



tophotels.wien

Privacy Policy

Preamble

With the following privacy policy we would like to inform you which types of your personal data (hereinafter also abbreviated as "data") we process for which purposes and in which scope. The privacy statement applies to all processing of personal data carried out by us, both in the context of providing our services and in particular on our websites, in mobile applications and within external online presences, such as our social media profiles (hereinafter collectively referred to as "online services"). The terms used are not gender-specific.

Last Update: 15. February 2023

[Created with Datenschutz-Generator.de by Dr. jur. Thomas Schwenke](#)

Table of contents

- Preamble
- Controller
- Overview of processing operations
- Legal Bases for the Processing
- Security Precautions
- Transmission of Personal Data
- Data Processing in Third Countries
- Erasure of data
- Use of Cookies
- Provision of online services and web hosting
- Contact and Inquiry Management
- Job Application Process
- Web Analysis, Monitoring and Optimization

- Online Marketing
- Profiles in Social Networks (Social Media)
- Plugins and embedded functions and content
- Changes and Updates to the Privacy Policy
- Rights of Data Subjects

Controller

tophotels.wien (members see imprint)

info@tophotels.wien

E-mail address:

info@tophotels.wien

Legal Notice:

tophotels.wien

Overview of processing operations

The following table summarises the types of data processed, the purposes for which they are processed and the concerned data subjects.

Categories of Processed Data

- Inventory data.
- Contact data.
- Content data.
- Usage data.
- Meta, communication and process data.
- Job applicant details.
- Event Data (Facebook).

Categories of Data Subjects

- Communication partner.
- Users.
- Job applicants.

Purposes of Processing

- Provision of contractual services and customer support.
- Contact requests and communication.
- Security measures.
- Web Analytics.
- Targeting.
- Conversion tracking.
- Affiliate Tracking.
- Managing and responding to inquiries.
- Job Application Process.
- Content Delivery Network (CDN).
- Feedback.
- Marketing.
- Profiles with user-related information.
- Provision of our online services and usability.
- Information technology infrastructure.

Legal Bases for the Processing

Below you will find an overview of the legal basis of the GDPR on the basis of which we process personal data. Please note that in addition to the provisions of the GDPR, national data protection regulations may apply in your or our country of residence or domicile. If, in addition, more specific legal bases are applicable in individual cases, we will inform you of these in the data protection declaration.

- Consent (Article 6 (1) (a) GDPR) - The data subject has given consent to the processing of his or her personal data for one or more specific purposes.
- Performance of a contract and prior requests (Article 6 (1) (b) GDPR) - Performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.
- Legitimate Interests (Article 6 (1) (f) GDPR) - Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data.

- Job application process as a pre-contractual or contractual relationship (Article 6 (1)(b) GDPR) – If special categories of personal data within the meaning of Article 9 (1) GDPR (e.g. health data, such as severely handicapped status or ethnic origin) are requested from applicants within the framework of the application procedure, so that the responsible person or the person concerned can carry out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law, their processing shall be carried out in accordance with Article 9 (2)(b) GDPR , in the case of the protection of vital interests of applicants or other persons on the basis of Article 9 (2)(c) GDPR or for the purposes of preventive health care or occupational medicine, for the assessment of the employee's ability to work, for medical diagnostics, care or treatment in the health or social sector or for the administration of systems and services in the health or social sector in accordance with Article 9 (2)(d) GDPR. In the case of a communication of special categories of data based on voluntary consent, their processing is carried out on the basis of Article 9 (2)(a) GDPR.

In addition to the data protection regulations of the GDPR, national regulations apply to data protection in Austria. This includes in particular the Federal Act on the Protection of Individuals with regard to the Processing of Personal Data (Data Protection Act - DSG). In particular, the Data Protection Act contains special provisions on the right of access, rectification or cancellation, processing of special categories of personal data, processing for other purposes and transmission and automated decision making in individual cases.

Security Precautions

We take appropriate technical and organisational measures in accordance with the legal requirements, taking 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, in order to ensure a level of security appropriate to the risk.

The measures include, in particular, safeguarding the confidentiality, integrity and availability of data by controlling physical and electronic access to the data as well as access to, input, transmission, securing and separation of the data. In addition, we have established procedures to ensure that data subjects' rights are respected, that data is erased, and that we are prepared to respond to data threats rapidly.

Furthermore, we take the protection of personal data into account as early as the development or selection of hardware, software and service providers, in accordance with the principle of privacy by design and privacy by default.

TLS encryption (https): To protect your data transmitted via our online services, we use TLS encryption. You can recognize such encrypted connections by the prefix https:// in the address bar of your browser.

