Appendix No. 2 to the Terms and conditions

Data Processing Agreement

§ 1.

Definitions

1. **Processor** - Service Provider in the meaning given to this term in the Terms and conditions.
2. **ADO** - Service Recipient in the meaning given to this term in the Terms and conditions.
3. **Data** - personal data entrusted to the Processor for processing by ADO in connection with the Basic Agreement.
4. **Sub- processor** - further processor whose services are used by the Processor in connection with the implementation of the Basic Agreement.
5. **Terms and conditions** - Terms and conditions of the service under which the Processor provides the Subscriber with software used to support law firms and the office of a restructuring advisor.
6. **GDPR** - Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 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 ("RODO ").
7. **Basic agreement** - an agreement together with the Terms and conditions in connection with the Service referred to in the Terms and conditions, which is the basis for entrusting the Data.

§ 2.

Preliminary Provisions

1. In connection with the conclusion of the Basic Agreement by the Parties, the Parties conclude a Data Processing Agreement.
2. ADO entrusts the processing of Data in relation to which it is the controller of personal data within the meaning of the GDPR, and the Processor undertakes to process them within the limits set out in the Agreement and generally applicable law.
3. Each Data processing by the Processor takes place only on the documented instructions of ADO, in particular those contained in the Basic Agreement, as well as expressed by ordering further services.
4. The data is processed for the purpose of implementing the Basic Agreement and to the extent necessary for its proper performance.
5. This Agreement supersedes all previous agreements, arrangements and understandings in this regard.
6. ADO declares and ensures that it has legal grounds for processing Data, and entrusting a Data Processor for processing will not violate the rights and freedoms of data subjects, as well as legal provisions (in particular the GDPR).
7. The data will be made available to the Processor only for the purpose of implementing the Basic Agreement.
8. ADO will inform the Processor about any activities of competent public administration bodies related to the processing of Data by ADO.
9. Access to the Data will only be granted to persons authorized by the Processor to process data, obliged to properly protect this Data - in accordance with the Processor's internal security procedures and the provisions of the GDPR, and also obliged to keep the Data in confidentiality or subject to a legal obligation to keep such secret.
10. The Processor takes all measures required by the applicable law, in particular by art. 32 of the GDPR, according to which the Processor implements appropriate technical and organizational measures, taking into account the state of technical knowledge, the cost of implementation and the nature,

scope, context and purposes of processing as well as the risk of violating the rights or freedoms of natural persons with varying probability and severity of threat, to ensure a level of security corresponding to this risk.

11. Data processing will take place during the term of the Basic Agreement.
12. By concluding the Agreement, the Service Recipient instructs the processing of the Data by the Service Provider, as well as to any person acting under the authority of the Service Provider who has access to Personal Data, which is a documented instruction within the meaning of art. 28 sec. 3 lit. and in relation joke. 29 GDPR.
13. The Processor is certified according to the ISO 27001 safety standard.

§ 3.

Data

1. The Service Provider may process personal data entrusted to it for processing by the Service Recipient in order to perform the Agreement and to the extent necessary for this, which includes in particular personal data contained in the database of the Program and the Website. Some categories of this data are defined by functionalities or fields available in the Program, Website and include, among others:

- names, surnames, contact details and identification data of natural persons who are clients of the Service Recipient and other persons whose data the Service Recipient entered into the Program, Website;
- financial data, including payment details, bank account numbers, credit cards, etc.

In addition, due to the purpose of the Program as supporting the conduct of cases conducted by a restructuring advisor or by a lawyer within the law firm, the Program may also process personal identification data (containing NIP, PESEL numbers, etc.), as well as data belonging to special categories (referred to in the GDPR as "sensitive data"), such as data on criminal records, health, sexual orientation, religion, origin, etc. However, it is emphasized that each time it is only the Service Recipient who decides on the scope and categories of personal data entered by him into the Program and thus covered by the entrustment, subject to the exceptions resulting from the Agreement, and the Service Provider indicates and stipulates that d any of these:

- should be limited to a minimum in accordance with the principle of minimizing the processing of personal data set out in the GDPR, and therefore should be subject to selection by the Customer, if possible;
- their introduction to the Program, the Website may not constitute an act violating the mandatory provisions of law;
- may be introduced only in accordance with the purpose and functionalities of the Program.

