



Privacy Policy

Welcome to OTA Sync our website at www.otasync.me and www.app.otasync.me , as well as our iOS and Android mobile application. This privacy policy applies to all websites published under our domain and our mobile applications. OTA Sync is a full hotel & property management system with integrated channel manager and booking engine system.

All users facilitating, implementing, or otherwise using our booking technology are responsible for the data processing in relation to their use of our technology. For clarity, OTA Sync merely provides the technological environment to allow its service users to implement our booking technology, as such OTA Sync only processes personal data necessary to establish and maintain the contractual relationship between us and the relevant service user and service users assume all responsibility over data obtained from end-users unless specifically provided for by applicable data protection law. For details on processing in relation to the EU's General Data Protection Regulation (GDPR), please refer to our GDPR Compliance Statement.

Responsible party

We, OTA Sync, are responsible for this online offer and our IOS and Android mobile apps. In this Privacy Policy we inform you about the type, scope and purposes of the collection and use of personal data in a precise, transparent, comprehensible and easily accessible form in clear and simple language.

We attach great importance to the security of your data and compliance with applicable data protection regulations. The collection, processing and use of personal data is subject to the provisions of Serbia's Data Protection Law on 9 November 2018 (published in the Official Gazette of the Republic of Serbia, no. 87/2018) ("DP Law") and the EU's General Data Protection Regulation (GDPR).

With the following privacy policy, we would like to show you how we handle your personal data and how you can contact us:

OTASync OÜ
A. Lauteri 3, 10114 Tallinn, Estonia

You can contact us at any time regarding this and other questions on the subject of data protection using office@otasync.me.

General Information

The personal data of users processed within the scope of this online offer includes inventory data (e.g., name and addresses of customers), contract data (e.g., services used, payment information), usage data (e.g., interest in the products) and content data (e.g., entries in an order form, product advertisements).

"Users" includes all categories of persons affected by the data processing. This includes, for example, our business partners, customers, interested parties and other visitors to our online offer.

Specific Information

We guarantee that we will only collect, process, store and use your data in connection with the processing of your queries and for internal purposes as well as in order to provide the services you have requested or to make content available.

Principles of data processing

We process users' personal data only in compliance with the relevant data protection regulations. The data of the users are only processed if the following legal permissions exist:

- in order to provide our contractual services and online services
- processing is required by law
- with your consent



Privacy Policy

- on the basis of our legitimate interests (i.e., interest in the analysis, optimisation and economic operation and security of our online offer in particular in the case of advertising and marketing purposes as well as collection of access data and use of third-party services).

Legal basis for the processing of personal data

Insofar as we obtain the consent of the data subject for processing operations involving personal data, consent serves as the legal basis for the processing of personal data.

When processing personal data that is necessary for the performance of a contract to which the data subject is a party, the performance of a contract serves as the legal basis. This also applies to processing operations that are necessary for the performance of pre-contractual measures. If processing of personal data is necessary for compliance with a legal obligation to which our company is subject, a legal obligation serves as the legal basis.

If processing is necessary to protect a legitimate interest of our company or a third party and if the interests, fundamental rights and freedoms of the data subject do not outweigh the first-mentioned interest, legitimate interest serves as the legal basis for the processing.

Data transfer to third parties

Data is only passed on to third parties within the framework of legal requirements. We only pass on users' data to third parties if this is necessary, for example, for contractual purposes or on the basis of legitimate interests in the economic and effective operation of our business.

If we use subcontractors to provide our services, we take appropriate legal precautions as well as corresponding technical and organisational measures to ensure the protection of personal data in accordance with the relevant legal regulations.

Data transfer to a third country or an international organisation

Third countries are countries in which the GDPR is not directly applicable law. This basically includes all countries outside the EU. This takes into account that appropriate/adequate safeguards are in place and that enforceable rights and effective remedies are available to you. Such transfer takes place exclusively based on your consent. You give your consent by selecting the appropriate option in the consent management tool, which is displayed when you access our site. You can view and adjust your data protection settings using the consent management tool at any time.

