

## Privacy Protection

We comply with all applicable data protection provisions of the GDPR (General Data Protection Regulation) and the DPA (Data Protection Act) when processing your personal data (e.g., master data).

Below, you will find further information regarding our data processing activities. Under the tab labeled 'privacy', you can view, print and save our privacy policy at any time.

### 1. Responsible

#### **conova communications GmbH**

Karolingerstrasse 36A, 5020 Salzburg

Telephone: [+43 662 22 00 0](tel:+4366222000)

E-Mail: [office@conova.com](mailto:office@conova.com)

We have not appointed a data protection officer as we are not legally required to do so.

### 2. Affected Rights

#### **2.1.** You have the following rights concerning your personal data:

- Right to information (article 15 GDPR): You reserve the right to request confirmation from us as to whether we are processing your personal information. Should this be the case, you have the right to information regarding this personal data and the information according to article 15 of the GDPR.
- Right to rectification (article 16 GDPR): You reserve the right to request correction of personal data without delay or to have incomplete personal data completed if necessary.
- Right to deletion ('right to be forgotten'; article 17 GDPR): You have the right to demand immediate deletion of personal data concerning you if one of the reasons stated in article 17 of the GDPR exists (e.g., data processing is no longer necessary).
- Right to data portability (article 20 GDPR): You have the right to receive the personal information you provided us in a structured, current and machine-readable format and to transmit that information to another person without hindrance. However, this right only exists if the data processing is based on consent (article 6 (1)(a) or article 9 (2)(a) GDPR) or based on a contract (article 6 (1)(b) GDPR) and if the processing is done by means of automated procedure.

## 2.2. Right to objection

You have the right, at any time, to object to the processing of your personal data for reasons arising from your particular situation. **However, you are only entitled to this right if the data processing is required for the completion of a public interest or in the execution of public authority** (article 6(1) GDPR) or if required for the protection of our **legitimate interests** or that of a third party (article 6 (1) GDPR).

When exercising your right to objection, we ask that you explain your reasons why we should not process your personal data as previously done. We then verify the situation and either adjust or adapt the data processing or indicate our compelling and legitimate reasons for continuing the data processing. We will also continue to process the data if it serves the enforcement, practice or defense of legal claims.

You may object to data processing for the purposes of **direct mail and data analysis** (profiling in the context of direct mail advertising) at any time and free of charge. We discontinue the processing of data in this case.

## 2.3. Right of revocation

You may **revoke** your **consent** for the processing of your personal data **at any time**. Your revocation does not affect the legality of the data processing carried out until the time of retraction, i.e., it applies to the future.

## 2.4. How to exercise your rights

To carry out the above rights, you must inform us personally, by telephone or in writing:

**conova communications GmbH**  
**Karolingerstrasse 36A, 5020 Salzburg**  
**Telephone: [+43 662 22 00 0](tel:+4366222000)**  
**E-Mail: [datenschutz@conova.com](mailto:datenschutz@conova.com)**

Please note that we can only give information if you can properly identify yourself.

## 2.5. Right to appeal the supervisory authority

Should you believe that our data processing violates applicable data protection laws or that we have violated your privacy claims, you also reserve the right to **file an official complaint** to the regulatory authority. This applies independently of any other administrative or judicial appeals.

You may submit your complaint to the supervisory authority in the member state of your whereabouts, your place of work or the location of the alleged infringement.

Should you choose to file your complaint with the supervisory authority in Austria, please send it to:

**Oesterreichische Datenschutzbehoerde**  
**Barichgasse 40-42**  
**1030 Wien**  
**Telephone: [+43 1 52 152 0](tel:+431521520)**  
**E-Mail: [dsb@dsb.gv.at](mailto:dsb@dsb.gv.at)**

### **3. Information regarding the processing of your personal data**

- 3.1. Website visits
- 3.2. Handling of requests via website form
- 3.3. Cookies
- 3.4. Customer administration, accounting, logistics, bookkeeping
- 3.5. Personnel administration and applicant management
- 3.6. Access management for computer systems
- 3.7. Customer care and marketing for own purposes
  - 3.7.1. Remarketing/Retargeting
- 3.8. Product registration
- 3.9. Video surveillance in the data center
- 3.10. Access control system – building
- 3.11. Access control system – data center (biometric access system)
- 3.12. Access control system – rack locking system
- 3.13. Telephone system
- 3.14. Visitor management
- 3.15. Project management
- 3.16. Documentation system
- 3.17. Ticket system & mail
- 3.18. ConApp
- 3.19. Push messages
- 3.20. YouTube
- 3.21. Google Maps
- 3.22. HubSpot
- 3.23. Matomo
- 3.24. Fact Advisor
- 3.25. Octopus
- 3.26. Services of Hornetsecurity GmbH
- 3.28. Google Marketing Services
- 3.29. Services provided by Dacoso GmbH for SOC services
- 3.30. N-Able

### 3.1. Website visits

- Purpose: If the website is used for information purposes only (without registration or other information), personal data will be collected and transmitted by the browser to the server. This is technically required in order to help you view the website and to ensure the stability and security of the site.
- Legal basis: Article 6 section 1 (legitimate interest); § 96 section 3 TKG 2003
- The following data is processed: IP address, date and time of request, time zone difference to GMT, content of request (concrete page, access status/HTTP status code, amount of data transferred, requesting website, browser, operating system and interface, language, version of browser software.
- Duration of storage: The duration of the website visit.

