

PROCESING OF PERSONAL DATA AGREEMENT

Concluded in accordance with § 1746 of Act No. 89/2012 Coll., the Civil Code as amended and Art. 28 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27th 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 as amended (hereafter referred to as “**GDPR**”) (this contract hereafter referred to as the “**Contract**”)

1. CONTRACTUAL PARTIES AND THEIR RELATIONS

1.1. The Controller

as the User of the Service (hereafter as “**Controller**”)

1.2. The Processor

My Callsheet s.r.o., a limited-liability company registered in the Commercial Register administered by the Regional Court in Plzeň, section C, file 34227, with registered office K Ovčínu 297/18, Litice, 321 00 Plzeň, company reg. No.: 058 79 582 (hereafter as the “**Processor**”)

(The Controller and the Processor hereafter also as “**Parties**” or individually as a “**Party**”)

2. THE SUBJECT OF THE CONTRACT

- 2.1. The subject of the Contract is a processing of selected personal data of third parties, who are not parties to the Contract (“**Personal data**”). The Personal Data of the third parties are either entered into the Service as the Data or the Information. The scope of the Personal data processed by the Service is determined by the Controller, since the Processor has no control over the personal data entered into the Service by the User. The processor carries out the Personal data processing in the scope set out in the Contract and according to instructions issued by the Controller.
- 2.2. Processing of the Personal data governed by this Contract is based on the agreement of the Parties, the content of which is set forth in the Contractual arrangements and with which the Controller has agreed to by the conclusion of this Contract (“**Contractual arrangements**”).
- 2.3. If the contractual relationship between the Controller and the Processor based on the Processing agreement is terminated, the contractual relationship between the Parties governed by the Contractual arrangements and the reverse shall also be terminated.
- 2.4. The terms used in this Contract with a capital letter correspond to the terms used in the Contractual arrangements with a capital letter unless these terms are also defined in this Contract.

- 2.5. Satisfying the obligations arising from the Contract, the Processor processes the following categories of personal data:
- a) Name
 - b) Surname
 - c) Email
 - d) Phone number
 - e) Social sites
 - f) Photo
 - g) Team role
 - h) Based in
 - i) About me
 - j) Transportation
 - k) Accommodation
 - l) Receipts
 - m) Other
- 2.6. Satisfying the obligations arising from the Contract, the Processor processes personal data of the following categories of data subjects:
- a) Employees of the Controller
 - b) Team members
 - c) Other Users of the Software
- 2.7. Further categories of the Personal Data and data subjects may be expanded by the Controller by their actual insertion into the Service. For the avoidance of any doubt, the data entered by the Controller into the Service is considered to be the data processed by the Processor under this Agreement.
- 2.8. The purpose of the Personal data processing as well as the categories of the Personal data are determined by the Controller in their capacity as the User.
- 2.9. The Personal data are processed during the duration of the contractual relation between the Processor and the Controller governed by the Contractual arrangements. By its termination or by the termination of the Contract the Personal data processing terminates as well.
- 2.10. For the avoidance of any doubt, the personal data of the User are not third party personal data, and as such fall outside the scope of this Contract.

3. THE CONTROLLER'S OBLIGATIONS

- 3.1. The Controller is obliged to process only the Personal data, for the processing of which it has a lawful basis pursuant to the Applicable regulations for personal data protection.
- 3.2. The Controller undertakes to fulfil its obligation to provide information to all the relevant Data subjects whose Personal data are processed under this Contract in accordance with the Applicable regulations. Should the Controller ascertain that it is not fulfilling its obligation to provide

information in the scope set out in the Applicable regulations then the Controller is obliged to ensure redress without delay.