Transmission of Personal Data

In the context of our processing of personal data, it may happen that the data is transferred to other places, companies or persons or that it is disclosed to them. Recipients of this data may include, for example, service providers commissioned with IT tasks or providers of services and content that are embedded in a website. In such cases, the legal requirements will be respected and in particular corresponding contracts or agreements, which serve the protection of your data, will be concluded with the recipients of your data.

Data Transmission within the Group of Companies: We may transfer personal data to other companies within our group of companies or otherwise grant them access to this data. Insofar as this disclosure is for administrative purposes, the disclosure of the data is based on our legitimate business and economic interests or otherwise, if it is necessary to fulfill our contractual obligations or if the consent of the data subjects or otherwise a legal permission is present.

Data Processing in Third Countries

If we process data in a third country (i.e. outside the European Union (EU), the European Economic Area (EEA)) or the processing takes place in the context of the

use of third party services or disclosure or transfer of data to other persons, bodies or companies, this will only take place in accordance with the legal requirements. Subject to express consent or transfer required by contract or law, we process or have processed the data only in third countries with a recognised level of data protection, on the basis of special guarantees, such as a contractual obligation through so-called standard protection clauses of the EU Commission or if certifications or binding internal data protection regulations justify the processing (Article 44 to 49 GDPR, information page of the EU Commission: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection_en).

Erasure of data

The data processed by us will be erased in accordance with the statutory provisions as soon as their processing is revoked or other permissions no longer apply (e.g. if the purpose of processing this data no longer applies or they are not required for the purpose). If the data is not deleted because they are required for other and legally permissible purposes, their processing is limited to these purposes. This means that the data will be restricted and not processed for other purposes. This applies, for example, to data that must be stored for commercial or tax reasons or for which storage is necessary to assert, exercise or defend legal claims or to protect the rights of another natural or legal person. Our further information on individual processing operations may also contain additional and specific information on data retention and erasure applicable to the respective processing operations.

Use of Cookies

Cookies are small text files or other data records that store information on end devices and read information from the end devices. For example, to store the login status in a user account, the contents of a shopping cart in an e-shop, the contents accessed or the functions used. Cookies can also be used for various purposes, e.g.

for purposes of functionality, security and convenience of online offers as well as the creation of analyses of visitor flows.

Information on consent: We use cookies in accordance with the statutory provisions. Therefore, we obtain prior consent from users, except when it is not required by law. In particular, consent is not required if the storage and reading of information, including cookies, is strictly necessary in order to provide an information society service explicitly requested by the subscriber or user. The revocable consent will be clearly communicated to the user and will contain the information on the respective cookie use.

Information on legal bases under data protection law: The legal basis under data protection law on which we process users' personal data with the use of cookies depends on whether we ask users for consent. If users consent, the legal basis for processing their data is their declared consent. Otherwise, the data processed with the help of cookies is processed on the basis of our legitimate interests (e.g. in a business operation of our online services and improvement of its usability) or, if this is done in the context of the fulfillment of our contractual obligations, if the use of cookies is necessary to fulfill our contractual obligations. For which purposes the cookies are processed by us, we do clarify in the course of this privacy policy or in the context of our consent and processing procedures.

Retention period: With regard to the retention period, a distinction is drawn between the following types of cookies:

- Temporary cookies (also known as "session cookies"): Temporary cookies are deleted at the latest after a user has left an online service and closed his or her end device (i.e. browser or mobile application).
- Permanent cookies: Permanent cookies remain stored even after the terminal device is closed. For example, the login status can be saved, or preferred content can be displayed directly when the user visits a website again. Likewise, user data collected with the help of cookies can be used for reach measurement. Unless we provide users with explicit information about the type and storage duration of cookies (e.g., as part of obtaining consent), users should assume that cookies are permanent and that the storage period can be up to two years.

General information on revocation and objection (opt-out): Users can revoke the consent they have given at any time and also file an objection to processing in accordance with the legal requirements in Article 21 GDPR. Users can also declare their objection by means of the settings of their browser, e.g. by deactivating the use of cookies (whereby this may also limit the functionality of our online services). An objection to the use of cookies for online marketing purposes, can also be declared via the websites <https://optout.aboutads.info> and <https://www.youronlinechoices.com/>.

Further information on processing methods, procedures and services used:

- Processing Cookie Data on the Basis of Consent: : We use a cookie management solution in which users' consent to the use of cookies, or the procedures and providers mentioned in the cookie management solution, can be obtained, managed and revoked by the users. The declaration of consent is stored so that it does not have to be retrieved again and the consent can be proven in accordance with the legal obligation. Storage can take place server-sided and/or in a cookie (so-called opt-out cookie or with the aid of comparable technologies) in order to be able to assign the consent to a user or and/or his/her device. Subject to individual details of the providers of cookie management services, the following information applies: The duration of the storage of the consent can be up to two years. In this case, a pseudonymous user identifier is formed and stored with the date/time of consent, information on the scope of the consent (e.g. which categories of cookies and/or service providers) as well as the browser, system and used end device.