### 3.2. Handling of requests via website form

- Purpose: Processing of inquiries/registrations via conova forms such as contact, test versions, newsletters, etc.
- Legal basis: Article 6 Section 1 b (fulfillment of contract); Article 6 Section 1 f (legitimate interest); § 96 Section 3 TKG 2003
- The following data is processed: Master data, content data of the request/registration, customer number (if available/specified).
- Duration of storage: Until answering of request. If legal storage requirements exist, the processing is limited to that point in time.
- The contact forms on our website use reCAPTCHA, a free Captcha service offered by Google. This service is designed to ensure that the forms are filled out by a human rather than a bot, thereby serving as a security measure on our website. reCAPTCHA is activated only through filling out a form field. With this service, Google can determine from which website a request is being sent as well as from which IP address you are using the reCAPTCHA input box. In addition to your IP address, Google may collect further information that is necessary to the service. Google offers further information regarding the handling of user data at <https://policies.google.com/privacy>.

We require the provision of your personal data in order to answer your request. Without this data, we cannot process your inquiries.

### 3.3. Cookies

This website uses so-called cookies. A cookie is a small file that can be stored on your computer when you visit a website. Generally, cookies are used to offer users additional functions on a

website. For example, they can be used to make it easier for you to navigate a website, to enable you to continue using a website from the same place you left it and/or to save your preferences and settings for when you visit it again. Cookies cannot access, read or alter any other data on your computer.

Most of the cookies on this website are so-called session cookies. They are automatically deleted when you leave the website. Permanent cookies, however, remain on your computer until you have manually deleted them in your browser. We use permanent cookies in order to recognize you the next time you visit our website.

Should you give your explicit consent to the storage and use or deployment of cookies when you visit our website, then our website will operate with these cookies in several places. They serve the purpose of making our service more user-friendly and effective. Cookies are small text files that are stored on your computer by the browser. A distinction is made between

- functionally essential and
- non-functionally essential cookies.

**Functionally essential** cookies guarantee the functionality of the website and are therefore absolutely necessary in order to use it. They can be deactivated in the browser settings, which can lead to an impairment of use and accessibility within the website.

**Non-functionally essential** cookies, on the other hand, are not absolutely necessary in order to be able to access and use the website. Regardless, they are beneficial in order to make the website as user-friendly as possible. This service will no longer be available in the event of deactivation. Once deactivated, we can no longer save the settings and preferences you have made or provide you with offers and suggestions tailored to your preferences and wishes. Non-essential cookies can be deactivated via the slider.

Should you wish to control all cookies on your computer, you can choose your browser settings accordingly to receive notification when a website requests to save cookies. You can also block or delete cookies that have already been saved on your computer. Please use the 'Help' function in your browser to learn more about taking these steps. Please note that blocking or deleting cookies could affect your online experience and prevent you from using the website to its full potential.

Keep in mind that you can delete cookies that have already been saved at any time. All relevant instructions for managing and deleting cookies can be found within the help functions of the respective browser and at:

Internet Explorer: <https://windows.microsoft.com/de-DE/windows-vista/Block-or-allow-cookies>

Firefox: <https://support.mozilla.org/de/kb/cookies-erlauben-und-ablehnen>

Chrome: <https://support.google.com/chrome/bin/answer.py?hl=de&hlrm=en&answer=95647>

Safari: <https://support.apple.com/de-at/guide/safari/sfri11471/mac>

Opera: <https://help.opera.com/Windows/10.20/de/cookies.html>

With regard to the functionally essential cookies, data processing takes place on the basis of our legitimate interest in providing fully functional website services (Art. 6 section 1 lit. f GDPR, § 96 Par. 3 TKG) as well as due to the consent obtained (Art 6 section 1 lit a GDPR).

The use of non-functionally essential cookies is neither legally nor contractually required and is also not required in order to conclude a contract. Therefore, there is no obligation to allow such cookies. The legal basis for use of this category of cookies is therefore the consent you have given (Art 6 section 1 lit a GDPR). Should your consent not be given, then the non-functionally essential cookies will not be used.

You reserve the right to revoke your consent to the use of cookies at any time without stating any reason. To do this, you may send us an e-mail to [datenschutz@conova.com](mailto:datenschutz@conova.com) or a letter to the company address shown below. However, we would like to point out that all processing and transmissions carried out until the revocation date remain lawful.

