

# **Iskon Internet's user data protection policy**

## **Introduction**

Iskon Internet d.d., Garićgradska 18, 10000 Zagreb (hereinafter: Iskon), pays special attention to the protection and privacy of its users' personal data (hereinafter: data protection) in accordance with applicable regulation and best European practice. Iskon users' data protection is an essential part of our services and products and an important factor in the user experience.

By implementing Iskon Internet's user data protection policy (hereinafter: Policy) we wish to provide our users with clear information about the processing and protection of their personal data at Iskon and provide them with simple means of supervision and management of their personal data and consents.

This Policy does not reduce rights, nor does it create obligations for users with regard to personal data processing, that users possess based on applicable regulation and possible contractual terms about personal data protection. This Policy is a unilateral legally binding act by Iskon.

- 1. The scope of this Policy**
- 2. Principles of personal data processing**
- 3. How we collect personal data**
- 4. Types of personal data that we collect**
- 5. Purposes for which we use collected personal data**
- 6. Linking of personal data**
- 7. User consent**
- 8. Cookies**
- 9. How we protect personal data**
- 10. Where personal data is processed**
- 11. Circumstances under which we make personal data available to third parties**
- 12. User rights (correction, erasure, objection, access, restriction of processing, portability)**
- 13. Who you can contact**
- 14. Policy amendments, supplements and transitional provisions**

## **1. The scope of this Policy**

This Policy applies to all Iskon users' personal data that is collected, used or in any other way processed by Iskon directly or through its partners. Personal data is any data relating to a natural person whose identity is determined or can be determined, directly or indirectly (hereinafter: data or personal data). Data processing is any action done with personal data, for

instance, the collection, recording, storing, use, transfer of personal data or insight into personal data.

This Policy does not apply to anonymized data. Anonymous data is data that has been changed in such a way that it cannot be linked to a specific natural person or it cannot be linked without using disproportionate effort, and is thus, according to applicable regulation, not considered to be personal data. Iskon applies best European practices of data anonymization.

The Policy applies to all Iskon services and products including personal data processing. Iskon services are all services provided by Iskon. The user's last expression of consent regarding personal data processing applies to all other Iskon services that the user uses. For instance, if a user when procuring one service did not give some of the consents but has given this consent subsequently when procuring another service, it will be considered that he has given this consent. The opposite also applies, if a user when procuring the first service gave some of the consents but has subsequently when procuring an additional service denied this consent, it will be considered that he denied the concerned consent for the first service. Iskon lists users according to their user identification number (ID) and as a rule every user has a single ID that the aforementioned rules apply to. If a user has multiple IDs, consents may be collected and recorded for each of them separately.

As a rule, Iskon is the controller regarding its users' personal data within the meaning of applicable regulations about personal data protection.

The Policy primarily applies to natural persons who file a request or use Iskon services (hereinafter: Users) and/or are interested in using Iskon services (hereinafter: Potential users). However, taking into consideration the legitimate interests of users who are legal persons, the Policy does also, according to applicable regulation, appropriately apply to legal persons. In order to avoid confusion, the Policy in any event entirely applies to employees of legal persons who are Iskon users when these employees are in a contractual relationship with Iskon (e.g. the service of an individual employee's private account as part of a business user's plan).

## **2. Principles of personal data processing**

### **2.1. Trust**

We strive to be a reliable partner for Users in the protection of their data and to prove we are worthy of the trust given to us. We also strive to be completely transparent and clear with regard to the processing of Users' personal data. That, among other things, is the purpose of this Policy, especially through the active role of the User in data management. Users can always contact us with the request to change personal data concerning them or to express their intent about the purposes they want or do not want their data to be processed for.

### **2.2. Legitimacy and best practices**

When processing personal data, we act in accordance with the law, but we also try to always follow higher standards and best European practices. For instance, as part of the Deutsche Telekom Group we apply DT Group's Binding corporate rules for data protection that were approved in a special procedure by all relevant Personal data protection agencies in the EU.

### **2.3. The limited purpose of processing**

We collect and process personal data only for a specific and legal purpose and we do not further process it in a way that is not in accordance with the purpose for which it was collected, except if that is not required by law or on the basis of user consent.

### **2.4. Data minimization**

We always use only User data that is appropriate and necessary for the achievement of a certain legal purpose and no more data than that.