4. THE PROCESSOR'S OBLIGATIONS

- 4.1. The Processor undertakes to process personal data and the results solely by virtue of written instructions by the Controller. If the Processor is obliged, following a ruling by a public authority, to transmit the personal data processed upon the instructions from the Controller, the Processor shall inform the Controller of such fact without unnecessary delay and subsequently the public authority as well, unless such conduct contradicts the law.
- 4.2. The Processor declares that all persons participating in the processing are obliged to maintain confidentiality by the Processor or by an act of law. The Processor further declares that the non-disclosure obligation lasts even after such persons stop participating in the processing for any reason.
- 4.3. The Processor undertakes to take into account the nature of the data processing and to support the Controller by appropriate technical and organizational measures in order to enable the Controller to satisfy the data subjects' rights according to Chapter III of GDPR. If the Processor receives a request by a data subject that clearly indicates that the data subject mistakenly considers the Processor to be the Controller, the Processor is obliged to pass the request to the Controller without unnecessary delay and inform the sender, i.e. the given data subject. If such request occurs, the Processor shall not alter the data subject's personal data without the Controller's knowledge.
- 4.4. The Processor shall assist the Controller with ensuring that obligations arising from Articles 32 to 36 of GDPR are met (e.g. the security of processing, notification of a personal data breach, data protection impact assessment and prior consultation).
- 4.5. The Controller is entitled to supervise the Processor in terms of the personal data transmitted, including the technical and organizational measures, to check the processing carried out by the Processor, as well as the persons assigned by the Processor to process the data, and perform an audit thereof. The Processor is obliged to assist the Controller with performing these activities. The Controller may appoint another person to perform the activities according to the previous sentence. The Processor undertakes to provide the Controller with any information necessary for the supervision of obligations determined in the Contract. The Processor is entitled to claim compensation from the Controller for the demonstrable expenses arising from such performed supervisory activities.
- 4.6. Upon the termination of the Contract, the Processor is obliged to dispose of the results of the processing and all media containing personal data to the Controller and to erase all existing copies. If the Processor processes the personal data in a special format, the Processor is obliged to transmit the personal data upon the termination of the Contract in accordance with the Controller's requirement in the given special format, or the format in which the Processor obtained the personal data from the Controller, or a format typically used for transferring information (e.g. XML).

- 4.7. The Processor is obliged to immediately inform the Controller if, according to the Processor's opinion, an instruction violates GDPR or other EU regulations or regulations of a given Member State concerning personal data protection.
- 4.8. The Processor is obliged to immediately inform the Controller if an inspection occurs or measures are taken against the Controller by the supervisory authority, with regard to the Contract. This also applies to situations when the Processor is being investigated by an authority in the case of a violation of private or public law, especially administrative or criminal law if this relates to the processing of personal data according to the Contract.
- 4.9. If the Controller participates in any proceedings, especially administrative or criminal, or if a claim was made against the Controller within private law in terms of the processing by virtue of the Contract, the Processor is obliged to make all efforts to be of assistance to the Controller.
- 4.10. The Processor is obliged to notify the Controller without delay of all cases of personal data breach and fully cooperate as far as the context requires. Similarly, the Processor is obliged to cooperate to the necessary extent in assessing the impact on the protection of personal data, including prior consultation with the supervisory authority. The Processor is entitled to claim compensation from the Controller for the losses demonstrably caused by the Controller's activities.

5. TECHNICAL AND ORGANIZATIONAL MEASURES

- 5.1. The Processor undertakes to implement organizational and technical measures pursuant to Article 32 of GDPR.
- 5.2. According to Article 32, paragraph 1 of GDPR, the Processor shall take into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons. Appendix No. 1 includes details.

6. THE VENUE FOR PROCESSING OF PERSONAL DATA

- 6.1. **The Processor is not permitted to transfer the Personal data to so-called third countries**, i.e. outside the territory of the European Union, or the European Economic Area, provided that such Personal Data originate from the Data subjects of that territory.
- 6.2. Processing of personal data may at least partially take place outside the European Union or the European Economic Area, i.e. in the third countries. Appropriate protection of personal data in these countries arises, in particular, from:
 - 6.2.1. An adequacy decision according to Article 45 of GDPR; or
 - 6.2.2. Standard data protection clauses according to Article 46, paragraph 2, letter c) and d) of GDPR.
- 6.3. The Processor informs the Controller and the Data subjects on the third countries in which the processing takes place in the Privacy policy.

7. OTHER PROCESSORS

- 7.1. The Processor is authorized to involve other processors in the processing, while the choice of other processors rests fully on the Processor.
- 7.2. The Processor informs the Controller and the Data subjects on the other processors involved in the processing, as well as about the purposes of their involvement in the processing, in the Privacy policy.
- 7.3. The Processor shall ensure that the same obligations apply to such other processors as to the Processor arising from the Contract. If such other processors fail to satisfy their obligation or obligations with regard to protection of personal data, including the obligations specified in the Contract, the Processor is accountable to the Controller for such failure.

8. VALIDITY AND EFFECT OF THE CONTRACT

- 8.1. The Contract becomes valid and effective on the day of its approval by electronic means from the Controller, as the User.
- 8.2. The Contract is concluded for an indefinite period, but its validity and effectiveness are connected to the contractual relationship between the Controller and the Processor concluded by acceptance of the Contractual arrangements by the Controller. A termination of the contractual relationship arising from the Contractual arrangements results in the termination of this Contract.
- 8.3. The Contract terminates by means specified in the Contract, law or by virtue of a written agreement of the Parties.
- 8.4. The Contract terminates by deleting the User's account.