Storage period of your personal data

We adhere to the principles of data minimisation and data economy. This means that we only store the data you provide to us for as long as is necessary to fulfil the aforementioned purposes or as specified by the various storage periods provided for by law. If the respective purpose ceases to apply or after the relevant periods have expired, your data will be routinely blocked or deleted in accordance with the statutory provisions.

Data Breaches/Notification

Databases or data sets that include Personal Data may be breached inadvertently or through wrongful intrusion. Upon becoming aware of a data breach, we will notify all affected individuals whose Personal Data may have been compromised, and the notice will be accompanied by a description of action being taken to reconcile any damage as a result of the data breach. Notices will be provided as expeditiously as possible after which the breach was discovered.

Contact

If you contact us by e-mail, you agree to electronic communication. Personal data is collected when you contact us. Your data will be transmitted SSL-encrypted. The information you provide will be stored exclusively for the purpose of processing the query and for possible follow-up questions. We



Privacy Policy

would like to point out that e-mails can be read or changed unauthorised and unnoticed during transmission. Furthermore, we would like to point out that we use software to filter unwanted e-mails (spam filter). The spam filter can reject e-mails if they have been falsely identified as spam by certain characteristics.

Data processing in the context of visiting the OTA Sync website

For the simple use of our website, only the processing of your IP address is absolutely necessary. Without internet protocol addresses, or "IP addresses" for short, the internet would not function - to put it very simply. In computer networks, an IP address is an address that can be used to address and reach web servers and/or individual end devices. Without an IP address, the web server and the end devices cannot communicate - and thus cannot display anything. The web server on which OTA Sync is hosted is therefore pinged with a data request from you, because you want to use OTA Sync!.

In order to provide you with the data, the web server needs to know your IP address. Consequently, the web server must save your IP address at this moment of the data request. For this purpose, the web server receives information about which website or file was accessed, which browser and which operating system was used. The whole process is called a log file. We store the IP addresses and the log files for 60 days in order to quickly detect brute force attacks and other manipulations and to be able to take countermeasures.

Further storage for purposes of technical support of our IT security is based on legitimate interest, as we have a legitimate interest in protecting our services from attacks and manipulation. A predominantly legitimate interest of the data subject is not recognisable, as only the IP address is stored, which we as the responsible party cannot de-pseudonymise, i.e., we cannot establish a personal reference by means of the IP address.

Device information

We collect information from and about the device(s) you use to access our services, including: hardware and software information such as IP address, device ID and type, device-specific and apps settings and characteristics, app crashes, advertising IDs (such as Google's AAID and Apple's IDFA, both of which are randomly generated numbers that you can reset by going into your device's settings), browser type, version and language, operating system, time zones, identifiers associated with cookies or other technologies that may uniquely identify your device or browser (e.g., IMEI/UDID and MAC address); information on your wireless and mobile network connection, like your service provider and signal strength; information on device sensors such as accelerometers, gyroscopes and compasses.

How We Use Technical Information

The main reason we use your information is to deliver and improve our services. Additionally, we use this info to help keep you safe.

- To provide our services to you,
- To create and manage our App and provide new features,
- To improve our services and develop new ones,
- To conduct research and analysis of users' behaviour to improve our services and content (for instance, we may decide to change the look and feel or even substantially modify a given feature based on users' behaviour),
- To prevent, detect and fight fraud or other illegal or unauthorized activities,
- To Perform data analysis to better understand and design countermeasures against these activities
- To ensure legal compliance
- To Assist law enforcement
- To Enforce or exercise our rights.



Privacy Policy

Contractual and Association work

We process the data of our clients, supporters, interested parties, business partners or other persons if we have a contractual or other business relationship with them and, as a result, perform our tasks and are recipients of services and benefits. This may include e-mail, phone number, guest data provided from third party systems or directly from client, revenue information, costs, and other information needed for our clients to use our enterprise solution. As well as sign up data such as name of the business, e-mail and password, payment information, details for room and price management, price modelling, photos, descriptions, etc.

