Privacy Policy
- Controller according to the GDPR
- Data collection on our website
- Technologies on our website
  - Brevo (formerly SendInBlue)
  - External payment providers
  - Competitions / promotions
  - Google Signals for Google Analytics
  - Newsletter Registration
  - Online applications
  - Pingdom
  - Cloudflare
  - Cookies and Local Storage
  - Hosting
  - Google Analytics
  - Google Ad Manager (formerly DoubleClick for Publishers + DoubleClick Ad Exchange)
  - Google Tag Manager
  - jsDelivr
  - Contact
  - LinkedIn Insight Tag
  - Meta Pixel
  - Server-Logfiles
  - SSL Encryption
  - Webcare
  - Webcare Consent Conserve
  - Webcare Statistics
  - YouTube
  - The Hotels Network

General information on data protection
- Personal data
- Legal basis for the processing of personal data
- Transfer of personal data
- Cooperation with processors
- Transfer to third countries
- Data transfer to the U.S.
- Storage periods in general
- Storage periods in particular
- Rights of data subjects
- Assertion of rights of data subjects
- Privacy Notice – CCTV Surveillance

Privacy Policy

Last update: November 15, 2026

Thank you for your interest in the information on our website!

With the help of this Privacy Policy we would like to inform the users of our website about the type, scope and purpose of the personal data processed. Personal data in this context is all information that can be used to personally identify you as a user of our website (theoretically in an alternative way or by linking various data), including your IP address. Information that is stored in cookies is generally not or only in exceptional cases personally identifiable; however, cookies are covered by specific regulations that makes the permissibility of the use of cookies dependent on their purpose to a large extent on the active consent of the user.

In a general section of this Privacy Policy, we provide you with information on data protection, which generally applies to our processing of data, including data collection on our website. In particular, you as a data subject will be informed about the rights to which you are entitled.

The terms used in our Privacy Policy and our data protection practice are based on the provisions of the EU General Data Protection Regulation ("GDPR") and other relevant national legal provisions.

Controller according to the GDPR

VAYA Holding II GmbH
Registration Number: 511239y
Dr.-Helmut-Marsoner-Weg 3C
6175 Kematen in Tirol
Austria

e: datenschutz@vayagroup.at
t: +43 50 1256

Data Protection Officer:
Mr. Thiemo Sammern

Data collection on our website

On the one hand, personal data is collected from you when you expressly communicate such data to us, on the other hand, data, especially technical data, is automatically collected when you visit our website. Some of this data is collected to ensure that our website functions without errors. Other data may be used for analysis purposes. However, you can use our website without a need to provide personal information.

Technologies on our website

Brevo (formerly SendInBlue)

Provider: Sendinblue S.A.S, 7 Rue de Madrid, 75008 Paris, France, e-mail: dpo@brevo.com
Purpose: Sending newsletters, SMS and transactional emails and carrying out marketing automation
Category: Marketing
Recipient: EU
Processed data: Email addresses, names, telephone numbers, demographic information (e.g. location), interaction data (e. g. open rates, clicks on links)
Data subjects: Users
Technology: Cookies (details in the cookie list), tracking pixels, JavaScript, web beacons, API interfaces
Legal basis: Consent, legitimate interest, fulfillment of contract
Website: https://www.brevo.com
Further information:
https://www.brevo.com/legal/privacypolicy/
https://www.brevo.com/legal/termsofuse/

We use the Brevo service on our website to optimize our marketing communication and provide personalized content. The technical purpose of the tool is to create and execute automated email campaigns and to analyze the interaction with our customers.

Brevo allows users to design emails via an intuitive drag-and-drop interface. It offers ready-made templates and customization options for newsletter design. The platform collects data on user behavior, such as which links were clicked and whether emails were opened. This information is used to create targeted marketing campaigns and measure the success of the campaigns.

All relevant information about the cookies, including name, purpose of use and storage duration, is contained in our detailed list of cookies used.

The storage period of the data varies depending on the type of data and the statutory retention obligations. Once these periods have expired, the data is deleted immediately.

Additional details can be found in the linked further information. We recommend that you check these links regularly for changes, especially with regard to Brevo. Additional information on the rights of data subjects and the relevant contact details can be found in the general section of this privacy policy.