### **3.4. Customer administration, accounting, logistics, bookkeeping**

- Purpose: The processing of personal data in the context of all business relationships with customers and suppliers in the setting of commercial practice, including the systematic recording of all business transactions relating to revenue and expenditure.
- Legal basis: Article 6 section 1 a (consent of persons concerned); Article 6 section 1 b (fulfillment of contract); Article 6 section 1 c (fulfillment of a legal obligation, in particular § 132 BAO, §§ 190, 212 UGB); Article 6 section 1 f (legitimate interests, in particular defense, exercise and assertion of legal rights)
- Duration of storage: Until termination of the business relationship or until expiry of the guarantee, warranty, statute of limitations and legal retention periods applicable to the person responsible (in particular BAO: 7 years). In addition, until the termination of any legal disputes in which the data is required as proof.
- Recipient/beneficiary categories: Customers, banks, legal representatives, accountants, courts, authorities, debt collection authorities, debtors, contributing contract and business partners, insurance institutions.

The provision of your personal data is necessary to fulfill the contract or to carry out pre-contractual measures. We cannot conclude a contract with you without this data.

### 3.5. Personnel administration and applicant management

- Purpose: Processing and maintenance of personal data for wages, salary, payroll and compliance with recording, information and reporting and compulsory registration to the extent required by law or employment contract law. Processing and maintenance of personal data provided by the person concerned.
- Legal basis: Article 6 section 1 lit. a (consent of person concerned); Article 6 section 1 lit. b (fulfillment of contract); Article 6 section 1 lit. c (fulfillment of legal obligation); Article 6 section 1 lit. f (legitimate interests, in particular defense, exercise and assertion of legal claims); Article 9 section 2 a (explicit consent); Article 9 section 2 b (required in order to fulfill obligations listed under labor and social law); Article 9 section 2 f (assertion, exercise or defense of legal claims).
- Duration of storage: Until termination of relationship with the party concerned and beyond, as long as legal retention periods exist or as long as claims can be asserted from the employment relationship. Applicant data will be deleted immediately after the position has been filled, unless consent has been obtained. Speculative applications are kept for a period of 9 months. Data will be deleted following this period.
- Recipient/beneficiary categories: Banks, legal representatives, courts, authorities, insurance institutions, creditors of the person concerned as well as other parties who may be involved including in the case of voluntary salary abandonment for claims due, social insurance institutions (including company health insurance funds), election committee for works council elections, labor inspectorate, traffic labor inspectorate and agricultural and forestry inspectorate – especially according to § 8 of the Labor Inspection Act, members of the workplace representation, apprenticeships according to § 19 of the Vocational Training Act and vocational schools, labor market service, construction workers'/holiday/severance pay, unions specified by the employee with consent of the person concerned, legal interest representation, works council funds in accordance with § 73 section 3 of the Labor Relations Act, company doctors, pension funds, co-insured persons, employee benefit funds pursuant to § 11 section 2 Z 5 and § 13 of the BMVG, customers, interested parties

The provision of your personal data is necessary to fulfill the contract or to carry out pre-contractual measures. We cannot conclude or carry out a contract with you without this data.

### 3.6. Access management for computer systems

- Purpose: Management of usernames and passwords as well as system access logging (user ID management).
- Legal basis: Article 6 section 1 c (fulfillment of a legal obligation, in particular compliance with access control measures, e.g., password policy or access authorizations, § 96a Austrian Labor Act); article 6 (1) (f) (legitimate interests, in particular defense, exercise and assertion of legal rights).
- Duration of storage: Data is deleted when the system rights of the person concerned have expired and all litigation in which the data is required as evidence is completed. In any case, all data will be deleted when there is no legal retention period necessary anymore.
- Recipient/beneficiary categories: customers, interested parties, system users

The provision of your personal data is necessary to fulfill the contract. We cannot operate our (software) systems safely without this data. Without this data, we cannot employ you in our company (employees) or fulfill a contract with you (customers).

### 3.7. Customer care and marketing for own purposes

- Purpose: Use of own or purchased customer and interested party data for the initiation of business regarding the own delivery or service offer as well as for the realization of advertising measures and newsletter distribution; customer relation management.
- Legal basis: Article 6 section 1 a (consent of the person concerned); Article 6 section 1 b (fulfillment of contract); Article 6 section 1 c (fulfillment of a legal obligation); Article 6 section 1 f (legitimate interests, especially the exercise, defense and assertion of legal rights)
- Duration of storage: The data will be stored until the end of the third year after the last contact with the person concerned and then deleted. Regarding newsletter distribution, data is deleted at the latest with revocation of consent (in particular § 107 of the telecommunications act).
- Recipient/beneficiary categories: Contract processors (e.g., newsletter services, telephone system operators)