We also process your data on the basis of our legitimate interests, e.g., when administrative tasks or public relations work are involved.

The data processed in this way, the type, scope and purpose and the necessity of its processing, are determined by the business or contractual relationship concluded with you, which also determines the necessity of any data disclosures (we will of course explicitly point this out to you).

We delete data that is no longer required to fulfil our statutory and business purposes. This is determined according to the respective tasks and contractual relationships. The retention period of your data is determined according to how it may be relevant for business processing, as well as with regard to any warranty or liability obligations based on our legitimate interests in regulating them. We continuously review the necessity of retaining the data. The statutory retention obligations always apply.

Updating your information

If you believe that the information, we hold about you is inaccurate or that we are no longer entitled to use it and want to request its rectification, deletion, or object to its processing, please do so within your user account or contact us. For your protection and the protection of all of our users, we may ask you to provide proof of identity before we can answer the above requests.

Keep in mind, we may reject requests for certain reasons, including if the request is unlawful or if it may infringe on trade secrets or intellectual property or the privacy of another user. Also, we may not be able to accommodate certain requests to object to the processing of personal information, notably where such requests would not allow us to provide our service to you anymore.

Administration, financial accounting, office organization, contact management

We process information in the context of administrative tasks as well as organization of our operations, financial accounting and compliance with legal obligations, such as archiving. In this regard, we process the same information that we process in the course of providing our contractual services. The deletion of information with regard to contractual services and contractual communication corresponds to the information mentioned in these processing activities.

In this context, we disclose or transfer information to the tax authorities, consultants, such as tax advisors or auditors, as well as other fee offices and payment service providers.

Furthermore, based on our business interests, we store information on suppliers, event organizers and other business partners, e.g., for the purpose of contacting them at a later date. This information, most of which is company-related, is generally stored permanently.

Data processing within the framework of payment processing

Payment by credit card and SEPA direct debit is made via the payment service provider "[Stripe](#)", to which we pass on your mandatory details (e-mail address) provided during the registration process, together with information about your booked services. Your data will only be passed on for the purpose of payment processing with the payment service provider Stripe and only insofar as it is necessary for this purpose.



Privacy Policy

Prevention and detection of fraud and abuse

In order to protect our online offer from fraud and abuse, we have implemented security measures which check whether there are indications of abuse of our online offer or of an attempted fraud. These measures also serve to protect you. The data processed within the framework of the security measures may include all security risk-relevant user information that accrues within the framework of the use of our online offer. For example, but not exhaustively, this includes inventory data (e.g., names, addresses), contact data, usage data (e.g., websites visited, access times), meta/communication data (e.g., device information, IP addresses), contract data (e.g., subject matter of contract, term), content data (e.g. advertisements and chat content: text entries and images), payment data (e.g. bank details, invoices).

Processing of personal data when using the offered services

Personal data will be collected, processed, or used ("used") in connection with the services offered. This is always done in compliance with the provisions of the BDSG and the GDPR. Insofar as we use your personal data for a purpose that requires your consent according to the legal provisions, we will always ask for your express consent.

Administration, financial accounting, office organisation, contact management

We process data in the context of administrative tasks as well as organisation of our operations, financial accounting and compliance with legal obligations, such as archiving. In this regard, we process the same data that we process in the course of providing our contractual services. The processing bases are our legal obligations and contract. Customers, interested parties, business partners and website visitors are affected by the processing. The purpose and our interest in the processing lies in the administration, financial accounting, office organisation, archiving of data, i.e., tasks that serve the maintenance of our business activities, performance of our tasks and provision of our services. The deletion of data with regard to contractual services and contractual communication corresponds to the data mentioned in these processing activities.

In this context, we disclose or transfer data to the tax authorities, consultants, such as tax advisors or auditors, as well as other fee offices and payment service providers.

