. protecting the Administrator's computer equipment against malware;
c. deletion of personal data from the data carrier in a way that prevents their re-establishment, and in the event of entrusting this activity to third parties - concluding an appropriate contract for entrusting the processing of personal data;
d. using a shredder to effectively remove documents containing personal data;
e. securing access to devices with access passwords,
f. applying the "clean desk" principle.

VIII. Entrusting the processing of personal data

1. The Administrator has the right to entrust the processing of personal data to a processor that provides sufficient guarantees for the implementation of appropriate technical and organizational measures to ensure that the data processing is lawful and protects the rights of the data subjects.
2. Entrusting the processing of personal data may take place only on the basis of a written contract that meets the conditions of art. 28 GDPR.

IX. Transferring personal data to a third country

The Administrator will not transfer personal data to a third country, except for situations where it occurs at the request of the data subject.

X. Cookies

Cookies are small text files installed on your device. Cookies usually contain the name of the website domain they come from, the storage time on the end device and a unique identifier. Taking care of the privacy of our users, we have implemented software whose purpose is to prevent the storage of cookies, the use of which the User does not consent to (if the legal basis for processing is the User's consent).

We use cookies primarily to determine the number of users of our website and traffic tracking, session statistics, approximate geolocation of users and information about the browser and device they use.

This is primarily to improve the quality of our services and website operation, as well as for marketing purposes, such as directing our offer to interested persons. Therefore, together with entities providing analytical and statistical services to us, we use cookies by storing information or accessing information already stored on your computer, phone, tablet, etc.).
Cookies used for this purpose include:
1. cookies with data entered by you;
2. authentication cookies used for services that require authentication for the duration of the session;
3. cookies used to ensure security, e.g. used to detect fraud in the field of authentication;
4.permanent cookies used to personalize your interface,
5.cookies used to monitor traffic on the website, i.e. data analytics, including Google Analytics cookies (these are files used by the Google company - i.e. the entity entrusted with the processing of personal data - to analyze how our website is used website by the user, including the creation of statistics and reports on the operation of the website).

XI. Final Provisions

The employee is responsible for failure to comply with the obligations arising from this document on the basis of the Labor Code and the provisions on the protection of personal data.