#### 3.7.1. Remarketing/Retargeting

We use LinkedIn Insight Conversion, a tool by LinkedIn Corporation, 2029 Stierlin Court, Mountain View, CA 94043, USA, which allows us to obtain information regarding the use of our website and to present you with advertising content tailored to your interests on other websites. For this purpose, a cookie with validity of 120 days is set in your browser and enables LinkedIn to recognize you when you visit a website. LinkedIn uses the data

to compile anonymous reports for us regarding ad activity and information about how you interact with our website. You can deactivate the LinkedIn Insight Conversion Tool as well as interest-based advertising simply by opting out via the following link: <https://www.linkedin.com/psettings/guest-controls/retargeting-opt-out>

In case you are already a LinkedIn member, click on the “Decline LinkedIn” box.

Further information regarding data protection on LinkedIn can be found here: <https://www.linkedin.com/legal/privacy-policy#choices-oblig>

### 3.8. Product registration

- Purpose: formal registration of merchandise to be ordered for the client, in particular hardware, software licenses, manufacturer service contracts, domain names, digital certificates and IP addresses (including storage of documents generated during this activity).
- Legal basis: Article 6 section 1 b (fulfillment of contract); Article 6 section 1 f (legitimate interests, in particular defense, exercise and assertion of legal rights)
- Duration of storage: According to the legal storage or other discarding regulations.
- Recipient/beneficiary categories: Supplier/manufacturer, internet domain name registrar, digital certificate registrar, hardware/software suppliers and manufacturers in third country, international registrars for internet domain names, international registrars for digital certificates, RIPE network coordination center.

The provision of your personal data is necessary to fulfill the contract. We cannot carry out a contract with you without this data.

### 3.9. Video surveillance in the data center

- Purpose: Video surveillance for protection of conova communications GmbH data center property (or to prevent criminal offenses) only to be evaluated in specifically defined cases.
- Legal basis: § 12 section 2 in conjunction with section 3 DSG idF (Data Protection Deregulation Act 2018) in conjunction with article 6 section 1 f (legitimate interests of the person responsible, in particular preventative protection of persons and property); §§ 353 et seq. ABGB; § 80 Code of Criminal Procedure; Article 9 section 1 f (assertion, exercise or defense of rights); Article 10 GDPR in conjunction with § 4 section 3 DSG (legitimate interest – disclosure of records regarding criminal data to enforce rights to the relevant law enforcement agencies)
- Duration of storage: Generally, recorded data will be deleted after a period of 31 days at

the latest, unless specifically required for the realization of the underlying protection or evidence purposes (retention period authorized by the data protection authority; dated August 16, 2010 – 4002645/001)

- Recipient/beneficiary categories: Courts, authorities, insurance institutions – incident based.

### **3.10. Access control system – building**

- Purpose: Control of access rights to buildings and demarcated areas by the person responsible with help from the systems that automatically collect and store personal data, including automated and archived text documents (such as mail correspondence) – whereby no biometric data from those affected is processed.
- Legal basis: Article 6 section 1 a (consent of the person concerned); Article 6 section 1 b (contract fulfillment); Article 6 section 1 c (fulfillment of legal obligation to implement technical and organizational measures for the protection of personal data, § 96a Austrian Labor Constitutional Act); Article 6 section 1 f (legitimate interests, in particular defense, exercise and assertion of legal rights)
- Duration of storage: Until the end of the access authorization period and beyond, as long as legal retention periods exist, or as long as special legal claims can be asserted from the employment relationship or the customer relationship with conova. Provided there are no specific retention periods, the data will be deleted 6 months after the end of the access authorization period.
- Recipient/beneficiary categories: Customers, if required by contract or in special cases.

The provision of your personal data is necessary to fulfill the contract. We cannot operate a secure access control system without this data. We cannot employ you in our company (employees) or fulfill a contract with you (customers) without this information.

### **3.11. Access control system – Data center (biometric access system)**

- Purpose: Control of access rights to the data center with help from systems that automatically collect and store personal information, including automated and archived text documents (such as mail correspondence) – where biometric data from those affected is processed.
- Legal basis: Article 6 section 1 a (consent of the person concerned); Article 6 section 1 b (contract fulfillment); Article 6 section 1 c (fulfillment of legal obligation to implement technical and organizational measures to protect personal data, § 96a Austrian Labor Constitutional Act); Article 6 section 1 f (legitimate interests, in particular defense, exercise

and assertion of legal rights); Article 9 section 2 a (explicit consent from the person concerned); Article 9 section 2 f (assertion, exercise or defense of rights).