Furthermore, based on our business interests, we store information on suppliers, event organisers and other business partners, e.g., for the purpose of contacting them at a later date. This data, most of which is company-related, is generally stored permanently.

General technical organisational measures

OTA Sync has taken a variety of security measures to protect personal information to an appropriate extent and adequately. All information held by OTA Sync is protected by physical, technical, and procedural measures that limit access to the information to specifically authorised persons in accordance with this Privacy Policy.

Secure transfer of your data

In order to best protect the data, we store against accidental or intentional manipulation, loss, destruction or access by unauthorised persons, we use appropriate technical and organisational security measures. The security levels are continuously reviewed in cooperation with security experts and adapted to new security standards.

The exchange of data to and from our website is always encrypted. We offer HTTPS as the transmission protocol for our website, in each case using the current encryption protocols.

In addition, we offer our users content encryption as part of the contact forms and for applications. The decryption of this data is only possible for us. In addition, there is the option of using alternative communication channels (e.g., the postal service).

When you send a data subject access request



Privacy Policy

The legal basis for the processing of your personal data in the context of handling your data subject access request is our legal obligation and the legal basis for the subsequent documentation of the data subject access request is both our legitimate interest and our legal obligation. The purpose of processing your personal data in the context of processing data when you send a data subject access request is to respond to your request. The subsequent documentation of the data subject access request serves to fulfil the legally required accountability.

Your personal data will be deleted as soon as they are no longer required to achieve the purpose for which they were collected. In the case of the processing of a data subject access request, this is three years after the end of the respective process. You have the possibility at any time to object to the processing of your personal data in the context of the processing of a data subject access request for the future. In this case, however, we will not be able to further process your request. The documentation of the legally compliant processing of the respective data subject access request is mandatory. Consequently, there is no possibility for you to object.

Legal defence and enforcement of our rights

The legal basis for the processing of your personal data in the context of legal defence and enforcement of our rights is our legitimate interest. The purpose of processing your personal data in the context of legal defence and enforcement of our rights is the defence against unjustified claims and the legal enforcement and assertion of claims and rights.

Your personal data will be deleted as soon as they are no longer necessary to achieve the purpose for which they were collected. The processing of your personal data in the context of legal defence and enforcement is mandatory for legal defence and enforcement of our rights. Consequently, there is no possibility for you to object.

SSL or TLS Encryption

For security reasons and to protect the transmission of confidential content, such as orders or queries that you send to us as the site operator, this site uses SSL or TLS encryption. You can recognise an encrypted connection by the fact that the address line of the browser changes from "http://" to "https://" and by the lock symbol in your browser. If SSL or TLS encryption is activated, the data you transmit to us cannot be read by third parties.

Accountability

In certain countries, including in the European Union, you have a right to lodge a complaint with the appropriate data protection authority if you have concerns about how we process information. The data protection authority you can lodge a complaint with notably may be that of your habitual residence, where you work or where we are established.

Automated decision-making and profiling

We do not use automation for decision-making and profiling.

Do Not Track

Do Not Track is a privacy preference you can set in most browsers. We support Do Not Track because we believe that you should have genuine control over how your info gets used and our site responds to Do Not Track requests.

Do Not Sell My Personal Information

We do not sell information that directly identifies you, like your name, address or phone records.

Accuracy

It is important that the data we hold about you is accurate and current, therefore please keep us informed of any changes to your personal data.



Privacy Policy

Children Data

Our website is not intended for children, and we do not knowingly collect data relating to children. If you become aware that your Child has provided us with Personal Data, without parental consent, please contact us and we take the necessary steps to remove that information from our server.

Integration Of Services and Contents of Third Parties

We use within our online offer on the basis of our legitimate interests, content or services offered by third-party providers in order to integrate their content and services.

