

# DOHOP

## Privacy Policy

### 1 INTRODUCTION

At Dohop.ehf., ID No. 480904-3030, Nóatún 17, 105 Reykjavík (“Dohop”, “we”, “us”, “our”) we strive to protect personal data of individuals and to respect their rights. Dohop operates worldwide and has business relationships with different entities, such as airlines and other transport carriers, airports, financial institutions, and other businesses, to provide convenient and efficient services globally for consumers and businesses. To provide our services, we may process information that can be used to personally identify an individual (“Data Subject”, “you”, “your”), directly or indirectly, from the information alone or in combination with additional data (“Personal Data”).

This Privacy Policy expresses our commitment to data privacy and explains how we collect and handle your information while operating our business. Terms not otherwise defined in this Privacy Policy will have the same meaning as set forth in the (EU) 2016/697 General Data Protection Regulation (“GDPR”).

### 2 DOHOP’S PRIVACY PRINCIPLES

At Dohop, the guiding principle in all of our operations is that your information belongs to you! Therefore, when operating and managing our business, building and improving our solutions, products and services and handling Personal Data in general, we carefully analyse what type of information is needed and limit the processing to the data that is considered necessary and relevant. Where feasible and appropriate, we consider using anonymous, pseudonymized or aggregate data instead of Personal Data, and we delete or anonymize the data when we no longer need it for business or legal purposes. Access to Personal Data is limited to those who reasonably require it to fulfil their responsibilities. Dohop uses appropriate security safeguards and appropriate technical and organizational measures to protect the Personal Data processed and does not disclose Personal Data except as set out in our policies or as required or otherwise permitted by contract or applicable law.

All our processing activities take place in accordance with the Icelandic Act No. 90/2018 on Data Protection and Processing of Personal Data (“the Icelandic Data Protection Act”) and the GDPR in a fair and lawful manner. The Personal Data is only processed for specified, explicit and legitimate purposes. When Dohop determines the purpose, means and conditions of processing Personal Data, we are the decision-maker, generally referred to as “Data Controller”. Where we act as a service provider on behalf of others, typically our clients or business partners, we are a “Data Processor”. When acting as a Data Processor, Dohop processes Personal Data in accordance with its written agreements or instructions from the relevant Data Controller in compliance with applicable laws and policies. Dohop does not assume any responsibility for compliance requirements that apply to its client’s or partner’s business that does not apply to Dohop.

Individuals can always refuse to provide Dohop with Personal Data when requested. However, please note that if you choose not to provide the information necessary, we may not be able to accomplish some or all of the purposes outlined in this Privacy Policy. Additionally, if you provide us with the Personal Data of another person, you are responsible for ensuring that such person is made aware of the information contained in this Privacy Policy and that the person has given you his/her consent for sharing the information with Dohop.

### 3 HOW MAY WE PROCESS YOUR PERSONAL DATA?

Our legal basis for processing Personal Data will depend on the type of data concerned and the specific context in which we process it. However, we only process your information where you’ve given us your consent, where it is necessary to deliver the services you’ve requested, where it’s necessary to exercise or comply with legal rights or obligations, or for normal business purposes as set out in this Privacy Policy.

- When visiting Dohop’s websites ([www.dohop.is](http://www.dohop.is) and [www.dohop.com](http://www.dohop.com)), the only Personal Data that is processed by us is anonymised and/or aggregated data that is automatically collected from your browser by cookies and other storage technologies. You have the right to accept or restrict the use of cookies or even completely prevent them from being set. For the avoidance of doubt, if you use Dohop’s travel search engine to make a booking, that booking is made directly with the third-party vendor named on the booking page, and the vendors’ terms and privacy policy applies to such booking.
- When visiting our client’s website, which is based on our software solution (“Partner Microsite”), we may process anonymised and/or aggregated data that is automatically collected from your browser by cookies and other storage technologies. If you book an itinerary on our Partner Microsite, we, as Data Processors, may process your Personal Data on behalf of and under the direction of our Partners, who are Data Controllers of such data provided by you. For the avoidance of doubt, our Partners, as Data Controllers, are responsible for complying with any regulation or laws that

require providing notice, disclosure, and/or obtaining consent prior to collecting their customers' Personal Data on the Microsite. Where Dohop Connection Service forms a part of the booking process, we may also process Personal Data for our own purpose as Data Controllers.