2. The categories of persons whose personal data may be processed under the Program and who are therefore entrusted with their processing to the Service Provider are defined as follows: clients of the Service Recipient; employees, contractors, partners, trainees, associates of the Service Recipient's clients; other natural persons whose personal data will be entered into the Program by the Service Recipient; representatives of public authorities participating in the proceedings conducted by a restructuring advisor or lawyer.
3. The processing of entrusted Data includes the following processing activities: recording, organizing, ordering, storing, downloading, viewing, matching or combining, limiting, deleting or destroying.

§ 4.

Support and audits

1. Taking into account the nature of the processing, the Processor will provide ADO support ("Support"). As part of the Support, the Processor will, as far as possible, help the ADO, through appropriate technical and organizational measures, to fulfill the obligation to respond to the requests of data subjects in the exercise of their rights set out in Chapter III of the GDPR - if in a given case they are incumbent on the ADO and will help ADO fulfill its obligations set out in art. 32 - 36 GDPR - taking into account the information available to him.
2. The processor is obliged to provide ADO with all information necessary to demonstrate the obligations set out in art. 28 of the GDPR and to enable ADO or an auditor authorized by ADO to conduct audits, including inspections ("Audit") and contribute to them.
3. In the event that the instructions issued by ADO in connection with the previous paragraph, in the Processor's opinion, constitute a violation of the provisions of the GDPR or other provisions of EU law or Polish law - the Processor will immediately inform ADO about it.
4. The Processor may refuse to provide ADO with information covered by a legally protected secret, including the secret of the Processor's or third parties' enterprise, as well as information constituting personal data that is not Data, if this information can be replaced with other information (including the Processor's statements), and in the case of when this is not possible - this information will be made available to ADO (or persons designated by it) only at the headquarters of the Processor, after prior conclusion by ADO and all persons acting on behalf of ADO, an agreement presented by the Processor obliging them to properly protect this information.
5. Conducting the Audit is possible after prior written notification of the Processor by ADO about the intention to conduct it at least thirty days in advance, along with an indication of the list of persons involved in conducting the Audit on the part of ADO. The notification should also specify the duration of the Audit and its scope.
6. If the Audit is not directly related to the activities of authorized public administration bodies addressed to ADO in connection with data processing or a confirmed and documented violation of Data processing by the Processor - the total duration of Audits conducted by ADO may not exceed three days in a calendar year.
7. The audit may be carried out only after prior conclusion by ADO and all persons acting on behalf of ADO, an agreement presented by the Processor obliging them to duly protect all information obtained in connection with the Audit.
8. The audit is carried out during the working hours of the Processor and may not in any way interfere or negatively affect the current activity of the Processor.
9. Audits are carried out at the expense of ADO. The costs of providing Support and supervision over the Processor by ADO are borne solely by ADO. The costs of support or supervision are, in particular, the costs incurred by the Processor in connection with carrying out checks, audits or preparation of documents, providing information or assistance to ADO. If the costs referred to in this paragraph have been incurred by the Processor - ADO will immediately reimburse them to the Processor. The hourly rate for handling the Audit by the Processor is PLN 350 net/hour/person.
10. The Processor cooperates with the authorities competent for the protection of personal data in the scope of their tasks.
11. Unless the provisions of law or this Agreement provide for a different time limit - performance of activities by the Processor in connection with the Agreement, including the provision of any information, will take place immediately, not later than within 30 days of receiving the relevant request.

§ 5.