Provision of online services and web hosting

We process user data in order to be able to provide them with our online services. For this purpose, we process the IP address of the user, which is necessary to transmit the content and functions of our online services to the user's browser or terminal device.

- Processed data types: Usage data (e.g. websites visited, interest in content, access times); Meta, communication and process data (e.g. IP addresses, time

information, identification numbers, consent status); Content data (e.g. text input, photographs, videos).

- Data subjects: Users (e.g. website visitors, users of online services).
- Purposes of Processing: Provision of our online services and usability; Information technology infrastructure (Operation and provision of information systems and technical devices, such as computers, servers, etc.); Security measures; Content Delivery Network (CDN).
- Legal Basis: Legitimate Interests (Article 6 (1) (f) GDPR).

Further information on processing methods, procedures and services used:

- Provision of online offer on rented hosting space: : For the provision of our online services, we use storage space, computing capacity and software that we rent or otherwise obtain from a corresponding server provider (also referred to as a "web hoster"); Legal Basis: Legitimate Interests (Article 6 (1) (f) GDPR).
- Collection of Access Data and Log Files: : The access to our online services is logged in the form of so-called "server log files". Server log files may include the address and name of the web pages and files accessed, the date and time of access, data volumes transferred, notification of successful access, browser type and version, the user's operating system, referrer URL (the previously visited page) and, as a general rule, IP addresses and the requesting provider. The server log files can be used for security purposes, e.g. to avoid overloading the servers (especially in the case of abusive attacks, so-called DDoS attacks) and to ensure the stability and optimal load balancing of the servers; Legal Basis: Legitimate Interests (Article 6 (1) (f) GDPR); Retention period: Log file information is stored for a maximum period of 30 days and then deleted or anonymized. Data, the further storage of which is necessary for evidence purposes, are excluded from deletion until the respective incident has been finally clarified.
- E-mail Sending and Hosting: : The web hosting services we use also include sending, receiving and storing e-mails. For these purposes, the addresses of the recipients and senders, as well as other information relating to the sending of e-mails (e.g. the providers involved) and the contents of the respective e-mails are processed. The above data may also be processed for

SPAM detection purposes. Please note that e-mails on the Internet are generally not sent in encrypted form. As a rule, e-mails are encrypted during transport, but not on the servers from which they are sent and received (unless a so-called end-to-end encryption method is used). We can therefore accept no responsibility for the transmission path of e-mails between the sender and reception on our server; Legal Basis: Legitimate Interests (Article 6 (1) (f) GDPR).

- Cloudflare: : Content-Delivery-Network (CDN) – service with whose help contents of our online services, in particular large media files, such as graphics or scripts, can be delivered faster and more securely with the help of regionally distributed servers connected via the Internet; Service provider: Cloudflare, Inc., 101 Townsend St, San Francisco, CA 94107, USA; Legal Basis: Legitimate Interests (Article 6 (1) (f) GDPR); Website: <https://www.cloudflare.com>; Privacy Policy: <https://www.cloudflare.com/privacypolicy/>; Data Processing Agreement: <https://www.cloudflare.com/cloudflare-customer-dpa>; Standard Contractual Clauses (Safeguarding the level of data protection when processing data in third countries): <https://www.cloudflare.com/cloudflare-customer-scc>.
- Internex: : Services in the field of the provision of information technology infrastructure and related services (e.g. storage space and/or computing capacities); Service provider: internex GmbH, Firmensitz Lagerstraße 15, 3950 Gmünd, Austria; Legal Basis: Legitimate Interests (Article 6 (1) (f) GDPR); Website: <https://www.internex.at>; Privacy Policy: <https://www.internex.at/de/datenschutz-erklaerung/>.

Contact and Inquiry Management

When contacting us (e.g. via mail, contact form, e-mail, telephone or via social media) as well as in the context of existing user and business relationships, the information of the inquiring persons is processed to the extent necessary to respond to the contact requests and any requested measures.

- Processed data types: Contact data (e.g. e-mail, telephone numbers); Content data (e.g. text input, photographs, videos); Usage data (e.g. websites visited, interest in content, access times); Meta, communication and process data (e.g. IP addresses, time information, identification numbers, consent status).
- Data subjects: Communication partner (Recipients of e-mails, letters, etc.).
- Purposes of Processing: Contact requests and communication; Managing and responding to inquiries; Feedback (e.g. collecting feedback via online form); Provision of our online services and usability.
- Legal Basis: Legitimate Interests (Article 6 (1) (f) GDPR); Performance of a contract and prior requests (Article 6 (1) (b) GDPR).