- Dohop may use Personal Data for direct marketing in accordance with laws and regulations if a Data Subject participates in competitions, instructions or recommendations or requests to be notified of Dohop's services, newsletters, or offers via email, e.g., by registering their e-mail in a mailing list.
- When operating and managing our business, we may also process Personal Data of our Personnel and personnel of former, actual or potential clients, business partners and other business contacts, suppliers, vendors, shareholders and independent contractors etc.

#### **4 WHOSE INFORMATION DO WE PROCESS?**

We may process and transfer Personal Data of our website users and in relation to complainants, correspondents and enquirers; customers and prospective customers; our prospective, actual and former clients (including employees, officers, agents, consultants and other professional experts) and their customers; individuals attending our events; other persons as appropriate to conduct business such as vendors, suppliers, contractors, shareholders, authorised signatories for the customer in the case of legal entities and other registered individuals and of our employees, consultants, agents, other professional experts and applicants ("Personnel"), former Personnel, dependants and beneficiaries of Personnel and former Personnel.

#### **5 WHAT INFORMATION DO WE PROCESS?**

**Customer data:** This may include basic booking and payment data provided by our customers such as name, address, gender, date of birth, e-mail address, telephone number, card number, expiry date, cvc, contact, data in relation to advertising and marketing preferences, other Personal Data in relation to communications, complaints and enquiries handling.

**Website visitors' data:** This may include tracking data from cookies and other technology such as your anonymized or shortened IP address, your device type, domain, browser type, language, operating system, country, time zone, previously visited websites, or information about your interaction with our websites such as click behaviour, purchases and other preferences expressed through selections/viewing etc., that is automatically collected from the Data Subject's browser/device when the individual visits our web properties and/or websites based on our platform/solutions. Please visit our Cookie Policy for further information in relation to this.

**Client's and prospects data:** This may include data of the Personnel of former, actual or potential clients such as name, all types of contact details (such as job title, e-mail, phone number, place of work address), Personal Data related to events and/or management of business relationships, and data of the client's customers such as; basic booking and payment data provided by our customers such as name, address, gender, date of birth, e-mail address, telephone number, card number, expiry date, cvc, and other Personal Data in relation to communications, complaints and enquiries handling.

**Vendors, service providers, suppliers, shareholders, independent contractors and other business contact's data:** This may include data of former or current Personnel of such third parties, such as: name, all types of contact details (such as job title, e-mail, phone number, place of work address), Personal Data related to events and/or management of business relationships, and information derived from the deployment and use of information systems and tools from third parties etc.

**Employment Data:** This may include Personal Data of our employees, consultants, and applicants ("Personnel"), former Personnel, dependants and beneficiaries of former, actual or potential Personnel in connection with their working relationship or application for employment or engagement, such as names, addresses, date of birth, national identification or other social security numbers, work location, job title, details of residency or work permit, education information and professional or employment-related information, financial information for compensation, payroll and benefits (e.g., salary and expenses information, benefits, banking information, trade union membership, pension records), information on leaves of absences, Personnel shareholdings, next of kin and emergency contact information, talent management information (e.g. background checks, staff development records, attendance records, disciplinary procedures) recruitment information, information in relation to the termination of the employment or service contract, photograph, and images/footage captured/recorded on CCTV and/or other related security/monitoring systems. Where the Personnel is provided with access to Dohop's systems, Dohop may collect information required to access such systems and applications such as System ID, LAN ID, e-mail account, and internet or other electronic network activity information, including access logs, activity logs. Where travel outside of a normal place of work is required for undertaking any of Personnel's duties Dohop may collect passport data. The aforementioned data can be collected from a number of sources e.g., provided by the Data Subject itself, third parties such as former employers, public sources/databases, automated means etc., and/or from records/documents created by us.

**Sensitive data:** Dohop only processes Personal Data that may be considered sensitive in relation to Dohop's Personnel where the processing is necessary for the purpose of complying with legal obligations according to national applicable law and regulations or with your consent. This may include trade union membership, social security numbers and other national identifier numbers, criminal record data, dietary requirements or allergies. Dohop will always treat sensitive Personal Data with more scrutiny as such data requires additional privacy, legal and security safeguards.