### **2.5. Processing in unnamed form**

Whenever it is possible and justified, we use data in unnamed form. Data in unnamed form is primarily anonymous data. However, whenever possible and justified, especially to protect personal User data, we pseudonymize personal data, i.e. we "mask" it by special procedures of pseudonymization (e.g. substitution, *hashing*, etc.) so that it cannot be linked to any individual User without the use of additional information that is stored safely and separately (e.g. the use of a key).

### **2.6. Integrity and confidentiality**

We process personal data in a safe way, including protection from unauthorized or illegal processing and accidental loss, destruction or damage (e.g. access to User personal data is restricted only to authorized persons for whom this is necessary to carry out their work, and is not permitted to other employees).

### **2.7. Personal data quality**

We attach great importance to the quality of the data we process. Personal data that we process must be accurate, complete and up-to-date so we can ensure maximum User data protection and stop potential misuse. For that reason, it is important that the User informs us about every change in data immediately or as soon as possible.

### **2.8. Limited storage time**

We store and process User data only for as long as it is necessary for the performance of a certain legitimate purpose, except if applicable regulation did not for a specific purpose provide a longer or a shorter storage time or in other cases when it is explicitly required by law. After that, data is permanently erased or made anonymous.

## **3. How we collect personal data**

Iskon collects User personal data (hereinafter: data) in these basic ways:

- 3.1. We collect data primarily directly from the User** or Potential user, in such a way that the users deliver the data themselves. The most common example for this kind of data collection is the filing of a request for a certain service or product, where the User, if he wants to use a certain service or product provides data and documents necessary for identification (e.g. name, surname, address, photocopy of a document, personal identification number, etc.). Furthermore, we collect data during Iskon's communication with the User through the customer service, websites and social networks, during the solving of objections, etc.
- 3.2. We collect data created automatically when the User uses Iskon services and/or products.** For instance, by using voice services we collect data about the dialed number, call duration, internet connection data, IP address, communication time, signalization, etc.
- 3.3. We collect data from publicly available sources** such as data from the public telephone book, publicly available services or publicly available numbering.

The prerequisite for every collection of User's personal data is the existence of an adequate legal basis based on the law.

#### 4. Types of personal data that we collect

Depending on the agreed service or product, User consent and the purpose for which data is used, Iskon is authorized to collect the kinds of User data mentioned below. In doing so, we always collect only data that is necessary for the achievement of a certain legal purpose. Also, on the request form for a service the data required to conclude an agreement is marked, whereas other data is provided voluntarily.

##### 4.1. Contractual data

In the broader sense, contractual data includes the so-called **master data**, i.e. data that the User gave for the purpose of concluding and executing an agreement (e.g. name and surname, sex, date of birth, postal address/installation address, connection address, delivery address, contact data). Contractual data also includes **data about services and products** that the User is using or was using at Iskon (e.g. the User uses the IPTV service – what data plan he uses, the existence or absence of a contractual obligation), as well as **the data about the method and history of payment for Iskon services** (e.g. debt amounts, whether a standing order is used, bank account number, preferred payment method). Contractual data includes **data from the service invoice specification** (aggregated data from the first page of the invoice, e.g. amount of calls in mobile networks, amount of calls to special numbers, etc.), but does not include a detailed list of calls (caller number, dialed number, time of call, duration of call, etc.). Contractual data does not include the content of the communication, a detailed list of calls, location data with or without traffic data, or traffic data.

##### 4.2. Usage data

Usage data in the strict sense is generated automatically through the use of specific Iskon services and products, because it is necessary for the provision of these services, and includes, among others, data on **electronic communication traffic (so-called traffic data**, e.g. date, time, communication duration, caller number and dialed number data, signalization, **approximate device location**, user device data, amount of used data traffic, IP address), data about the way

services are used, User habits when using Iskon products and services (e.g. data about the usage of self-service services, applications usage data), etc. This data does not include the content of the User's communication, which is never collected by Iskon.

**4.3. User's communication with Iskon**, e.g. recordings of User conversations with the Customer service, written and electronic communication of the User with Iskon, communication with Iskon on social networks, the User's preferred communication channels with Iskon, etc.

**4.4. Ratings data** such as data on ratings of the Iskon IPTV service, Iskon TV Player and such.

#### **4.5. Data about Potential users**

These data include master data, especially contact data (e.g. name and surname, e-mail address), but also the Potential user's interests concerning Iskon services. Generally, Iskon will record the data of those Potential users who approach Iskon with the wish to receive information and/or an offer on certain products and/or services from Iskon. Data about Potential users is erased or anonymized after one year or earlier on the Potential user's request.