This always requires that the third-party providers of this content are aware of your IP address, since the content or service could not send to your browser without the IP address. The IP address is thus required for the display of this content, and we endeavour to use providers that only use your IP address for the delivery of the content or services. However, Third-party providers 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. The pseudonymous information may also be stored in cookies on the user's device and may contain, among other things, technical information about the browser and operating system, referring websites, time of visit and other information about the use of our online offer, as well as be linked to such information from other sources.

Hosting

The services for hosting and displaying the website and app are partly provided by our service providers as part of processing on our behalf. Unless otherwise explained in this privacy policy, all access data and all data collected in forms provided for this purpose on this website are processed on their servers. If you have any questions about our service providers and the basis of our relationship with them, please contact them as described in this privacy policy.

Public cloud servers

We use [Microsoft Azure](#) servers for hosting. For hosting in the Microsoft Azure cloud servers, the EU region is used. However, Microsoft Azure cloud operates according to the principle of a multi-tenant environment, so that data is replicated between several geographically distributed data centres ([data centre resilience](#)).

Firebase

The App uses the [Firebase](#) tool, which is part of the Firebase platform of Google Inc, 1600 Amphitheatre Parkway Mountain View, CA 94043, USA, to obtain statistics on how the App is used, in particular active user numbers, session length, stability rating and storage time. Answers logs the use of the app, and [we evaluate](#) user behaviour and user activity in general, i.e., not on a personal basis.

For this purpose, the following data is transferred to the Analytics Engine: name and AppStore ID, build version, individual device installation key (e.g. IDFA [iOS], Advertising ID, and Android ID), timestamp, device model, device name, device operating system name and version numbers, the language and country settings of the device (iOS), the number of CPU cores on the device (iOS), whether a device has the status "jailbreak" (iOS) or "root " (Android), app lifecycle events (iOS) and app activities (Android);

The legal basis for this data processing is our legitimate interest. The data collected via Google will be deleted after 6 months at the latest. You can select in the settings under data services whether or not you want to send data to Google. This setting also applies to the use of Crashlytics.

Crashlytics

The app uses the tool [Crashlytics](#), which is part of the platform Firebase of Google Inc., 1600 Amphitheatre Parkway Mountain View, CA 94043, USA, to log crashes of the app. No personal data is transmitted. Only real-time crash reports with precise details of code locations and device information are sent, which is intended to simplify maintenance and improve the resulting stability of the app.



Privacy Policy

The legal basis for data processing is our legitimate interest. In the settings under data services, you can select whether you want to send crash reports or not. This setting also applies to the use of Google.

Content Delivery Network

For the purpose of a shorter loading time, we use a so-called Content Delivery Network ("CDN") for some offers. With this service, content, e.g., large media files, are delivered via regionally distributed servers of external CDN service providers. Therefore, access data is processed on the servers of the service providers. Our service providers work for us within the framework of order processing. If you have any questions about our service providers and the basis of our cooperation with them, please use the contact option described in this privacy policy.

Cookies

During the use of our website, so-called "cookies", small text files, are stored on your computer. Such cookies register information about your computer's navigation on our website (pages selected, day, time and duration of use, etc.). A cookie is downloaded via a browser the first time you visit a website. The next time you visit this website with the same device, the browser checks whether a corresponding cookie is present (i.e., contains the website name). It sends the data stored in the cookie back to the website. Some cookies are important for the website's functionality and are automatically activated by us when a user visits. Our website also uses cookies to make it easier to use and to provide you with content tailored to your information needs.

You cannot be personally identified from any of the information we collect. The use of the cookies we use is necessary in order to be able to provide the online offer of OTA Sync at all and, moreover, to be able to optimise it on an ongoing basis. The data processing in this context is therefore based on our legitimate interest. Our legitimate interest is to provide visitors to our website with a functioning online service and to make visiting and using the website as pleasant and efficient as possible.

For further information on cookies in general, please visit www.allaboutcookies.org and for specific info on the cookies we use please read our Cookie Policy.