9. EXPRESSION OF AGREEMENT

- 9.1. The Controller expresses its will to be bound by this Contract by ticking the appropriate box, which is without any doubt associated with the agreeing act of the User.
- 9.2. The Processor expresses its will to be bound by the Contract by making it available on the Website.

Appendices:

Appendix 1 – Technical and Organizational Measures

CONFIDENTIALITY

- Admission management: reinforced concrete walls, armoured doors, chip system protected by PIN numbers, perimeter protection, camera system in HD, independently lockable racks
 - Access rights: combination of the correct username and password
 - Separate processing: Processing of personal data takes place in only our company, we do not share your personal data with third parties.
 - Pseudonymization: If the processing of personal data enables it, the data on a data subject's identity shall be removed from the given data application and stored separately; We do store your personal data, but the data we collect is not very sensitive. Therefore, we do not do pseudonymization. On the other hand, the user is free to delete his or her profile. The profile is deleted after twenty-four hours from the time the request was made. User's name and details connected to his or her profile are removed from every callsheet and contact list.. Guest accounts are automatically deleted from our system forty-eight hours after the callsheet period assigned to that user has ended and the callsheet has served its purpose.
 - Data classification system: public
 - Access management: We have implemented Role Based Access Control
1. **Only callsheet administrator** can change **joint details** in the **callsheet's joint part** and details of **every team member (every team member's callsheet's personal section)**.
 2. **Only an agent assigned to a user** can manage the assigned user's callsheet's personal section.
 3. **User can manage only his or her private info and receipts in his or her callsheet's personal section.**

Our callsheet is made of five parts.

Two joint sections and three personal sections.

- **The joint section (seen by every team member on a callsheet) contains:**

Basic information

callsheet name
project name
project date
location (added via Google maps)
call time
duration
additional info (text or a file)

Team

Here you can find all the team members, who have been added to the same callsheets with the same dates as you were. If you are an administrator, you can see every team member. Do not forget, even if your profile is set to “private”, other team members can see it as “public” during the time you work together according to the dates set on your callsheet. One day before the job and one day after the job your profile will be private. During the job, it will be viewed as “public” to every team member.

The personal section (visible only to the actual person, assigned agent or assigned administrator):

Trip details

Transportation (flight, train, bus, ship, car, other)
Hotel (added via Google maps)

Private info

Every user, assigned agent or callsheet administrator can add text or a file for the user.

Receipts

Add your receipts and share them with your agents or clients.
Assigned agents and administrators can see them without you sharing them.

INTEGRITY

- Transfer management: Encryption with HTTPS protocol
- Handling management: In this moment we cannot provide details by whom and when were data entered, altered or deleted in the personal data processing systems and by whom

RESILIENCE AND AVAILABILITY

- Availability management: Data is backed up on the server online and off-site, uninterruptible power supply by UPS and diesel unit, anti-virus, firewall, incident report procedure, security checks at the level of infrastructure, server is hosted by a company fulfilling the ISO 9001 and ISO 27001 requirements (automatic identification of potential risks and eliminating them before they can materialize, plans for a case of extraordinary events caused by a person or force majeure and constant improvement of the ability of our systems to overcome any consequences, very high protection against cyber-attacks and constant improvement of that protection, procedures according to the structured and globally renowned methodology of information security, in compliance with the valid legislation and trends, determined precautions to prevent failures and outages of the provided services)

- Swift recovery after an incident: we do have Service-level agreement for a smooth application development and maintenance
- Periods of personal data storage: Personal data is stored until the User deletes any of it, by deleting his data it is automatically deleted from the whole system. The user can also delete his or her profile, the profile is deleted after 24hrs from the time the request was made, and his or her name is removed from every active callsheet, along with every personal part from each active callsheet. Guest accounts are automatically deleted from our system in twenty-four hours after the active callsheet period has ended and the callsheet has served its purpose.

PROCEDURES FOR REGULAR REVIEW AND ASSESSMENT

- Management of personal data protection, including regular employee training: Only the very necessary amount of people has access to the personal data, all of them are highly professional and do respect the importance of personal data protection
- Incident management: We have plans for a case of extraordinary events caused by a person or force majeure and we constantly improve the ability of our systems to overcome any consequences
- Standard protection of personal data: Active protection against cyber-attacks and constant improvement of that protection, automatic identification of potential risks and eliminating them before they can materialize
- Processing management: according to the standards ISO 9001 and ISO 27001