- Duration of storage: Until the end of the access authorization period and beyond, as long as legal retention periods exist, or as long as special legal claims can be asserted from the employment relationship or the customer relationship with conova. Provided there are no specific retention periods, the data will be deleted 6 months after the end of the access authorization period.
- Recipient/beneficiary categories: Customers, or others in special cases

The provision of your personal data is necessary to fulfill the contract. We cannot operate a secure access control system to the data center without this data. We cannot employ you in our company (employees) or fulfill a contract with you (customers) without this information.

### **3.12. Access control system – rack locking system**

- Purpose: Control of access to the server racks in the data centers with help from systems that automatically identify and store personal data, including automated and archived text documents (such as mail correspondence) whereby no biometric data from those affected is processed.
- Legal basis: Article 6 section 1 a (consent of the person concerned); Article 6 section 1 b (contract fulfillment); Article 6 section 1 c (fulfillment of legal obligation to implement technical and organizational measures to protect personal data, § 96a Austrian Labor Constitutional Act); Article 6 section 1 f (legitimate interests, in particular defense, exercise and assertion of legal rights).
- Duration of storage: Until the end of the access authorization period and beyond, as long as legal retention periods exist, or as long as special legal claims can be asserted from the employment relationship or the customer relationship with conova. Provided there are no specific retention periods, the data will be deleted 6 months after the end of the access authorization period.
- Recipient/beneficiary categories: Customers

The provision of your personal data is necessary to fulfill the contract. We cannot operate a secure access control system to the server racks without this data. We cannot employ you in our company (employees) or fulfill a contract with you (customers) without this information.

### **3.13. Telephone system**

- Purpose: Digital telephone system with accurate recording of all call data, telephone activities and voice recordings for quality assurance in the call center area.

- Legal basis: Article 6 section 1 a (consent of the person concerned); Article 6 section 1 f (legitimate interests of the personal responsible, in particular regarding quality assurance of telephone inquiries).
- Duration of storage: Telephone system log files are stored for 1 month, call recordings are stored for 3 months and then deleted.
- Recipient/beneficiary categories: Contract processors (e.g., newsletter companies, telephone system operators).

### 3.14. Visitor management

- Purpose: Logging of customer attendance, interested parties and suppliers who have access to areas considered security sectors according to ISO 27001 – in particular conova office areas.
- Legal basis: Article 6 section 1 a (consent of the person concerned); Article 6 section 1 f (legitimate interests, particularly compliance with documentation requirements according to ISO 27001 standards)
- Duration of storage: In accordance with the storage and discarding laws, in any case at least 7 years – longer if a lawsuit is pending.

### 3.15. Project management

- Purpose: Project management software for handling internal and external projects, including automatically generated and archived text documents (such as mail correspondence).
- Legal basis: Article 6 section 1 b (contract fulfillment); Article 6 section 1 f (legitimate interests, in particular defense, exercise and assertion of legal claims).
- Duration of storage: Until the end of the relationship with the person concerned and beyond as long as legal retention periods exist, or legal claims can be asserted.
- Recipient/beneficiary categories: Customers, interested parties, suppliers/manufacturers

The provision of your personal data is necessary to fulfill the contract. We cannot pursue projects with you (customers, interested parties, suppliers) or employ you in our company (employees) without this data.

### 3.16. Documentation system

- Purpose: System for the documentation of internal and external IT landscapes, including automatically supported and archived text documents (such as mail correspondence) as

well as system mapping.

- Legal basis: Article 6 section 1 b (contract fulfillment); Article 6 section 1 f (legitimate interests, in particular defense, exercise and assertion of legal claims)
- Duration of storage: Until the end of the relationship with the person concerned and beyond as long as legal retention periods exist, or legal claims can be asserted.

The provision of your personal data is necessary to fulfill the contract. Without this information we cannot conclude any contracts with you (customers, suppliers) or employ you in our company (employees).

### 3.17. Ticket system & mail

- Purpose: Service management system for the transparent recording and documentation of customer communication, including automatically supported and archived text documents (such as mail correspondence) as well as system mapping.
- Legal basis: Article 6 section 1 b (fulfillment of contract); Article 6 section 1 f (legitimate interests, in particular defense, exercise and assertion of legal claims)
- Duration of storage: Until the end of the relationship with the person concerned and beyond as long as legal retention periods exist, or legal claims can be asserted.
- Recipient/beneficiary categories: Customers, interested parties, suppliers/manufacturers

Since tickets can also be sent to the ticketing system via Email, this must be mentioned here for the sake of completeness. The security check of our incoming E-mails is carried out by the company Hornetsecurity. They carry out data checks for malware and remove whatever is necessary.

The provision of your personal data is necessary for the fulfillment of the contract and for the transparent recording and documentation of customer communication. Without this data, we cannot conclude or fulfill a contract with you (customers, interested parties and suppliers) or employ you in our company (employees).