Further information on processing methods, procedures and services used:

- Contact form: : When users contact us via our contact form, e-mail or other communication channels, we process the data provided to us in this context to process the communicated request; Legal Basis: Performance of a contract and prior requests (Article 6 (1) (b) GDPR), Legitimate Interests (Article 6 (1) (f) GDPR).

Job Application

We are members of tophotels.wien (see Imprint) and process your personal data in order to handle your application and to ensure that we can fill any open positions in an optimal manner. The legal basis for this is our overriding legitimate interest in conducting an efficient application process (Article 6 (1) (f) General Data Protection Regulation (GDPR)) as well as the necessity to take certain pre-contractual steps (Article 6 (1) (b) GDPR). We collect this data as part of the application process, either when you provide it to us (for example, by sending us your CV via email or the application tool) or when we collect it ourselves (for example, by taking notes during an interview). If the application process is not successful, we will retain your data for up to seven months from the date of rejection. If you are interested in remaining on our list for future consideration, we will need to ask for your consent to store the data for a longer period of time. Our consent form provides for a period of one year, after which your data will be deleted. You are not obliged to provide us with your

personal data or agree to remain on our list. However, if you do not do so, we will not be able to complete the application process with you or continue to store your data for future consideration. I agree that the data I entered for my application at tophotels.wien will be stored and processed accordingly for the purpose of filling other vacant positions matching my application profile for the period of one year. You may withdraw your consent by e-mail to info@tophotels.wien without the need to give any reason. In this case, we will delete your data promptly. If you do not withdraw your consent, we will automatically delete your data after one year.

Web Analysis, Monitoring and Optimization

Web analysis is used to evaluate the visitor traffic on our website and may include the behaviour, interests or demographic information of users, such as age or gender, as pseudonymous values. With the help of web analysis we can e.g. recognize, at which time our online services or their functions or contents are most frequently used or requested for repeatedly, as well as which areas require optimization.

In addition to web analysis, we can also use test procedures, e.g. to test and optimize different versions of our online services or their components.

Unless otherwise stated below, profiles, i.e. data aggregated for a usage process, can be created for these purposes and information can be stored in a browser or in a terminal device and read from it. The information collected includes, in particular, websites visited and elements used there as well as technical information such as the browser used, the computer system used and information on usage times. If users have agreed to the collection of their location data from us or from the providers of the services we use, location data may also be processed.

Unless otherwise stated below, profiles, that is data summarized for a usage process or user, may be created for these purposes and stored in a browser or terminal device (so-called "cookies") or similar processes may be used for the same purpose. The information collected includes, in particular, websites visited and elements used there as well as technical information such as the browser used, the computer system used and information on usage times. If users have consented to the collection of their location data or profiles to us or to the providers of the services we use, these may also be processed, depending on the provider.

The IP addresses of the users are also stored. However, we use any existing IP masking procedure (i.e. pseudonymisation by shortening the IP address) to protect the user. In general, within the framework of web analysis, A/B testing and optimisation, no user data (such as e-mail addresses or names) is stored, but pseudonyms. This means that we, as well as the providers of the software used, do not know the actual identity of the users, but only the information stored in their profiles for the purposes of the respective processes.

- Processed data types: Usage data (e.g. websites visited, interest in content, access times); Meta, communication and process data (e.g. IP addresses, time information, identification numbers, consent status).
- Data subjects: Users (e.g. website visitors, users of online services).
- Purposes of Processing: Web Analytics (e.g. access statistics, recognition of returning visitors); Profiles with user-related information (Creating user profiles); Targeting (e.g. profiling based on interests and behaviour, use of cookies); Provision of our online services and usability.
- Security measures: IP Masking (Pseudonymization of the IP address).
- Legal Basis: Consent (Article 6 (1) (a) GDPR).