## **5. Purposes for which we use collected personal data**

### **5.1. Execution of the agreement**

Iskon collects and processes user data (hereinafter: uses) primarily for the purpose of concluding and executing agreements between the User and Iskon. This especially includes the use of data for the purpose of checking the User's identity, the User's solvency, provision of the contracted service, calculation and charging of expenses, delivery of ordered products, contact with the User when necessary related to the provision of services, installation of a device, repair, resolving objections, troubleshooting, analysis and assurance of service and product quality, customer support, assistance and help with the use of products and services, as well as other actions related to the conclusion and execution of the agreement in accordance with the law.

The legal basis for data processing for these purposes is the necessity to execute the User agreement or to take steps upon the request of the User before concluding the agreement. If the User declines to give the data necessary for concluding and executing the agreement, Iskon will not be able to conclude the agreement and/or execute the individual actions related to the execution of the agreement.

### **5.2. Internal purposes**

Furthermore, Iskon uses certain User data with the sole purpose of keeping Iskon's in-house records, with the purpose of protecting legitimate interests of the User and/or Iskon. This includes, among others, the use of User's data to prevent, uncover and prosecute misuse that could harm the User or Iskon, to assure the safety of employees, of the User, of Iskon products and services, to design services and offers that will satisfy Users' needs and preferences, to assure a high-quality User experience, personalized user support, market research and analysis, optimization of the electronic communications network, etc. Telephone conversations between the User and Iskon employees can be recorded and later used with the

purpose of improvement of Iskon employee's work quality, the resolving of possible User objections, as well as the purpose of security, about which the User will be informed before the start of a conversation.

The legal basis for data processing regarding this purpose is Iskon's legitimate interest, except when this is surpassed by the interests and basic rights and freedoms requiring User data protection and/or the legal basis for the protection of the User's or another natural person's key interests. The exception are cases cited in Article 7 of this Policy when the legal basis is consent. Without the User's consent we will never process the traffic data, the content ratings data or other potential data of the User for this purpose, except when that is necessary for the prevention of misuse or the optimization, i.e. normal functioning of the electronic communications network.

### ***5.3. Publication in the public telephone book***

The User is familiar with the fact that necessary User data from the electronic communication services agreement, namely, the name, surname, telephone number and address, will be published in Iskon's public telephone book, as well as in other operators' telephone books to which Iskon is legally required to deliver the data. The public telephone book is available in electronic and/or printed form and/or through the user number information provision service. The User has the right to ask, free of charge, for the User's data not to be entered into the telephone book and has the right to a free check and correction of the data in the telephone book.

The legal basis for data processing for this purpose is compliance with Iskon's legal obligations (Iskon's legal obligation according to Article 47 of the Electronic Telecommunications Act).

### ***5.4. Direct promotion of services and products***

Iskon can also use all of the User's contact data to send promotional information about all **Iskon services and products** through all promotional channels, unless the User decides otherwise. For the User to be able to receive information in accordance with his preferences and habits, it is necessary for Iskon to use certain User data to create personalized promotional information and offers for the User. The User can at any moment opt-out of receiving promotional information. In this case the User's data will cease to be processed for the purpose of direct promotion. Iskon will send the User promotional activities about **third-party services and products** (partners) only with the User's consent. A list of third parties is available at any time on the Iskon website [www.iskon.hr](http://www.iskon.hr)

The legal basis for data processing for this purpose is Iskon's legitimate interest, except when this is surpassed by the interests and basic rights and freedoms requiring User data protection. The exception are cases cited in Article 7 of this Policy when the legal basis is consent. Without the User's consent we will never process the traffic data, the content ratings data or other potential data of the User for the purpose of promoting Iskon services and products.

### ***5.5. For the purpose of meeting legal obligations***

On written request based on applicable regulation, Iskon has the obligation to send or enable access to certain User's personal data to competent national authorities (e.g. courts, police, HAKOM: Croatian Regulatory Authority for Network Industries, AZOP: Croatian Personal Data Protection Agency, etc.).

The legal basis for data processing for these purposes is the fulfilment of Iskon's obligations (Iskon's legal obligations, e.g. data retention obligation in Article 109 of the Electronic Telecommunications Act).

## 6. Linking of personal data

When needed, we link the User's personal data linked to a certain Iskon service or product with personal data of the same user linked with other services and products, for the above-mentioned purposes in compliance with the mentioned legal basis (5) in order to acquire more precise information about the needs and habits of the User and to ultimately provide the User with optimal customer support, service and/or product.