Receiving messages (push notification)

For individual areas, the app offers the option of being informed via push notification (push technology or Server Push describes a type of communication in which data is transmitted even though the receiving app is running in the background).

You can configure this function via the settings of your smartphone settings and activate/deactivate the notifications there. For the delivery of the messages, it is necessary to store a push token of your mobile end device.

Authorisations and Access

We may request access or permission to certain functions from your mobile device. The legal basis for data processing is our legitimate interest and the provision of contractual or pre-contractual measures. You can deactivate push notifications at any time via Settings/Messages (iOS) or Settings/Notifications/ (Android).

Electronic notifications

We send notifications, e-mails and other electronic notifications only with the consent of the recipients or with a legal permission. If the contents of a notification are specifically described in the course of registration, they are decisive for the consent of the users. In addition, our notifications contain information about our services and us.



Privacy Policy

In order to subscribe to our notifications, it is generally sufficient to provide your e-mail address. However, we may ask you to provide a name, for the purpose of personal address in the notification, or further details, if these are necessary for the purposes of the notification.

The registration for our notification is always carried out in a so-called double opt-in procedure. This means that after registration you will receive an e-mail in which you are asked to confirm your registration. This confirmation is necessary so that no one can register with other people's e-mail addresses. The registrations for the notification are logged in order to be able to prove the registration process in accordance with the legal requirements. This includes the storage of the registration and confirmation time as well as the IP address. Changes to your data stored with the dispatch service provider are also logged.

We may store unsubscribed email addresses for up to three years based on our legitimate interests before deleting them in order to be able to prove consent previously given. The processing of this data will be limited to the purpose of a possible defence against claims. An individual deletion request is possible at any time, provided that the former existence of consent is confirmed at the same time. In the case of obligations to permanently observe objections, we reserve the right to store the e-mail address in a block list (so-called "block list") for this purpose alone.

The logging of the registration process takes place on the basis of our legitimate interests for the purpose of proving its proper course. If we commission a service provider to send e-mails, this is done on the basis of our legitimate interests in an efficient and secure sending system.

Notes on legal basis: The notification is sent on the basis of the recipients' consent. The registration process is recorded on the basis of our legitimate interests to prove that it has been carried out in accordance with the law.

The notifications contain a so-called "tracking pixel", i.e., a pixel-sized file that is retrieved from our server or, if we use a dispatch service provider, from their server when the notification is opened. Within the scope of this retrieval, technical information such as information on the browser and your system, as well as your IP address and the time of the retrieval, are initially collected.

This information is used for the technical improvement of our notification on the basis of the technical data or the target groups and their reading behaviour on the basis of their retrieval locations (which can be determined with the help of the IP address) or the access times. This analysis also includes determining whether the notifications are opened, when they are opened, and which links are clicked. This information is assigned to the individual notification recipients and stored in their profiles until they are deleted. The analyses help us to recognise the reading habits of our users and to adapt our content to them or to send different content according to the interests of our users.

The measurement of opening rates and click rates as well as the storage of the measurement results in the users' profiles and their further processing are based on the users' consent.

When you use our Social Media Pages

We also process information that you have provided to us via our company pages on the relevant social media website. Such information may be the username used, contact details or a message sent to us. We regularly process this personal data only if we have previously expressly requested you to provide us with this data, for example as part of a survey. These processing operations are carried out by us as the sole data controller.

We process this data on the basis of our legitimate interest in contacting people who make enquiries. In addition, we may process such data for evaluation and marketing purposes. This processing is carried out on the legal basis of our legitimate interest and serves our interest in further developing our offer and informing you specifically about our offers. Further data processing may take place if you have



Privacy Policy

consented or if this serves the fulfilment of a legal obligation. The sole controller of this processing of personal data is the relevant social media website.

When you send a data subject access request

The legal basis for the processing of your personal data in the context of handling your data subject access request is our legal obligation and the legal basis for the subsequent documentation of the data subject access request is both our legitimate interest and our legal obligation.