### 3.18. conova App

- Purpose: To make the app available; to further develop the app; to improve the functions of the app and our service; in order to trace and track attacks as well as to protect our systems and prevent abusive or fraudulent behavior, log files are saved. These consist of the IP address, the mobile device, the access date and time, the client's request, the http response code, the amount of data transferred, and the app version used. No personal user profiles are created. There is no access to the log files stored in the system. These are automatically queried each time the app starts.
- Legal basis: Article 6 section 1 lit. b (fulfillment of contract); Article 6 section 1 lit. f

(legitimate interests) – storage period: Until the app is deleted, and beyond as long as statutory retention periods exist, or legal claims can be asserted.

- Recipient/beneficiary categories: exclusively for internal conova use.

Our app accesses the following device functions via the interfaces of your mobile device: Internet

– The app retrieves content such as texts and images from the internet; Wi-Fi connection information – The app uses the Wi-Fi connection from your mobile device, in order to establish a connection to the internet and thus enable you to use the app to its full potential. The prerequisite for this is that the Wi-Fi function on the mobile device is activated. The app is available in the usual stores (Google Playstore and Apple Appstore).

The provision of your personal data is necessary to fulfill the contract. Without this data, we cannot enable you to use the app.

### **3.19. Push notifications**

Push notifications are messages that are sent from the app to the device, where they are then displayed with priority. You can switch these notifications on and off in the app settings of your mobile device. When you activate push notifications for the first time - for example when you start the app for the first time – a unique identification number corresponding to your mobile device (device ID) is communicated to the service that provides the push functionality at your operating system provider (for Android: Google Cloud Messaging, for iOS: Apple Push Notification Service). This service presents with a so-called 'identifier' (push notification identifier) that does not allow for conclusions to be drawn regarding the device ID or about the user. Communication then always takes place with this identifier. This ensures that the device ID is no longer used.

- Purpose: Delivery of push messages at the request of the user
- Legal basis: Article 6 section 1 lit. b (fulfillment of the contract); article 6 section 1 lit. f (legitimate interests)
- Duration of storage: Duration of use of the push service
- Recipient/beneficiary categories: Provider of the push functionality (for Android: Google Cloud Messaging, for iOS: Apple Push Notification Service); affected data: device ID.

### **3.20. Integration of YouTube videos**

We have integrated YouTube videos from YouTube LLC, 901 Cherry Ave, San Bruno, CA 94066, USA ("YouTube"), into our service offering that are stored on <https://www.youtube.com> and can be played directly from our website. We have included this service in order to enable you the most convenient use of the website. Cookie consent is required for this purpose.

When you visit our website, YouTube is informed that you have accessed a corresponding subpage of our website. Log data is also transmitted. This takes place regardless of whether YouTube provides a user account that you are logged in to or not. If you are logged in to Google, your data will be assigned directly to your account. If you do not wish for this data to be assigned to your profile on YouTube, you must log out prior to visiting our website. YouTube saves your data as a user profile and uses this information for advertising, market research and/or needs-based design of its website. This type of evaluation takes place in particular (even for users who are not logged in) in order to provide needs-based advertising and to inform other users within the social network about your activities on our website. You reserve the right to object to the creation of such user profiles, but you must contact YouTube directly to exercise this right.

Further information regarding the purpose and scope of data collection and its processing by YouTube can be found within the YouTube privacy policy. There, you will also find further information regarding your rights and the setting options to protect your privacy: <https://policies.google.com/privacy?hl=de>.

- Purpose: Provision of videos
- Legal basis: Article 6 section 1 S. 1 lit. a GDPR
- The following data is processed: Device information, IP address, referrer URL, videos viewed, etc.
- Duration of storage: 6 months
- Recipient: Google LLC, Google Ireland Limited

### **3.21 Integration of Google Maps**

We have integrated Google Maps from Google Ireland Limited Google Building Gordon House, 4 Barrow St, Dublin, D04 E5W5, Ireland into our online service that are stored on maps.google.com and can be accessed directly via our website. The integration of Google Maps has been undertaken to enable you to conveniently use the website. This requires cookie consent.

- Legal basis Article 6 section 1 S. 1 lit. f GDPR

When you visit our website, Google is informed that you have accessed a corresponding subpage of our website. Log data is also transmitted. This takes place regardless of whether Google provides a user account that you are logged in to or not. If you are logged in to Google, your data will be assigned directly to your account. If you do not wish for this data to be assigned to your profile on Google, you must log out prior to visiting our website. Google saves your data as a user profile and uses this information for advertising, market research and/or needs-based design of its website. This type of evaluation takes place in particular (even for users who are not logged in) in order to

provide needs-based advertising and to inform other users within the social network about your activities on our website. You reserve the right to object to the creation of such user profiles, but you must contact Google directly to exercise this right.