External payment providers

Category: General processing activity
Purpose: Execution of payments
Types of data: Payment, transaction, address, and communication data, technical processing information
Data subjects: Customers
Recipients: External payment providers, internal departments, technical processing service providers
Technologies: Payment processing and transaction systems
Legal basis: Contract fulfillment (payment execution), legitimate interest (security & proof), consent (voluntary additional data)

External payment providers are used to process payments. If a payment is made via such a provider, the information required for this purpose is transmitted to the respective service provider and processed there. This may include, in particular:

- Name
- Billing and delivery address
- Payment information (e.g., account details, credit card details, wallet details)
- Transaction amount
- Time of payment
- Other payment-related information required by the provider

The processing is carried out for the purpose of executing the payment transaction, assigning the transaction, implementing security and verification mechanisms, and handling any queries or clarifications. The payment providers used are clearly identified in the order process. The specific processing is based on the terms and conditions of the respective payment service provider. The legal basis is the necessity of processing to execute the payment transaction and our legitimate interest in secure and efficient payment processing. Additional data provided voluntarily is processed on the basis of consent.

The data is only stored for as long as is necessary for processing the payment or due to legal requirements. Data is only passed on to other third parties if this is necessary to execute the payment or if there are legal obligations to do so.

A selection of the data protection regulations of the most important payment service providers can be found here:

- Paypal: https://www.paypal.com/webapps/mpp/ua/privacy-full
- Klarna / Instant bank transfer: https://www.klarna.com/uk/privacy-notice/
- Skrill: https://www.skrill.com/en/footer/privacypolicy/
- Giropay: https://www.giropay.de/agb/index.html (in German)
- Visa: https://www.visa.co.uk/legal/privacy-policy.html
- Mastercard: https://www.mastercard.co.uk/en-gb/about-mastercard/what-we-do/privacy.html
- American Express: https://www.americanexpress.com/uk/legal/online-privacy-statement.html
- Apple Pay: https://www.apple.com/legal/privacy/
- Amazon Payments: https://pay.amazon.co.uk/help/201751600
- Flattr: https://flattr.com/privacy
- Google Pay: https://policies.google.com/privacy?hl=en-GB
- Stripe: https://stripe.com/privacy
- Unzer: https://www.unzer.com/en/data-protection/

Competitions / promotions

Category: General processing activity
Purpose: Conducting competitions and promotions
Types of data: Contact details, participation data, technical data
Data subjects: Participants

Recipients: Internal departments, organizational service providers
Technologies: Participation or form system
Legal basis: Consent (participation), contract fulfillment (prize processing)

Competitions or other promotions are occasionally offered on our website. The data entered in this context is processed in order to record participation, organize the implementation, conduct prize draws, and inform participants. In addition, technical transmission data is processed in order to securely process form entries and participation procedures.

In particular, the following data is processed:

- Name
- Contact
- Participation data or submitted content
- Information on eligibility to participate
- Other information necessary for determining and notifying the winners
- Technical data such as time of transmission or IP address

This data is processed on the basis of contract fulfillment, as it is absolutely necessary for participation in and execution of the competition. Participation is not possible without providing this data.

If data is additionally processed within the scope of the competition for purposes such as advertising, future contact, profiling, statistical evaluations, or the publication of entries, this is done exclusively on the basis of separate, voluntary consent. This consent can be revoked at any time with effect for the future without affecting participation in the competition (provided that the additional purposes are not necessary for this).

The data will only be stored for as long as is necessary for the implementation, documentation, or verification of the competition. Data will only be passed on to external service providers if this is necessary for technical or organizational processing.

Google Signals for Google Analytics

Provider: Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland, parent company: Google LLC (USA).
Purpose: Additional function to Google Analytics, Cross-device tracking
Category: Statistics
Recipients: EU, USA
Processed data: IP Address, User Data
Data subjects: Users
Technology: Add-on to Google Analytics
Legal basis: consent, data privacy framework, https://www.dataprivacyframework.gov/s/participant-search/participant-detail?id=a2zt000000001L5AAI&status=Active
Website: https://www.google.com
Further information:
Explanations about Google Analytics in this privacy statement
https://policies.google.com/privacy
https://safety.google/intl/en/principles/
https://business.safety.google/adsprocessorterms/
Here you can find out where exactly Google data centers are located:
https://www.google.com/about/datacenters/locations/

On our website, we have extended existing Google Analytics features with Google Signals. It is Google Signals a cross-device tracking of users, which is integrated within Google Analytics.

By activating Google Signals for Google Analytics, data is processed and assigned to your Google account. Google can thus recognize, for example, if you have viewed products on our website via your smartphone and only purchased them later via another end device, e.g. via your computer. Google Signals makes it possible to run cross-device campaigns.