**Other individuals' Personal Data:** This may include data from public relations e.g. correspondence between you and us when it is sent to a dedicated mailbox or via other electronic communications means (including digital communication channels) such as e-mail address, name, PNR/Reference, address, phone number, workplace and job title; this may include Personal Data such as e-mail addresses that the Data Subject provides to Dohop when signing up for a mailing list to receive a newsletter, offers or other marketing communication related to our business; this may include audio-visual materials e.g., images/footage captured/recorded captured during marketing/public filming events/sessions/workshops; this may include Personal Data as may be required to process in response to a lawful request from a court or government agency or to otherwise comply with applicable law or compulsory process and/or other purposes required or permitted by law or regulations; this may include data relating to mergers, ventures and acquisitions such as management and employment information.

## **6 WHY DO WE PROCESS THE INFORMATION? (PURPOSE)**

Dohop collects, transfers, holds and processes Personal Data only for explicit and legitimate purposes, which are clearly explained to individuals when we process their data. We will not use your Personal Data for purposes that are incompatible with the purposes of which you have been informed unless it is required or authorized by law or it is in your own vital interest to do so. The processing undertaken by Dohop in relation to the categories of Data Subjects set out above includes processing for carrying out the following lawful business activities:

- Operating and managing our business; Business and market development and planning purposes;
- For administrative functions; Employee recruitment, Personnel management and administration, payroll and administration of Personnel benefits and other purposes as may be required or authorised by applicable law; Facilities management purposes;
- For advertising, marketing and public relation purposes;
- Providing customer support and other communications;
- To provide, operate, improve, customise and support our services and products;
- Conducting business and fulfilling contracts with our customers, clients, partners, vendors, suppliers and contractors;
- Fulfilling payment transactions for our and our client's products and services;
- Client, supplier and business partner management;
- Building and managing external relationships;
- Improving the functioning of our website/web property and networks; Maintaining technology infrastructure and support, database management, maintaining security, fraud prevention or investigation and/or other risk management purposes; Performing data analytics i.e. applying analytics to business operation and data to describe, predict and improve business performance within Dohop and/or to provide a better user experience; Monitoring the use of our systems; For identification and information verification purposes;
- Compliance, audit and insurance purposes, including supplier and customer due diligence: internal and external investigations including liaison with law enforcement/ other government agencies where required to do so by law; litigation management;
- To seek legal advice or seek to protect ourselves in the context of litigation and other disputes;
- To facilitate mergers and acquisitions, including due diligence and information relevant to potential ventures, joint ventures, mergers and acquisitions;
- In response to a lawful request from a court or government agency or to otherwise comply with applicable law or compulsory process; In emergencies where the health or safety of a person is endangered; Complying with legal requirements, as obligated and/or authorized by the Icelandic Data Protection Act and other applicable law and/or other purposes required or permitted by law or regulations;
- Other purposes that are not incompatible with the ones listed above or other purposes required and/or permitted by law or regulations.

## **7 SHARING OF PERSONAL DATA TO THIRD PARTIES**

You share your information as you use and purchase our products and services, and we may share your information to help us operate, provide, improve, understand, customise and support our services. Dohop only provides its service providers, e.g., outside professional advisors, vendors, suppliers, partners and other third parties (also known as Data Processors), with such Personal Data as is deemed necessary to achieve this objective. Where Data Processors are given access to Personal Data, Dohop safeguards confidentiality and ensures that the data in question is deleted once processing is completed. Dohop does not and never will, under any circumstances, sell or lease Personal Data to third parties.

Dohop does not share Personal Data with a third party except with permission or in accordance with the provisions of business agreements when the third party is considered to be a service provider or contractor of Dohop and then solely for the purpose of providing our services or products. We strive to select reliable third parties service providers to perform services on our behalf, including to facilitate payments, to help us provide, protect and improve our websites and optimize the user experience, to provide specific services from airports when requested, to provide customer support etc. When we share information as Data Controllers with third-party service providers in this capacity, we enter into contractual arrangements with them to ensure that they use your information on our behalf in accordance with our instructions and terms.