Further information on processing methods, procedures and services used:

- Google Analytics: : Web analytics, reach measurement and measurement of user traffic; Service provider: Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland; Legal Basis: Consent (Article 6 (1) (a) GDPR); Website: <https://marketingplatform.google.com/intl/en/about/analytics/>; Privacy Policy: <https://policies.google.com/privacy>; Data Processing Agreement: <https://business.safety.google/adsprocessorterms/>; Standard Contractual Clauses (Safeguarding the level of data protection when processing data in third countries): <https://business.safety.google/adsprocessorterms/>; Opt-Out: Opt-Out-Plugin: <https://tools.google.com/dlpage/gaoptout?hl=en>, Settings for the Display of Advertisements: <https://adssettings.google.com/authenticated>; Further Information: <https://privacy.google.com/businesses/adsservices> (Types of processing and data processed).
- Google Analytics 4: : We use Google Analytics to perform measurement and analysis of the use of our online services by users based on a pseudonymous

user identification number. This identification number does not contain any unique data, such as names or email addresses. It is used to assign analysis information to an end device in order to recognize which content users have accessed within one or various usage processes, which search terms they have used, have accessed again or have interacted with our online services. Likewise, the time of use and its duration are stored, as well as the sources of users referring to our online services and technical aspects of their end devices and browsers. In the process, pseudonymous profiles of users are created with information from the use of various devices, and cookies may be used. In Analytics, higher level geographic location data is provided by collecting the following metadata based on IP search: "city" (and the derived latitude and longitude of the city), "continent", "country", "region", "subcontinent" (and the ID-based equivalents). To ensure the protection of user data in the EU, Google receives and processes all user data via domains and servers within the EU. The IP address of users is not logged and is shortened by the last two digits by default. The shortening of the IP address takes place on EU servers for EU users. In addition, all sensitive data collected from users in the EU is deleted before it is collected via EU domains and servers; Service provider: Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland; Legal Basis: Consent (Article 6 (1) (a) GDPR); Website: <https://marketingplatform.google.com/intl/en/about/analytics/>; Privacy Policy: <https://policies.google.com/privacy>; Data Processing Agreement: <https://business.safety.google/adsprocessor/terms/>; Standard Contractual Clauses (Safeguarding the level of data protection when processing data in third countries): <https://business.safety.google/adsprocessor/terms/>; Opt-Out: Opt-Out-Plugin: <https://tools.google.com/dlpage/gaoptout?hl=en>, Settings for the Display of Advertisements: <https://adssettings.google.com/authenticated>; Further Information: <https://privacy.google.com/businesses/adsservices> (Types of processing and data processed).

- Google Tag Manager: : Google Tag Manager is a solution with which we can manage so-called website tags via an interface and thus integrate other services into our online services (please refer to further details in this privacy

policy). With the Tag Manager itself (which implements the tags), for example, no user profiles are created or cookies are stored. Google only receives the IP address of the user, which is necessary to run the Google Tag Manager; Service provider: Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland; Legal Basis: Consent (Article 6 (1) (a) GDPR); Website: <https://marketingplatform.google.com>; Privacy Policy: <https://policies.google.com/privacy>; Data Processing Agreement: <https://business.safety.google/adsprocessorterms>; Standard Contractual Clauses (Safeguarding the level of data protection when processing data in third countries): <https://business.safety.google/adsprocessorterms>.

Online Marketing

We process personal data for the purposes of online marketing, which may include in particular the marketing of advertising space or the display of advertising and other content (collectively referred to as "Content") based on the potential interests of users and the measurement of their effectiveness.

For these purposes, so-called user profiles are created and stored in a file (so-called "cookie") or similar procedure in which the relevant user information for the display of the aforementioned content is stored. This information may include, for example, content viewed, websites visited, online networks used, communication partners and technical information such as the browser used, computer system used and information on usage times and used functions. If users have consented to the collection of their sideline data, these can also be processed.

The IP addresses of the users are also stored. However, we use provided IP masking procedures (i.e. pseudonymisation by shortening the IP address) to ensure the protection of the user's by using a pseudonym. In general, within the framework of the online marketing process, no clear user data (such as e-mail addresses or names) is secured, but pseudonyms. This means that we, as well as the providers of online marketing procedures, do not know the actual identity of the users, but only the information stored in their profiles.

The information in the profiles is usually stored in the cookies or similar memorizing procedures. These cookies can later, generally also on other websites that use the

same online marketing technology, be read and analyzed for purposes of content display, as well as supplemented with other data and stored on the server of the online marketing technology provider.

Exceptionally, clear data can be assigned to the profiles. This is the case, for example, if the users are members of a social network whose online marketing technology we use and the network links the profiles of the users in the aforementioned data. Please note that users may enter into additional agreements with the social network providers or other service providers, e.g. by consenting as part of a registration process.

As a matter of principle, we only gain access to summarised information about the performance of our advertisements. However, within the framework of so-called conversion measurement, we can check which of our online marketing processes have led to a so-called conversion, i.e. to the conclusion of a contract with us. The conversion measurement is used alone for the performance analysis of our marketing activities.

Unless otherwise stated, we kindly ask you to consider that cookies used will be stored for a period of two years.