By activating Google Signals for Google Analytics, user data such as location, search history and other data about the use of our website is collected. This gives us better information about interests and demographic characteristics. This information helps us to form specific target groups of users in Google Analytics in order to better respond to wishes and interests.

Personalization by Google Signals is only possible if a user is logged into his Google account and allows personalized advertising and if a user has consented to the use of Google Analytics on our website.

The privacy policy on the use of Google Analytics can also be found in this privacy policy.

Newsletter Registration

You can register for a newsletter on our website. The newsletter provides regular information about products, services, offers and promotions.

Consent to our newsletter is given in a so-called double opt-in procedure. After entering the e-mail address, a confirmation e-mail with an activation link is sent. Only after clicking on this link will the registration be completed and the e-mail address added to the mailing list. This procedure serves to ensure that only the owner of the specified e-mail address registers and that misuse by third parties is prevented.

When registering for the newsletter, the data provided (e-mail address), the time of registration and confirmation, the IP address and changes to the data are logged. This logging serves exclusively to prove proper registration and to protect against misuse.

The newsletter is only sent on the basis of express consent. In addition, the newsletter may also be sent to existing customers if the email address was collected in connection with the purchase of goods or services. In this case, information on similar products and services will be sent by email without the need to register separately for the newsletter.

You can unsubscribe from the newsletter at any time. A corresponding unsubscribe link can be found in every newsletter. Alternatively, you can also unsubscribe by contacting us.

After unsubscribing, the e-mail address and the associated verification data will be stored for a limited period of time in order to be able to prove previously given consent or the existing customer relationship if necessary. The data will only be stored for as long as is necessary to fulfill legal obligations to provide evidence and documentation or to defend against possible claims. The data is then deleted or anonymized. The data will not be used for any other purpose.

Additional information on the rights of data subjects and the relevant contact details are listed in the general section of this privacy policy.

Online applications

Category: General processing activity
Purpose: Carrying out the application process
Types of data: Application and communication data, voluntary information
Data subjects: Applicants
Recipients: Internal departments, HR service providers
Technologies: Application form or application platform
Legal basis: Decision on an employment relationship, legitimate interest (internal processes), consent (voluntary additional information)

Applications can be submitted via our website. The information provided is processed in order to review the application and carry out the selection process. The data processed may include, in particular:

- Name
- Contact details
- Cover letter
- Resume
- Certificates and proof of qualifications
- Other application documents provided by you

- Technical metadata such as transmission time or IP address

The processing is carried out for the purpose of conducting the application process, assessing professional and personal suitability, and establishing contact. If necessary, data may be passed on internally to the relevant departments or specialist departments. The legal basis for this is the decision to establish an employment relationship and our legitimate interest in the proper and transparent execution of the application process.

Application data will only be stored for as long as is necessary for the selection process. If no appointment is made, the documents will be deleted after completion of the process, provided that there are no legal retention obligations or that longer storage has been expressly agreed. Data will only be passed on to third parties if this is necessary for the technical provision or processing of the online application.

Pingdom

On our website we use the monitoring system Pingdom from Solarwinds, 7171 Soutwest Parkway, Bldg 400, Ausin, Texas 78735, USA ("Solar Winds").

ATTENTION! Within the scope of this service, data transfer to the U.S. takes place or cannot be excluded. We would like to point out that as of July 10, 2023, the European Commission has issued an adequacy decision on the EU-US data privacy framework (Data Privacy Framework). Accordingly, organizations or companies (as data importers) in the U.S. that are registered in a public list under the self-certification option of the Data Privacy Framework provide an adequate level of protection for data transfers. Whether the specific provider of this service is already certified can be found here: https://www.dataprivacyframework.gov/s/participant-search

This service uses cookies that are stored on your computer and that allow an analysis of the use of the website.

In this case, data, in particular the IP address and activities of the users can be transmitted to a server of the company Solarwinds in the USA and stored there. The use of Pingdom takes place in the interest of a continuous content and technical optimization of the website.