- Purpose: Presentation of map information
- Legal basis: Article 6 section 1 S. 1 lit. f GDPR
- The following data is processed: Date and time of visit, IP address, usage data, location information, URL, etc.
- Duration of storage: 6 months
- Recipient: Google LLC, Google Ireland Limited

Further information regarding the purpose and scope of data collection and its processing by Google Maps can be found within Google's privacy policy. There, you will also find further information regarding your rights and the setting options to protect your privacy: <https://policies.google.com/privacy?hl=de>.

### **3.22. HubSpot**

This website uses HubSpot, a service of HubSpot Inc., a software provider from the USA with branches in Ireland (HubSpot Inc., 2<sup>nd</sup> Floor 30 North Wall Quay, Dublin 1, Ireland) and Germany (HubSpot Germany GmbH, Am Postbahnhof 17, 10243 Berlin), with which we cover various aspects of our online marketing. These include:

- E-Mail Marketing (newsletters and automated mail)
- Social Media Publishing & Reporting (e.g., LinkedIn, Facebook)
- Google Ads
- Reporting (e.g., traffic sources, accesses, etc.)
- Contact management (e.g., user segmentation and CRM)
- Provision of contact forms and appointment bookings (calenders)
- Provision of landingpages and live-chat

HubSpot uses cookies that are stored on your computer that enable us to analyze your use of the website. HubSpot then evaluates the collected information on our behalf in order to generate reports regarding the pages visited. Should you wish that your cookies not be recorded, you can prevent their storage at any time using your browser settings.

The data we collect through HubSpot is used by us exclusively to provide and optimize our marketing. Your data can then be used by us to contact you as a visitor to our website and to determine which of our services were interesting to you. If you subscribe to our email news and download studies and other documents, we can use HubSpot to record your visits using your

additional information (particularly name/email address) and, if necessary, send you specific information about your preferred topics. Where it is required by law, we will ask for your consent beforehand and separately regarding the collection, storage and processing of your data. You reserve the right to revoke this consent at any time.

- Purpose: Management of online marketing activities and statistics
- Legal basis: Article 6 section 1 S. 1 lit. a GDPR
- The following data is processed: IP address, duration of the visit and pages viewed, browser information, operating system, referrer URL, time of access, clickstream data, aggregated usage, device ID, device model, domain name, files viewed, geographic location of internet service provider, navigation information, login data for subscription service, etc.
- Duration of storage: session / 30 minutes / 1 day / 1 year / 13 months
- Recipient: HubSpot Inc

### 3.23. Matomo

This website uses the web analysis service Matomo, which is an open-source project.

- Purpose: gather statistical data regarding the website visit for the purpose of ongoing optimization of it.
- Legal basis: Article 6 section 1 lit. f (legitimate interests, in particular to improve our own services for the benefit of the users); § 96 section 3 TKG 2003
- The following data is processed: IP address (with the extension 'AnonymizeIP', so that a direct personal relationship can be excluded; the transmitted IP address is not merged with other data collected), the pages accessed and the time of access, referrer (the page from which a user has come to the website), browser and operating system, length of stay on the website and device type, etc.
- Duration of storage: 13 months
- Recipient/beneficiary categories: none, internal use only

The information collected in this manner is stored by us exclusively on a server located in Austria. You can find more information from the third-party regarding data protection at: <https://matomo.org/gdpr/>.

### 3.24. Fact Advisor

This website uses the web service Fact AI,

- Purpose: decision-support for end users via structured questions
- Legal basis: Art.6 para. 1 lit. f (legitimate interest, in particular to improve one's own services for the benefit of other users); § 96 Abs 3 TKG 2003
- The following data will be processed: IP addresses will be anonymized as soon as the process allows and will always be stored anonymously. The Fact Advisor works entirely without recording personal data if names, Emails, etc. are recorded by another tool (e.g., web forms).
- Storage period: no storage
- Recipients/categories of recipients: none, only internal use

For more information regarding data protection from third-party providers, please visit:  
<https://fact.ai/datenschutz.html>

### 3.25. Octopus

conova uses the analysis software from a Swiss company called Octopus Cloud AG.

- Purpose: The collection of necessary license information for potential notification to Microsoft as well as for the invoice preparation within the framework of SPLA agreements is carried out by a software component that is mandatory to install by conova or the customer and is on the basis of: <https://www.octopus.cloud/>
- Legal basis: Art. 6 para. 1 lit. f (legitimate interest, in particular to improve one's own services for the benefit of users); § 96 Abs 3 TKG 2003, as well as the GTC for SPLA of Microsoft Ireland
- The following data is processed: The software analyses, stores and transmits information regarding version, type of installed software, as well as relevant licensing information as required by the manufacturer, such as user account information (including name and Email address) to conova for the purpose of analysis and display in our TopHosting platform for the respective customer. Further, this information forms the basis for invoicing to our customers as well as proof of license compliance to Microsoft according to their terms and conditions.
- Storage period: 7 years according to HGB or AO and UstG (Value Added Tax Act)

The data hereby collected is stored by us exclusively on our own servers in Austrian data centers. Further information on data protection from third-party providers can be found here:  
<https://www.octopus.cloud/privacy-policy>

### 3.26. Services of Hornetsecurity GmbH

conova uses the cloud services of Hornetsecurity GmbH, a company based in Germany, for several of its products.