- Processed data types: Content data (e.g. text input, photographs, videos); Usage data (e.g. websites visited, interest in content, access times); Meta, communication and process data (e.g. IP addresses, time information, identification numbers, consent status); Event Data (Facebook) ("Event Data" is data that can be transmitted from us to Facebook, e.g. via Facebook pixels (via apps or other means) and relates to persons or their actions; the data includes, for example, information about visits to websites, interactions with content, functions, installations of apps, purchases of products, etc.; Event data is processed for the purpose of creating target groups for content and advertising information (Custom Audiences); Event Data does not include the actual content (such as written comments), login information, and Contact Information (such as names, email addresses, and phone numbers). Event Data is deleted by Facebook after a maximum of two years, the Custom Audiences created from them with the deletion of our Facebook account).
- Data subjects: Users (e.g. website visitors, users of online services).

- Purposes of Processing: Web Analytics (e.g. access statistics, recognition of returning visitors); Targeting (e.g. profiling based on interests and behaviour, use of cookies); Conversion tracking (Measurement of the effectiveness of marketing activities); Affiliate Tracking; Marketing; Profiles with user-related information (Creating user profiles); Provision of our online services and usability.
- Security measures: IP Masking (Pseudonymization of the IP address).
- Legal Basis: Consent (Article 6 (1) (a) GDPR).
- Opt-Out: : We refer to the privacy policies of the respective service providers and the possibilities for objection (so-called "opt-out"). If no explicit opt-out option has been specified, it is possible to deactivate cookies in the settings of your browser. However, this may restrict the functions of our online offer. We therefore recommend the following additional opt-out options, which are offered collectively for each area: a) Europe: <https://www.youronlinechoices.eu>. b) Canada: <https://www.youradchoices.ca/choices>. c) USA: <https://www.aboutads.info/choices>. d) Cross-regional: <https://optout.aboutads.info>.

Further information on processing methods, procedures and services used:

- Facebook Pixel and Custom Audiences (Custom Audiences): : With the help of the Facebook pixel (or equivalent functions, to transfer Event-Data or Contact Information via interfaces or other software in apps), Facebook is on the one hand able to determine the visitors of our online services as a target group for the presentation of ads (so-called "Facebook ads"). Accordingly, we use Facebook pixels to display Facebook ads placed by us only to Facebook users and within the services of partners cooperating with Facebook (so-called "audience network" <https://www.facebook.com/audiencenetwork/>) who have shown an interest in our online services or who have certain characteristics (e.g. interests in certain topics or products that are determined on the basis of the websites visited) that we transmit to Facebook (so-called "custom audiences"). With the help of Facebook pixels, we also want to ensure that our Facebook ads correspond to the potential interest of users and do not appear annoying. The Facebook pixel also enables us to

track the effectiveness of Facebook ads for statistical and market research purposes by showing whether users were referred to our website after clicking on a Facebook ad (known as "conversion tracking"); Service provider: Meta Platforms Ireland Limited, 4 Grand Canal Square, Grand Canal Harbour, Dublin 2, Ireland; Legal Basis: Consent (Article 6 (1) (a) GDPR); Website: <https://www.facebook.com>; Privacy Policy: <https://www.facebook.com/about/privacy>; Data Processing Agreement: <https://www.facebook.com/legal/terms/dataprocessing>; Further Information: User event data, i.e. behavioral and interest data, is processed for the purposes of targeted advertising and audience building on the basis of the joint controllership agreement ("Controller Addendum", https://www.facebook.com/legal/controller_addendum). The joint controllership is limited to the collection and transfer of the data to Meta Platforms Ireland Limited, a company located in the EU. Further processing of the data is the sole responsibility of Meta Platforms Ireland Limited, which concerns in particular the transfer of the data to the parent company Meta Platforms, Inc. in the USA (on the basis of standard contractual clauses concluded between Meta Platforms Ireland Limited and Meta Platforms, Inc.).

Profiles in Social Networks (Social Media)

We maintain online presences within social networks and process user data in this context in order to communicate with the users active there or to offer information about us.

We would like to point out that user data may be processed outside the European Union. This may entail risks for users, e.g. by making it more difficult to enforce users' rights.

In addition, user data is usually processed within social networks for market research and advertising purposes. For example, user profiles can be created on the basis of user behaviour and the associated interests of users. The user profiles can then be used, for example, to place advertisements within and outside the networks which are presumed to correspond to the interests of the users. For these purposes, cookies are usually stored on the user's computer, in which the user's usage

behaviour and interests are stored. Furthermore, data can be stored in the user profiles independently of the devices used by the users (especially if the users are members of the respective networks or will become members later on).

