



## Privacy Policy

### Introductory provisions

URKA d.o.o. – PerfectMeetings.hr respects your privacy and pays special care to the protection of your personal data. Therefore, this document serves to clarify which personal data are processed, why we process such data and how we deal with personal data we process.

Your data are collected and processed solely for the purpose of providing our services in a lawful, fair and transparent manner. We only process data necessary to provide a particular service, taking into account their adequate protection.

Such personal data are primarily about individuals (natural persons) with whom we have a business relationship or a legitimate interest to contact them (clients, suppliers, business partners, employees etc.)

When the need for processing your personal data expires, we erase all personal data or use adequate technical solutions for ensuring anonymity of data for the sole purpose of their use for statistical purposes.

Personal data are always processed in accordance with our fundamental values and principles, this Privacy Policy and the applicable EU and Croatian regulations relating to the protection of personal data. This Privacy Policy equally applies to personal data in electronic form, as well as to personal data in printed (paper) form, regardless of whether an electronic record is printed. The terms denoting gender used in this Privacy Policy relate equally to male and female gender.

### Principles relating to processing of personal data

When processing personal data, we do so by following the principles and rules as stipulated in 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 (General Data Protection Regulation). When processing personal data, we take into account the legal obligation of professional secrecy as regulated by the EU, i.e. Croatian law.

Our employees protect personal data as a trade secret, even after termination of employment.

We only process personal data as follows:

- lawfully, fairly and in a transparent manner;
- for specified, explicit and legitimate purposes;
- using only accurate, up-to-date, appropriate and relevant data limited to the purpose for which they are being processed;
- keeping them for no longer than is necessary for the purposes for which the personal data are processed and
- protecting them against unauthorised or unlawful processing and against accidental loss, destruction or damage.

Personal data of children below the age of 16 years are processed only based on the parental or carer consent in the extent and scope consented to. We handle such data with particular care.



### **Confidentiality and safety**

All personal data are handled with confidentiality, considering the adequate level of safety and technical, i.e. organisational protection. We never perform unauthorised collection, processing or any other way of such personal data use. Our employees only process the data necessary for them to perform their work and those they have been authorised to process. When our employees process personal data, they do so as authorised and within the scope of authorisation, that is, exclusively for the purpose for which data were collected or for which they are processed. When handling personal data, we follow the “need-to-know” principle in order to make sure that only authorised employees have access to certain personal data in a specified time period. Before introducing new technologies, which can be used for personal data processing, we perform thorough analysis and adjustment of technical and organisational measures to ensure that the highest personal data protection standards are applied.

### **Guidance for employee actions**

In their everyday work, our employees follow this Privacy Policy and valid regulations relating to personal data protection. Access to personal data is allowed only to those employees that need the access to perform their jobs, that is, to perform their tasks. Personal data are not distributed informally among employees and each access needs to be requested from the person in charge of a specific job, that is, a person who issued the order.

In cooperation with the Data Protection Officer, we organise training at least once in six months or make our employees familiar with their obligations and regulations relating to personal data protection in another suitable way. We always make sure to implement good data protection practices in accordance with recommendations of the Personal Data Protection Agency and other authorities competent for the protection of data in the European Union and Croatia.

Our employees take corresponding measures of organisational and technical protection to reduce the risk to personal data, in particular by:

- Using strong passwords on computers and mobile devices known only to them, changing them regularly and not distributing them to third persons;
- Regularly checking whether data are up to date and what their purpose is. If personal data are not used any more or if they are not up to date and cannot be updated, they are either deleted or anonymization is performed;
- Locking computers on which they work carrying personal data when they are left unsupervised;
- Making sure that personal data they have access to are not submitted to or disclosed to unauthorised persons and
- Consulting the Data Protection Officer or authorised person when in doubt regarding any aspects of personal data protection.

### **Data storage**



We pay special care regarding how data are stored, whether they are in printed, electronic or any other form. Personal data in printed form, regardless of whether they are in form of a print out of data generally kept in electronic form:

- When not used, are stored in a closed drawer or file cabinet accessible only by authorised persons;
- All employees are obligated not to leave such documents in visible places, that is, anywhere where unauthorised persons might access personal data and
- When they are no longer used, they are destroyed in a paper shredder, or using another technically acceptable way, and are appropriately disposed in an environmentally conscious way.