Sub- processor

1. The Processor may use the services of the sub- processor only o with prior detailed consent or general written consent of ADO.
2. The Processor will impose on each sub- processor, in particular by means of an agreement, the same Data protection obligations as those resulting from the Agreement, in particular the obligation to implement sufficient guarantees for the implementation of appropriate technical and organizational measures so that the processing meets the requirements of the GDPR.
3. If the sub- processor fails to fulfill its obligations in relation to the Data, full responsibility towards ADO for the fulfillment of obligations by the sub- processor rests with the Processor.
4. ADO consents to the Processor's use of Sub-Processors indicated in Appendix No. 5 to the Basic Agreement. Changing the attachment does not constitute a change to the Agreement and the provisions of section 3-4 of this paragraph shall apply accordingly.
5. Entrusting the processing of Data to other processors not indicated in Appendix no. 5 requires prior notification of this fact to ADO - in order to enable it to object. The objection may be made no later than seven days before entrusting the Data to the sub- processor. Notification of the intention to entrust by the Processor may be made in particular in electronic form.
6. In the absence of objections, it is assumed that ADO has consented to the use of Another Processor.
7. In the event of an objection by ADO, the Processor may not entrust the data to another processor to whom the objection relates. The Processor will be entitled to terminate the Basic Agreement in this case, with immediate effect, and ADO will not be entitled to any compensation in this respect.

§ 6

Data breach

1. The Processor is obliged to notify the ADO without undue delay, but not later than within 48 hours of becoming aware of any case of occurrence or suspected occurrence of an information security incident related to the Data entrusted to the Processor, in particular constituting a breach of personal data protection.
2. The Processor's obligation referred to in par. 1 above is not and will not be interpreted as confirmation by the Processor to the data subjects of a personal data breach.

§ 7.

Final Provisions

1. The Agreement is terminated upon termination of the Basic Agreement.
2. The Processor, after the provision of services related to the processing of Data for ADO, in particular in the event of termination of this Agreement or the Basic Agreement, depending on the decision of ADO:
    a) deletes the Data;
    b) returns to ADO all Data and deletes all existing copies thereof, unless European Union law or generally applicable Polish law requires the storage of personal data.
3. In the event of termination of the Basic Agreement, the ADO should provide the Processor with the decision referred to in the previous paragraph, no later than on the last day of the Agreement's validity. In the absence of such a decision within this period - it is assumed that the ADO ordered the Processor to delete the Data and all related consequences are borne solely by the ADO.
4. In matters not regulated, including changes to the Agreement, the provisions of the Basic Agreement shall apply.

Appendix no 3 to the Terms and conditions

The list of further processors

ADO agrees to entrust the Data by the Processor to the following Sub-Processors:

1. Microsoft Corporation. One Microsoft Way. Redmond, Washington 98052-6399.

2. Amazon Web Services, 38 Avenue John F. Kennedy, L-1855, Luxembourg

3. Mixpanel, Inc., Mixpanel International, Inc., Mixpanel S.L., Mixpanel UK Limited, and Mixpanel APAC Pte. Ltd.

Appendix No. 4 to the Terms and conditions

Minimum security standards

AWS, whose server services are used by the Service Provider, ensures a high standard of personal data processing security, meeting, among others, the following safety requirements:
- Internet connection encryption systems and AES256 database encryption (SSL, TLS, IPSec);
- physical and digital technical security measures for servers and other places where personal data is processed;
- ensures complete control of the movement of people and vehicles throughout the administrative area;
- the facilities are divided into security zones and movement in the zones is supported by the Access Control System ensuring full accountability and control of access rights;
- facilities are monitored by the CCTV System;
- facilities have a Burglary and Assault Signaling System;
- signals from security systems are received and monitored on a continuous basis (including those relating to network infrastructure, power supply and security of server rooms, administration and office facilities and other important resources used to provide services) - these systems are regularly tested;
- applies a backup policy (policy for creating backups),
- IT systems and applications used to process personal data are regularly updated, verified for vulnerability and secured by anti-virus systems,
- applies protection against unauthorized access to systems and networks using firewall systems,
- uses network traffic monitoring systems - detected anomalies are logged and reported,
- provides the following services to the Service Provider: RDS (databases), EC2 (virtual servers), Lightsail (website), S3 (document storage), S3 Glacier (backups), S3-Buckets;

- has ISO 27001/9001 certificate;
- has ISO 27017/27018 certificate;
- has a certificate of compliance with the CISPE Code of Conduct - a code of good practice for cloud service providers confirming compliance with the requirements of the GDPR.