For a detailed description of the respective processing operations and the opt-out options, please refer to the respective data protection declarations and information provided by the providers of the respective networks.

Also in the case of requests for information and the exercise of rights of data subjects, we point out that these can be most effectively pursued with the providers. Only the providers have access to the data of the users and can directly take appropriate measures and provide information. If you still need help, please do not hesitate to contact us.

- Processed data types: Contact data (e.g. e-mail, telephone numbers); Content data (e.g. text input, photographs, videos); Usage data (e.g. websites visited, interest in content, access times); Meta, communication and process data (e.g. IP addresses, time information, identification numbers, consent status).
- Data subjects: Users (e.g. website visitors, users of online services).
- Purposes of Processing: Contact requests and communication; Feedback (e.g. collecting feedback via online form); Marketing.
- Legal Basis: Legitimate Interests (Article 6 (1) (f) GDPR).

Further information on processing methods, procedures and services used:

- Instagram: : Social network; Service provider: Meta Platforms Ireland Limited, 4 Grand Canal Square, Grand Canal Harbour, Dublin 2, Ireland; Legal Basis: Legitimate Interests (Article 6 (1) (f) GDPR); Website: <https://www.instagram.com>; Privacy Policy: <https://instagram.com/about/legal/privacy>.
- Facebook-Seiten: : Profiles within the social network Facebook - We are jointly responsible (so called "joint controller") with Meta Platforms Ireland Limited for the collection (but not the further processing) of data of visitors to our Facebook page. This data includes information about the types of content users view or interact with, or the actions they take (see "Things that you and others do and provide" in the Facebook Data Policy: <https://www.facebook.com/policy>), and information about the devices used

by users (e.g., IP addresses, operating system, browser type, language settings, cookie information; see "Device Information" in the Facebook Data Policy: <https://www.facebook.com/policy>). As explained in the Facebook Data Policy under "How we use this information?" Facebook also collects and uses information to provide analytics services, known as "page insights," to site operators to help them understand how people interact with their pages and with content associated with them. We have concluded a special agreement with Facebook ("Information about Page-Insights", https://www.facebook.com/legal/terms/page_controller_addendum), which regulates in particular the security measures that Facebook must observe and in which Facebook has agreed to fulfill the rights of the persons concerned (i.e. users can send information access or deletion requests directly to Facebook). The rights of users (in particular to access to information, erasure, objection and complaint to the competent supervisory authority) are not restricted by the agreements with Facebook. Further information can be found in the "Information about Page Insights" (https://www.facebook.com/legal/terms/information_about_page_insights_data); Service provider: Meta Platforms Ireland Limited, 4 Grand Canal Square, Grand Canal Harbour, Dublin 2, Ireland; Legal Basis: Legitimate Interests (Article 6 (1) (f) GDPR); Website: <https://www.facebook.com>; Privacy Policy: <https://www.facebook.com/about/privacy>; Standard Contractual Clauses (Safeguarding the level of data protection when processing data in third countries): https://www.facebook.com/legal/EU_data_transfer_addendum; Further Information: Joint Controllership Agreement: https://www.facebook.com/legal/terms/information_about_page_insights_data. The joint controllership is limited to the collection and transfer of the data to Meta Platforms Ireland Limited, a company located in the EU. Further processing of the data is the sole responsibility of Meta Platforms Ireland Limited, which concerns in particular the transfer of the data to the parent company Meta Platforms, Inc. in the USA (on the basis of standard contractual clauses concluded between Meta Platforms Ireland Limited and Meta Platforms, Inc.).

- TikTok : Social network / video platform; Service provider: TikTok Technology Limited, 10 Earlsfort Terrace, Dublin, D02 T380, Ireland; Legal Basis: Legitimate Interests (Article 6 (1) (f) GDPR); Website: <https://www.tiktok.com>; Privacy Policy: <https://www.tiktok.com/de/privacy-policy>.
- Vimeo : Social network and video platform; Service provider: Vimeo Inc., Attention: Legal Department, 555 West 18th Street New York, New York 10011, USA; Legal Basis: Legitimate Interests (Article 6 (1) (f) GDPR); Website: <https://vimeo.com>; Privacy Policy: <https://vimeo.com/privacy>.

Plugins and embedded functions and content

Within our online services, we integrate functional and content elements that are obtained from the servers of their respective providers (hereinafter referred to as "third-party providers"). These may, for example, be graphics, videos or city maps (hereinafter uniformly referred to as "Content").