Personal data in electronic form are protected from unauthorised access, accidental changes or deletion, that is, unauthorised system access by applying a series of organisational and technical measures, such as:

- Using strong passwords which are regularly changed and known only to authorised persons and not distributed to third persons;
- If personal data are on portable media (e.g. CD, DVD, USB stick, portable HDD...), such portable media are safely stored, locked and put away at a location accessible only to authorised persons;
- For storage purposes, we exclusively use official storage media and servers, that is, selected cloud services with appropriate organisational and technical protection measures in place and with guarantee of their application;
- Servers where personal data are stored are at a safe location with access allowed only to authorised persons;
- Data backup is regularly performed, taking into account that unnecessary multiple copies are not made in order to ensure integrity, truthfulness and accuracy of data, in accordance with this Privacy Policy and valid regulations relating to personal data protection;
- Personal data shall not be directly stored on mobile devices (e.g. tablet, smartphone, etc.) unless this is necessary for performance of a contract, that is, performing an agreed service, and only in the agreed duration and scope and if necessary;
- All servers and computers with personal data have been protected with adequate technical protection measures such as encryption programmes, firewalls, etc.

### **Data processing**

All personal data are processed lawfully, in accordance with the terms, principles and standards of the General Data Protection Regulation and national legislation. Processing is primarily based on the performance of contractual relations or compliance with contractual and legal obligations, and on clear and unambiguous affirmative consents. Particular attention is paid to the processing of special categories of personal data.

We mostly deal with special categories of personal data of our employees, who provide explicit consent for their processing or the data are processed in a way to protect and exercise rights and interests of employees in the area of labour law and social security and social protection law. We



occasionally process special categories of our clients' personal data, who provide explicit consent for their processing, mostly to ensure their health is protected during travel (such as data about allergies, etc.). We do not use automated personal data processing, including profile creation, to make a decision that produces or may produce legal effects for data subjects or may otherwise significantly affect data subjects and exercise of their rights. We make sure that we collect personal data directly from the data subjects to whom the personal data relate. When collecting personal data, the data subjects are always informed about the reason and purpose of processing personal data as well as the legal basis for such processing. If we collect personal data from third parties, we primarily take steps to make sure that this person has a valid authorization, consent, or other legal basis for providing such personal data. In this case, we provide all the information provided for by the General Data Protection Regulation.

### **Transfer of personal data**

For each transfer of personal data, we use appropriate organizational and technical protection measures that correspond to the categories of personal data and the risk arising from such categorization, taking into account the particularities of each specific transfer. We shall never disclose your data to third parties, without your explicit request and a clearly given, unambiguous and specific consent, or when it is necessary to complete a contracted service. In exceptional cases, we may disclose your personal data to relevant international, state and public authorities, if that might be necessary to meet legal obligations, and to protect interests which are essential for the life of the data subject or those of other natural persons. Likewise, at a request of a court and for the purpose of court proceedings (independent of the stage of the proceedings), we can disclose your personal data within the scope and limits of a court order.

When we act as a processor on behalf of the controller, we guarantee the implementation of appropriate technical and organizational measures in accordance with the General Data Protection Regulation and this Privacy Policy, taking into account the protection of rights of the data subject. Such processing of personal data is governed by a written contract or another legal act in accordance with the European Union law or the Republic of Croatia law, stating that the controller determines the subject and duration of processing, the nature and purpose of processing, the type of personal data and the category of data subjects, as well as his/her own obligations and rights. In this case, we process personal data only in accordance with explicit and clearly defined instructions, i.e. orders, provided by the controller. As a processor, we do not process personal data, whether we have access to them or not, unless specifically requested by the controller, and in that case, we do so only in the manner and to the extent requested by the controller, in accordance with the General Data Protection Regulation.