- Purpose: To protect and sensitize our customers' employees from various cybersecurity attacks.
- Legal basis: Art. 6 para. 1 lit. F (legitimate interest, in particular to improve one's own services for the benefit of users); § 96 Abs 3 TKG 2003
- The following data is processed: Information regarding content of emails, the recipients and senders is analyzed, stored and transmitted in order to generate fake Emails for training purposes.
- Storage period: Data is stored for the duration of the product use and then deleted by Hornetsecurity.

The data collected in this way is stored by us exclusively on servers in our or Hornetsecurity European data centers. For further information regarding data protection from third-party providers, please visit: <https://www.hornetsecurity.com/en/privacy/>

### 3.27. 506.Ai

We use the marketing and remarketing services provided by Google Inc. (1600 Amphitheatre Parkway, Mountain View, CA 94043, USA) on the basis of our legitimate interests (Article 6(1)(f) of the GDPR).

These services enable us to display targeted advertisements to users that correspond to their interests. When you visit our website and other websites where Google marketing services are active, a code from Google is executed. With the help of cookies or similar technologies, information such as visited web pages, interests, clicks, browser and operating system data, and the IP address is collected. The IP address is truncated within the EU or the EEA and is only transferred in full to the USA in exceptional cases. The information may be combined by Google with data from other sources to display tailored adverts to users.

The data is processed pseudonymously, i.e. Google does not store personal data such as names or email addresses, but works with pseudonymous user profiles. Users can opt out of personalised advertising.

We use Google Ads, among other tools, to generate conversion statistics. These show how many users have clicked on an advert without allowing conclusions to be drawn about the identity of individual users. In addition, we use Google Optimizer for A/B testing and Google Tag Manager to manage the tags used.

### 3.28. Google Marketing Services

We use the marketing and remarketing services provided by Google Inc. (1600 Amphitheatre Parkway, Mountain View, CA 94043, USA) on the basis of our legitimate interests (Article 6(1)(f) of the GDPR).

These services enable us to display targeted advertisements to users that correspond to their interests. When you visit our website and other websites where Google marketing services are active, a code from Google is executed. With the help of cookies or similar technologies, information such as visited web pages, interests, clicks, browser and operating system data, and the IP address is collected. The IP address is truncated within the EU or the EEA and is only transferred in full to the USA in exceptional cases. The information may be combined by Google with data from other sources to display tailored adverts to users.

The data is processed pseudonymously, i.e. Google does not store personal data such as names or email addresses, but works with pseudonymous user profiles. Users can opt out of personalised advertising.

We use Google Ads, amongst other tools, to generate conversion statistics. These show how many users have clicked on an advert without allowing conclusions to be drawn about the identity of individual users. In addition, we use Google Optimizer for A/B testing and Google Tag Manager to manage the tags used.

### 3.29. Services provided by Dacoso GmbH for SOC services

Upon request, conova provides managed SOC and cyber security services in collaboration with dacoso.

- Purpose: early detection of security incidents and threats, as well as the investigation, containment and resolution of cyber security attacks
- Legal basis: Article 6(1)(b) and (f) of the GDPR, Section 96(3) of the TKG 2003
- The following data is processed: log data from networks, endpoints and applications, as well as cloud and infrastructure data
- Retention period: Data is stored for the duration of product use

The information collected in this way is stored by us exclusively on servers in our own or European data centres. Further information from the third-party provider regarding data protection can be found at: <https://dacoso.com/en/privacy-policy/>

### 3.30. N-Able

- conova uses cyber security services provided by N-Able. Purpose: security monitoring, early detection of security incidents and threats, as well as the investigation, containment and resolution of cyber security attacks
- Legal basis: Article 6(1)(b) and (f) of the GDPR, Section 96(3) of the Telecommunications Act 2003
- The following data is processed: log data from networks, endpoints and applications, as well as cloud and infrastructure data
- Retention period: Data is stored for the duration of product use

Further information from the third-party provider regarding data protection can be found at <https://www.n-able.com/legal/privacy>

### 4. Information regarding data transfers to third countries or international organizations

With the exception of processing of 'product registration', we do not transfer your personal information to third countries or to international organizations in the above-mentioned data processing activities. We would like to point out that the ECJ no longer certifies an adequate level of data protection for the USA. In the case of the following companies, we cannot currently guarantee that data will not be transferred to the USA: Google LLC., Apple Inc., ZSacler, Amazon Inc., Hornetsecurity GmbH, HubSpot. Therefore, there is a possibility that your data will be subject to access from US authorities for control and surveillance purposes and that no effective legal remedies are available.