The integration always presupposes that the third-party providers of this content process the IP address of the user, since they could not send the content to their browser without the IP address. The IP address is therefore required for the presentation of these contents or functions. We strive to use only those contents, whose respective offerers use the IP address only for the distribution of the contents. Third parties may also use so-called pixel tags (invisible graphics, also known as "web beacons") for statistical or marketing purposes. The "pixel tags" can be used to evaluate information such as visitor traffic on the pages of this website. The pseudonymous information may also be stored in cookies on the user's device and may include technical information about the browser and operating system, referring websites, visit times and other information about the use of our website, as well as may be linked to such information from other sources.

- Processed data types: Usage data (e.g. websites visited, interest in content, access times); Meta, communication and process data (e.g. IP addresses, time information, identification numbers, consent status); Contact data (e.g. e-mail, telephone numbers); Content data (e.g. text input, photographs, videos).
- Data subjects: Users (e.g. website visitors, users of online services).

- Purposes of Processing: Provision of our online services and usability; Provision of contractual services and customer support; Profiles with user-related information (Creating user profiles).
- Legal Basis: Legitimate Interests (Article 6 (1) (f) GDPR).

Further information on processing methods, procedures and services used:

- reCAPTCHA: : We integrate the "reCAPTCHA" function to be able to recognise whether entries (e.g. in online forms) are made by humans and not by automatically operating machines (so-called "bots"). The data processed may include IP addresses, information on operating systems, devices or browsers used, language settings, location, mouse movements, keystrokes, time spent on websites, previously visited websites, interactions with ReCaptcha on other websites, possibly cookies and results of manual recognition processes (e.g. answering questions asked or selecting objects in images). The data processing is based on our legitimate interest to protect our online services from abusive automated crawling and spam; Service provider: Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland, , parent company: Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA; Legal Basis: Legitimate Interests (Article 6 (1) (f) GDPR); Website: <https://www.google.com/recaptcha/>; Privacy Policy: <https://policies.google.com/privacy>; Opt-Out: Opt-Out-Plugin: <https://tools.google.com/dlpage/gaoptout?hl=en>, Settings for the Display of Advertisements: <https://adssettings.google.com/authenticated>.
- Vimeo: : video contents; Service provider: Vimeo Inc., Attention: Legal Department, 555 West 18th Street New York, New York 10011, USA; Legal Basis: Legitimate Interests (Article 6 (1) (f) GDPR); Website: <https://vimeo.com>; Privacy Policy: <https://vimeo.com/privacy>; Opt-Out: We point out that Vimeo may use Google Analytics and refer to the privacy policy (<https://policies.google.com/privacy>) as well as opt-out options for Google Analytics (<https://tools.google.com/dlpage/gaoptout?hl=en>) or the settings of Google for data use for marketing purposes (<https://adssettings.google.com/>).

Changes and Updates to the Privacy Policy

We kindly ask you to inform yourself regularly about the contents of our data protection declaration. We will adjust the privacy policy as changes in our data processing practices make this necessary. We will inform you as soon as the changes require your cooperation (e.g. consent) or other individual notification.

If we provide addresses and contact information of companies and organizations in this privacy policy, we ask you to note that addresses may change over time and to verify the information before contacting us.

Rights of Data Subjects

As data subject, you are entitled to various rights under the GDPR, which arise in particular from Articles 15 to 21 of the GDPR:

- **Right to Object:** You have the right, on grounds arising from your particular situation, to object at any time to the processing of your personal data which is based on letter (e) or (f) of Article 6(1) GDPR, including profiling based on those provisions. Where personal data are processed for direct marketing purposes, you have the right to object at any time to the processing of the personal data concerning you for the purpose of such marketing, which includes profiling to the extent that it is related to such direct marketing.
- **Right of withdrawal for consents:** You have the right to revoke consents at any time.
- **Right of access:** You have the right to request confirmation as to whether the data in question will be processed and to be informed of this data and to receive further information and a copy of the data in accordance with the provisions of the law.
- **Right to rectification:** You have the right, in accordance with the law, to request the completion of the data concerning you or the rectification of the incorrect data concerning you.
- **Right to Erasure and Right to Restriction of Processing:** In accordance with the statutory provisions, you have the right to demand that the relevant data

be erased immediately or, alternatively, to demand that the processing of the data be restricted in accordance with the statutory provisions.

- Right to data portability: You have the right to receive data concerning you which you have provided to us in a structured, common and machine-readable format in accordance with the legal requirements, or to request its transmission to another controller.
- Complaint to the supervisory authority: Without prejudice to any other administrative or judicial remedy, you shall have the right to lodge a complaint with a supervisory authority, in particular in the Member State of his or her habitual residence, place of work or place of the alleged infringement if you consider that the processing of personal data relating to you infringes the GDPR.

Supervisory authority competent for us:

tophotels.wien (members see imprint)

info@tophotels.wien

Vienna