We apply the same principle when providing our services. By using appropriate technical protection methods, such as encryption, and by respecting and enforcing this Privacy Policy, we ensure that our employees do not access or otherwise come into contact with any personal data that they are not authorized to access, or which are not required in order to provide the contracted service.



Before transferring personal data to third parties, we make sure that recipients comply with the General Data Protection Regulation and national legislation, and we may, if necessary, request guarantees or direct insight into their security and protection measures.

### **Data protection impact assessment**

If, after consulting the Data Protection Officer, we estimate that there is a probability that some sort of processing, especially when using new technologies and taking into account the nature, scope, context and purpose of processing, might cause a high risk to individuals' rights and freedoms, we perform an impact assessment of the envisaged processing procedures on the protection of personal data.

When performing an impact assessment, it normally consists of a systematic description of the envisaged processing procedures and the purpose of the processing, the assessment of the necessity and proportionality of processing procedures with respect to the purpose of processing, risk assessment of rights and freedoms, and measures to address the risk problem and demonstrate compliance with the General Data Protection Regulation.

### **International transfer of personal data**

We do not transfer personal data to third countries or international organizations (international transfer), except for the performance of contractual arrangements or services, in legally required cases or at your explicit request with a clear, unambiguous and accurate consent.

The possible transfer of personal data to a third country or an international organization is based solely on:

- a list of countries and international organizations which ensure an adequate level of protection, in accordance with the published European Commission Decision;
- envisaged appropriate protective measures such as binding corporate rules, instruments of public authorities, an approved code of conduct together with the binding and enforceable obligations of the controller or processor in the third country relating to the consistent application of the appropriate protective measures and
- the existence of appropriate institutional legal protection of data subjects in the third country.

Any court judgement or decision of a third country's administrative body requiring the transfer or disclosure of personal data shall not bind us nor shall we act upon it, unless it is based on an international agreement binding for the Republic of Croatia, such as a mutual legal assistance treaty.

### **Accuracy and updating of personal data**

It is important to us that data are accurate and up-to-date, not only in order to achieve the purpose of data processing, but also to allow you to exercise your rights and personal data protection. Therefore, we take appropriate technical and organizational measures to ensure that personal data are accurate and up-to-date, in accordance with personal data categories and their importance for achieving the purpose of processing.



## URKA, d.o.o. – Tourist Agency – PerfectMeetings.hr

Head office: Cernička 21, Office: Draškovićeva 66; 10000 Zagreb

VAT (OIB): 28424041057; ID code: HR-AB-01-060027010

Insurance policies at Jadransko osiguranje

To ensure that personal data are accurate and up-to-date, personal data will be located, i.e. stored at as few locations as possible (that is, only where it is necessary), and employees will not create or use unnecessary copies, additional databases, sets or other ways of grouping personal data. This is how we reduce the risk of unwanted treatment of personal data.

In a simple and affordable way, by using good practice examples, we enable all data subjects whose personal data we process to update their personal data.

If, during processing or use of personal data, certain personal data are found to be inaccurate or not up to date, and they cannot be updated, or such an update would result in unreasonable efforts or costs, such data will be erased.

### Keeping and erasing personal data

In accordance with the principles on which our Privacy Policy is based, we process your personal data only for as long as it is necessary to achieve the purpose of processing, that is, for as long as it is required by law or by-law, and after we no longer need the personal data, we delete them or anonymize them. If we are unable to accurately determine the time limit or length of keeping your personal data, we will provide you with a framework assessment based on past experience and good practice examples. We control and review personal data we process twice a year to ensure that all personal data the purpose of which has been achieved, i.e. which are no longer needed, are deleted or anonymized. The control is performed by an authorized employee, in cooperation with the Data Protection Officer who is required to make a report and any recommendations, if he or she establishes the existence of personal data which are no longer needed.

Exceptionally, we may keep your personal data longer than indicated if that might be necessary in order to comply with a court order or an authorized body's order for the purpose of meeting legal obligations to protect interests which are essential for the life of the data subject or those of other natural persons.