Dohop may also share information about you for legal, safety and security reasons, e.g. if we reasonably believe that disclosing the information is needed to; comply with any valid legal processing, governmental requests or applicable law, rule or regulation; investigate, remedy or enforce potential terms of service and community guidelines violations; protect the rights, property or safety of us, our users or other; or detect and resolve any fraud or security concerns. Additionally, if Dohop gets involved in a merger, asset sale, financing, liquidation or bankruptcy or acquisition of all or some portion of our business to another company, we may share your information with that company before and after the transaction closes.

## **8 THIRD PARTY CONTENT AND INTEGRATIONS**

Dohop's websites and/or our Partner's Microsite may contain third-party content and integrations, including third-party website links and other features and functionalities. We can only speak for ourselves, so this Privacy Policy doesn't cover the collection or use of your information by the majority of the airlines and other transport carriers or third parties that may link to Dohop, such as Facebook, Google, Apple, Microsoft, LinkedIn, Youtube, etc. If you interact with such third-party services or products that are linked through our services, the provider of those services or products may receive information about you that you grant them access to. Dohop is not in any way responsible for the privacy policy or actions of those third parties, and their own terms and privacy policies will apply. Therefore, as always, we encourage you to review the privacy policies and cookie information of every third-party service that you visit or use, including those third parties you interact with through our services.

## **9 INTERNATIONAL DATA TRANSFER**

Data transfer is an international transfer of Personal Data to another party or making the data accessible by it, where neither the sender nor the receiver is a Data Subject. Under Chapter V of the GDPR, Data Controllers and Data Processors cannot transfer Personal Data outside of the European Economic Area (to so-called "Third Countries") for any type of processing unless adequate levels of data protection can be ensured.

As Dohop operates globally, with users and businesses around the world, we may need to share information we collect globally, both internally within Dohop's entities and where the data centres we rely on are located, and externally with our third-party service providers, professional advisors, public and governmental authorities and/or third parties (including our clients and business partners) as relevant to the categories and purposes identified in this Privacy Policy. These transfers are necessary and essential to enable us to provide the relevant services and products and/or operate our businesses. Dohop is committed to ensuring adequate protection for the transfer of Personal Data. Therefore, Personal Data may not, and will not, be transferred or transmitted to, or stored and processed in, a Third Country unless an adequate transfer mechanism is in place prior to the transfer. Such transfer shall therefore either be based on an adequacy decision from the European Commission where they recognise that certain countries and territories outside the European Economic Area ensure an adequate level of protection for personal information or shall be governed by the standard contractual clauses approved by the European Commission ("EU SCCs"). We also make sure that any third party we share information with have an adequate transfer mechanism in place as well prior to sharing.

## **10 HOW TO EXERCISE YOUR RIGHTS**

Individuals have rights in relation to their Personal Data processed by Dohop. These rights include the right to be informed, to access, rectify, port, and erase your information, as well as the right to restrict and object to certain processing of your information. We respect these rights and have, as Data Controllers, processes in place to recognize and respond to individuals wishing to exercise these rights. We encourage you to exercise your rights by contacting Dohop's Data Privacy Team at: [gdpr@dohop.com](mailto:gdpr@dohop.com); or by sending a letter to Dohop ehf., Noatun 17, 105 Reykjavik, Iceland, and completing a formal individual rights request. Please be aware, however, that there are various restrictions to the above rights, so Dohop must assess each request individually. All requests are answered as promptly as possible.

Additionally, Dohop recognizes and honours the Data Subject's right to object to direct marketing by Dohop by providing the Data Subject with the opportunity to opt-out of marketing. Additionally, when Dohop processes your information based on your consent, you have the right to withdraw your consent at any time without affecting the lawfulness of processing based on such consent before the consent is withdrawn. Of course, if you do that, i.e., withdraw your consent, we might not be able to provide you with certain services or products.

An automated decision is when a decision is made about an individual using technology specifically designed for decision-making purposes; this includes profiling individuals. According to the GDPR, an individual has the right not to be subjected to solely automated decisions which produce legal effects or otherwise similarly significantly affect them. Currently, this does not apply to our processing, but if that changes at any point, Dohop will comply with the relevant requirements when making automated decisions and will institute any additional safeguards to protect individuals' rights where required to do so.