When needed, we process the User's personal data together with other users' data. However, this kind of processing is as a rule based on completely anonymous data or the User's explicit consent for the processing of certain types of data (e.g. traffic data), and only exceptionally on Iskon's legitimate interest, and even then, only if the data is pseudonymized.

When concluding agreements, Iskon, while processing User data, creates a so-called User profile with regard to the capability of the User to settle his future obligations, and based on this decides whether to conclude the agreement or to ask for additional payment guarantees for the purpose of concluding the agreement, all in accordance with special regulation (5.1).

## 7. User consent

User consent is the freely given, specific, informed and unambiguous expression of the User's wish, by which the User through a statement or clear affirmative action gives his consent for the processing of his personal data for a specific purpose (so-called *opt-in*). Consent can be given by a written statement or in some other appropriate way. **Without the User's consent:**

- We will never use the following User data for a purpose other than the execution of the agreement, i.e. the providing of services, preventing misuse, normal functioning of the network or fulfilling Iskon's legal obligations, and especially not for the purpose of direct promotion: User's **traffic data** (4.2), **ratings data** for specific content (4.4) and possible other data for which by applicable regulation or an Iskon decision User consent is required, because of special data sensitivity or processing method;
- We will never send the User **third-party promotional messages**;
- We will never process User data in other cases when according to applicable regulation consent is required.

The User manages the declarations of his will with regard to the use of his data depending on his needs and interests. For that purpose, we give the User the possibility to give or deny his consent at any time, through a simple and free method, through various communication channels (e.g. by calling Customer service, by using the *online* interface, at a retail store, etc.).

## 8. Cookies

In order to give Users and visitors the best possible functionalities and the best possible content when visiting our Iskon website or our partners' websites, and in order to create services and offers that satisfy the needs and preferences of Users, we use cookies and/or other usual techniques (hereinafter: cookies) that collect certain User data (e.g. the IP address from which the website has been accessed, connection time, etc.). Detailed information about cookies used by a certain website are sent to the User at the moment of his/her first visit to the website. Based on this information, the User gives or denies the website his consent for the use of cookies. Cookie settings can always be changed in the web browser. Iskon is not responsible for cookies from other websites that are not owned by Iskon. We will link information acquired about the User through cookies with other data about the User to gain a better understanding of the User and to provide a better User experience, but only on the basis of consent.

### Social networks

A User's personal data are made public on social networks by Iskon only with the User's consent. Personal data is published on social networks only when competitions are organized through social networks. If the User wants to take part in a competition, he will be provided with information about the terms and conditions of personal data used when participating in the competition. This personal data will not be used for other purposes. The type of personal data collected for the purpose of organizing competitions represents a minimal data set necessary to organize any competition. Acceptance of the terms and conditions of participation is the prerequisite for the use of personal data for the above-defined purpose. The User can revoke his consent for participation in the competition at any moment and the data he provided will be erased.

## 9. How we protect personal data

We use various technical and organizational measures to protect User data from unauthorized access by persons inside and outside Iskon, changes, loss, theft and any other data breach and misuse in accordance with best European practice. These measures include, among others, the following:

- our services and products, before we offer them to Users, comply with security requirements and requirements of data protection (so-called *privacy by design* and *security by design*);
- best practice of data anonymization;
- conclusion of agreements about User's personal data protection with all subcontractors;
- implementation of all protection measures on systems where User data is stored;



- regular controls of security measures and personal data protection measures;
- continuous education of employees;
- special organizational units inside Iskon deal only with User data protection and security, as well as the office of the personal data protection officer.

## **10. Where personal data is processed**

As a rule, we process User personal data in the Republic of Croatia. As an exception, we process data in other countries (e.g. when providing a certain service or part of a service that includes personal data processing by a subcontractor from another country), as a rule in European Union Member States. As an exception, we process data in other countries, but always assuring that adequate personal data protection is provided, as a minimum to the level of personal data protection in the Republic of Croatia (e.g. by implementing the so-called *EU Standard Contractual Clauses for Processors in Third Countries*)

## **11. Circumstances under which we make personal data available to third parties**

User data is extremely important to Iskon. Iskon does not sell Users' personal data to anyone. Iskon does not share or exchange User data with other legal or natural persons (hereinafter: persons), except in the following cases:

- a) when there is a legal obligation or a legally-based explicit authorization (e.g. based on a court's request);
- b) when we hire another person as a subcontractor, i.e. processor (e.g. for invoice printing and delivery, market research, system maintenance, checking of solvency, forwarding to a debt collection agency for the purpose of debt collection). It is important to emphasize that subcontractors act exclusively on Iskon's order and that Iskon ensures that all User data protection measures are met, as if this work were done by Iskon itself.
- c) when it is necessary to forward data to third persons for the purpose of executing an agreement with the User (e.g. telephone number transfer);
- d) when the other person is the User contract holder for services that are used by the User (e.g. the holder of a telephone connection in a family plan or an employer as holder of a business plan);
- e) assignments, i.e. assignment of claims to third persons in accordance with Article 80 of the Law on Obligatory Relations;
- f) based on User consent.

## **12. User rights (correction, erasure, objection, access, restriction of processing, portability)**

In conjunction with the User's active role regarding the management of consents, i.e. the User's right to give or revoke his consent at any moment (points 7 and 8), the User also has the following active roles, all in accordance with applicable regulation:

- a) Right to object: The User has the right to ask that the delivery of promotional information about Iskon services and products be terminated at any moment (5.4). The User also has the right to object to every other instance of User data processing based on Iskon's so-called legitimate interest, including the making of profiles based on these regulations (5.4 and 6) (so-called *opt-out*). In that case, Iskon will not process data for the said purposes, except when the law requires differently.
- b) Data safekeeping obligation: The User has the obligation to keep secret and with due caution all identification labels assigned to him by Iskon (e.g. invoice reference number, username, password, etc.) because all actions taken with the User's identifications labels will be considered actions by the User himself. The User also has the obligation to change his password or other access data as soon as he suspects an unauthorized use of his data and must without hesitation inform Iskon if he suspects misuse of his identification labels.
- c) The right of access: The User has the right to be informed whether his User personal data is being processed, and in the event that such personal data is processed, to gain access to this data and the information about the purpose of the processing, the categories of personal data being processed, the recipients or categories of recipients, about the foreseen period in which the data will be stored or other criteria used to determine this period, the existence of User rights, the existence of automatized decision-making including the making of profiles, as well as information about the logic of the processing, the importance and foreseen consequences of the processing, protective measures if data is transferred to so-called third countries.
- d) Right to erasure: The User has the right to secure an erasure of personal data related to him without unnecessary delay and under conditions cited in applicable data protection regulation.
- e) Right to rectification: The User has the right to procure the rectification of incorrect personal data which are related to the User.
- f) Right to data portability: The User has the right to be given User related personal data that he has provided to Iskon, in a structured, commonly used and machine-readable format and has the right to transfer them to another controller if the processing is based on consent or agreement and is carried out automatically. If technically feasible, the User has the right to a direct transfer from Iskon to the other controller.
- g) The right not to be entered into the public telephone book: The User has the right to request at any moment that User data are not entered into a public telephone book and Iskon will comply with this request.

### **13. Who you can contact**

The User can exercise the rights from Article 12 by submitting an appropriate request through the website [moj.iskon.hr](http://moj.iskon.hr). Exceptionally, in cases when the User cannot reach the website, he

can send the application to the e-mail address [prijava@iskon.hr](mailto:prijava@iskon.hr) or the postal address Iskon Internet d.d., Garićgradska 18, 10000 Zagreb or any other way that Iskon makes available to the User, depending on the type of request.

If the User suspects a breach of his personal data, he must report his suspicion in writing to the Iskon Customer service to the e-mail address [prijava@iskon.hr](mailto:prijava@iskon.hr) or the postal address Iskon Internet d.d., Garićgradska 18, 10000 Zagreb.

Should the User have any questions concerning this Policy and/or personal data protection at Iskon, he can send a query to the e-mail address [prijava@iskon.hr](mailto:prijava@iskon.hr) or the e-mail address of the personal data protection commissioner at [osobni.podaci@iskon.hr](mailto:osobni.podaci@iskon.hr)

The User also has the right to file an objection to the Personal Data Protection Agency.

#### **14. The DT Group's binding corporate rules for data protection**

Additional information about the way Iskon processes and protects the User's personal data is available in the DT Group's binding corporate rules for data protection published on the Iskon website.

#### **15. Policy amendments, supplements and transitional provisions**

This Policy becomes effective and applicable to Users on 25 May 2018 and will be available on the website and at the Iskon business premises. Users will be informed in a timely fashion about possible amendments to the Policy, including through announcements on the Iskon website.