### Data Protection Officer

In accordance with the General Data Protection Regulation and internal acts, we have appointed the company **GDPR-MEDIA** j.d.o.o. from Samobor, Ivica Sudnika 7, PIN (OIB): 23309501979 as the contracted Data Protection Officer. Data Protection Officer's contact information is: [info@gdpr-media.eu](mailto:info@gdpr-media.eu).

The Data Protection Officer informs and advises the company, as well as the employees of the company performing the processing, of their obligations regarding data protection. The Data Protection Officer also monitors compliance with the General Data Protection Regulation and other regulations of the European Union or the Republic of Croatia relating to the protection of data and controller's or processor's access in relation to the protection of personal data.

The Data Protection Officer cooperates with the Personal Data Protection Agency as a supervisory body and acts as a contact point for the supervisory authority when it comes to personal data processing and, where appropriate, for all other matters.

### Exercise of the data subjects' rights



Exercising the rights of data subjects is of particular importance to us, so we approach each request for exercising rights seriously and professionally, in line with the requirements of the General Data Protection Regulation and the principles on which this Privacy Policy is based. An overview of your rights in this Privacy Policy is simplified for ease of use and ease of reference. The General Data Protection Regulation and national legislation comprehensively govern the complex procedure for exercising rights; we therefore recommend that you familiarize yourself with the regulations that provide a comprehensive description of your rights and how to exercise them. The data subject has the right to receive confirmation whether or not his or her personal data are processed. If his or her personal data are processed, the data subject may request access to his / her personal data, with indication of the purpose of the processing, personal data categories and potential recipients to whom the personal data have been disclosed (or will be disclosed on the basis of a valid legal basis).

The data subject has the right to request his / her personal data to be corrected or erased, i.e. to restrict the processing of personal data as well as the data transferability.

Exercising the rights of the data subject from our side cannot affect the right of the data subject to contact the Personal Data Protection Agency or another supervisory body.

A claim for exercising the right shall be submitted by email to our Data Protection Officer: GDPR-MEDIA j.d.o.o., Ivica Sudnika 7, Samobor; PIN (OIB): 23309501979; Email: [info@gdpr-media.eu](mailto:info@gdpr-media.eu).

We reserve the right to create a separate electronic form on our website as a standardized way of submitting requests for exercising the data subject's rights, but this will not affect the option for the data subject to send such a request to the specified email address.

The Data Protection Officer will take appropriate steps to unambiguously establish the identity of the applicant before providing any information pertaining to personal data. We take security of personal data very seriously and, therefore, we carry out appropriate verification measures to reduce any risks. Data regarding exercising of rights are provided in electronic form, free of charge. In case of requesting a copy of such data or making repeated requests relating to the substantially equal exercise of rights, or in case of obviously unfounded or excessive requests, we will charge a monetary fee based on the actual administrative costs of meeting such a requirement.

If your personal data processing is based on your consent, you may withdraw such consent at any time in a simple and transparent way, and request that we stop processing your personal data for marketing and promotional purposes. Also, you may request that we erase your personal data without unnecessary delay if: personal data are no longer necessary for the purposes for which they were collected, or they must be erased in order to comply with the regulations of the European Union or the Republic of Croatia.

### **Procedure in case of personal data breach**

In the event of personal data breach, and particularly in case of unauthorized access into our computer system, we will notify the Personal Data Protection Agency of such a breach not later than 72 hours after having become aware of it. If personal data breach can cause a high risk to



**URKA, d.o.o. – Tourist Agency – [PerfectMeetings.hr](http://PerfectMeetings.hr)**

Head office: **Cernička 21**, Office: **Draškovićeva 66; 10000 Zagreb**

VAT (OIB): **28424041057**; ID code: **HR-AB-01-060027010**

Insurance policies at **Jadransko osiguranje**

individuals' rights and freedoms, we will notify all those data subjects whose personal data have been breached without any delay.

### **Final provisions**

If you believe that we do not handle your personal data appropriately or you feel that the processing of your data is not in compliance with the General Data Protection Regulation and national legislation, you are entitled to contact the Personal Data Protection Agency.

This Privacy Policy will be updated as needed and at least once a year, while considering good practice examples and news in the area of data protection.

Zagreb, 22 May 2018