We also want to make you aware of your right to lodge a complaint with Dohop's lead supervisory authority, Persónuvernd, or any other competent data protection supervisory authority at any time at: [postur@personuvernd.is](mailto:postur@personuvernd.is) or by letter to: Persónuvernd, Rauðarárstígur 10, 105 Reykjavík, Iceland. Individuals also have the right to make a claim against Dohop before the competent court, but we encourage and welcome individuals to come to Dohop first to seek resolution of any complaint.

## **11 RETENTION OF YOUR INFORMATION**

Dohop does not store data in a form which permits the identification of Data Subjects for longer than is necessary for the purposes for which the Personal Data are processed. Personal Data is only stored for the duration of business relationships, the existence of consent, as long as required by law or in respect of other legitimate interests of the company as Data Controllers and for an apposite reason. An apposite reason is considered to exist if the data is still being processed in accordance with the original purpose of its collection. As a result of the above, the storage periods are determined case-by-case and different retention periods may apply depending on the processing purpose, type, and nature of Personal Data. We maintain specific retention policies and procedures so that Personal Data is deleted after a reasonable time according to the purpose they were obtained or in accordance with legal/regulatory specified retention requirements. When Dohop no longer needs to retain, there are procedures for the secure disposal of Personal Data.

## **12 SECURITY OF YOUR INFORMATION**

Dohop strives to safeguard Personal Data and considers data privacy as an integral component of the design, development, operation and management of new projects, tools, applications, internal services and offerings which process Personal Data. Appropriate technical, organizational, administrative and physical security measures have been employed to ensure general data security and compliance with the principles of the processing of Personal Data. These measures are intended, first and foremost, to protect Personal Data against accidental loss or alteration and against unauthorized access, copying, use or disclosure. Other measures are aimed at ensuring, by default, that Personal Data collected and used as necessary for specific purposes is not stored longer than necessary and is not made available to unauthorized parties. Dohop undertakes regular privacy compliance auditing to ensure that necessary precautions are always taken.

Dohop has policies, procedures and protocols in place for managing and responding to data security breaches. In the event of suspected or known breaches, where there may have been inappropriate access to or unauthorized disclosure of Personal Data, defined internal procedures are activated. As part of our incident response processes, there are procedures that ensure that data security breaches are reported in an appropriate manner within the time limits required by law and regulations. Dohop maintains a record of data security breaches which includes details about the breach incident, the effect (if any) on whom it may concern, and remedial action necessary to resolve the breach.

To protect Personal Data, Dohop and its employees comply with the commitments which are appropriately reflected in this Privacy Policy (and any related policies, controls, procedures and guidance) and by acting with integrity. We limit access to and use of Personal Data to those who reasonably require it to fulfil their responsibilities and ensure they understand how data privacy impacts their role and their use of Personal Data.

## **13 PROTECTION OF PRIVACY FOR CHILDREN**

Dohop's services are intended for the general public, and data on children under the age of 13 are not collected deliberately. If a child under the age of 13 submits Personal Data to Dohop, we will not process the data unless with the consent of a guardian. Guardian who becomes aware of a child submitting Personal Data to the company without the guardian's consent is encouraged to contact Dohop. If we become aware of data on children that have been submitted without the consent of a guardian, we will immediately delete such data.

## **14 POLICY REVIEW AND FURTHER INFORMATION**

We may update this Privacy Policy from time to time and we encourage you to review it periodically. An updated policy takes effect when it is made available on our public websites and private intranet site. Any new version shall be indicated by means of a version date.

This document is a summary of key information in relation to Dohop's processing activities and sets out the overall approach to privacy and data protection. Further detailed information about Dohop's expectations and practices pertaining to Personal Data can be addressed to Dohop's Data Privacy Officer. Additionally, if you still have any questions, concerns or a complaint about Dohop's compliance with this Privacy Policy, or applicable laws and regulations, you are encouraged to contact us at [gdpr@dohop.com](mailto:gdpr@dohop.com) or write to us by mail at Dohop.ehf., Nóatún 17, 105 Reykjavík, Iceland. We will work with you to attempt to resolve any issue to your satisfaction, but where that is not possible, you can raise the issue before the competent Data Protection Authority or bring the issue before the courts of Reykjavík, Iceland.

The policy was last revised in September 2022.