The purpose of processing your personal data in the context of processing data when you send a data subject access request is to respond to your request. The subsequent documentation of the data subject access request serves to fulfil the legally required accountability.

Your personal data will be deleted as soon as they are no longer required to achieve the purpose for which they were collected. In the case of the processing of a data subject access request, this is three years after the end of the respective process.

You have the possibility at any time to object to the processing of your personal data in the context of the processing of a data subject access request for the future. In this case, however, we will not be able to further process your request. The documentation of the legally compliant processing of the respective data subject access request is mandatory. Consequently, there is no possibility for you to object.

Transfer of data

Unless otherwise stated above, we do not disclose personal data to companies, organisations, or persons outside our company, except in one of the following circumstances:

a) data sharing with affiliated companies in the context of joint data maintenance.

OTA Sync stores and processes your data collected from you in the course of using our website services and visiting our website in an IT system that can only be accessed by OTA Sync Employees based on a strict need to know basis.

b) With your consent

As far as already described in detail above, but in individual cases also beyond that, we pass on personal data to companies, organisations, or persons outside our company if we have received your consent for this.

c) processing by other bodies

We make personal data available to other companies that are affiliated with us, as well as to our third-party business partners, other trusted companies or persons who process it on our behalf. This is done on the basis of our instructions and in accordance with our privacy policy and other appropriate confidentiality and security measures.

d) for legal reasons

We will disclose personal data to companies, organisations or persons outside our company if we can reasonably assume that access to this data or its use, storage or disclosure is necessary, in particular, to comply with applicable laws, regulations or legal procedures or to comply with an enforceable official order.

Your Rights

You have a number of 'Data Subject Rights' below is some information on what they are and how you can exercise them.

Right to information: You can request information from us as to whether and to what extent we process your data.



Privacy Policy

Right to rectification: If we process your data that is incomplete or incorrect, you can request that we correct or complete it at any time.

Right to erasure: You may request that we erase your data if we are processing it unlawfully or if the processing disproportionately interferes with your legitimate interests in protection. Please note that there may be reasons that prevent immediate deletion, e.g., in the case of legally regulated retention obligations. Irrespective of the exercise of your right to deletion, we will delete your data immediately and completely, insofar as there is no legal or statutory obligation to retain data in this respect.

Right to restriction of processing: You may request us to restrict the processing of your data if you dispute the accuracy of the data for a period of time that allows us to verify the accuracy of the data, the processing of the data is unlawful, but you object to erasure and request restriction of data use instead, we no longer need the data for the intended purpose, but you still need this data to assert or defend legal claims, or you have objected to the processing of the data.

Right to object: If we process your data for legitimate interest, you may object to this data processing at any time; this would also apply to profiling based on these provisions. We will then no longer process your data unless we can demonstrate compelling legitimate grounds for the processing which override your interests, rights and freedoms, or the processing is for the assertion, exercise or defence of legal claims. You may object to the processing of your data for the purpose of direct marketing at any time without giving reasons.

Where the processing of your personal information is based on consent, you have the right to withdraw that consent without detriment at any time.

The above rights may be limited in some circumstances, for example, if fulfilling your request would reveal personal information about another person, if you ask us to delete information which we are required to have by law, or if we have compelling legitimate interests to keep it. We will let you know if that is the case and will then only use your information for these purposes. You may also be unable to continue using our services if you want us to stop processing your personal information.

We encourage you to get in touch if you have any concerns with how we collect or use your personal information.

Obligation to provide personal data

You are not obliged to provide us with personal data. However, depending on the individual case, the provision of certain personal data may be necessary for the provision of the above services. If you do not provide us with this personal data, we may not be able to provide the service.

Changes

This policy and our commitment to protecting the privacy of your personal data can result in changes to this policy. Please regularly review this policy to keep up to date with any changes.

Queries and Complaints

Any comments or queries on this policy should be directed to us. If you believe that we have not complied with this policy or acted otherwise than in accordance with data protection law, then you should notify us.