For more information about Pingdom, see https://www.solarwinds.com/pingdom and the Solarwinds Privacy Policy: https://www.solarwinds.com/legal/privacy

Cloudflare

Provider: Cloudflare, Inc, 101 Townsend St., San Francisco, CA 94107, USA
Representative in the EU: Cloudflare Portugal Unipessoal Lda, Praça Marquês de Pombal 14 7th floor, 1250-162 Lisboa, Portugal, DSA-legal-representative@cloudflare.com
Purpose: To measure and analyze website performance from the user's perspective
Category: Statistics
Recipient: USA
Processed data: Page load times, response times, web vitals metrics, URL, browser, operating system, country
Data subjects: Website visitors
Technology: JavaScript beacon, cookies (details in the cookie list)
Legal basis: Consent (purpose)
Certifications: EU-U.S. Data Privacy Framework, Swiss-U.S. Data Privacy Framework, UK Extension to the EU-U.S. Data Privacy Framework
Further information:
https://www.cloudflare.com/de-de/privacypolicy/
https://www.cloudflare.com/de-de/website-terms/

On our website, we use the Cloudflare Web Analytics service to measure and analyze website performance from the perspective of our users. This tool allows us to track and understand key performance metrics such as load times, responsiveness and visual stability of our website.

Cloudflare Web Analytics works by inserting a JavaScript snippet into HTML pages. This beacon collects data about the user experience, including metrics such as page load time, time to first byte and other web vitals. The tool also collects information about the browser used, the operating system and the user's country.

The collected data is updated in real time and is available shortly after a user request. This enables us to continuously monitor and improve the performance of our website. According to the manufacturer, Cloudflare Web Analytics does not use cookies for analysis purposes, but does use them to recognize users (identification cookie).

The data is stored for the duration of the statutory retention obligations and deleted immediately after this period has expired. Additional details can be found in the linked further information. We recommend that you check these links regularly for changes so that you are always informed about the current practices of Cloudflare Web Analytics.

Additional information on the rights of data subjects and the relevant contact details can be found in the general section of this privacy policy.

Cookies and Local Storage

We use cookies to make our website as user-friendly and functional as possible for you. Some of these cookies are stored on the device you use to access the site.

Cookies are small packages of data that are exchanged between your browser and our web server whenever you visit our website. They do not cause any damage and are used solely to recognise website visitors. Cookies can only store information provided by your browser, e.g. information that you have entered into your browser or that is available on the website. Cookies cannot execute code and cannot be used to access your terminal device.

The next time you access our website using the same device, the information stored in the cookies can then either be sent back to us (“first-party cookie”) or to a web application of third party to whom the cookie belongs (“third-party cookie”). The information that is stored and sent back allows each web application to recognise that you have already accessed and visited the website using the browser on your device.

Cookies contain the following information:

- Cookie name
- Name of the server from which the cookie originates
- Cookie ID number
- An expiry date, after which the cookie will be automatically deleted

We classify cookies in the following categories depending on their purpose and function:

- Technically necessary cookies, to ensure the technical operation and basic functions of our website. These types of cookies are used, for example, to maintain your settings while you navigate our website; or they can ensure that important information is retained throughout the session (e.g. login, shopping cart).
- Statistics cookies, to understand how visitors interact with our website by collecting and analysing information on an anonymous basis only. In this way we gain valuable insights to optimize both the website and our products and services.
- Marketing cookies, to provide targeted promotional and marketing activities for users on our website.
- Unclassified cookies are cookies that we are trying to classify together with individual cookie providers.

Depending on the storage period, we also divide cookies into session and persistent cookies. Session cookies store information that is used during your current browser session. These cookies are automatically deleted when the browser is closed. No information remains on your device. Persistent cookies store information between two visits to the website. Based on this information, you will be recognized as a returning visitor on your next visit and the website will react accordingly. The lifespan of a persistent cookie is determined by the provider of the cookie.

The legal basis for using technically necessary cookies is our legitimate interest in the technically fault-free operation and smooth functionality of our website. The use of statistics and marketing cookies is subject to your consent. These technologies are only activated after you have provided explicit consent via the cookie banner. You can withdraw your consent for the future use of cookies at any time. Your consent is voluntary. If consent is not given, no disadvantages arise. For more information about the cookies we actually use (specifically, their purpose and lifespan), refer to this Privacy Policy and to the information in our cookie banner about the cookies we use.

You can also set your web browser so that it does not store any cookies in general on your device or so that you will be asked each time you visit the site whether you accept the use of cookies. Cookies that have already been stored can be

deleted at any time. Refer to the Help section of your browser to learn how to do this.

Please note that a general deactivation of cookies may lead to functional restrictions on our website.

On our website, we also use so-called local storage functions (also called "local data"). This means that data is stored locally in the cache of your browser, which continues to exist and can be read even after you close the browser - as long as you do not delete the cache or data is stored within the session storage.

Third parties cannot access the data stored in the local storage. If special plug-ins or tools use the local storage functions, you are informed within the description of the respective plug-in or tool.

If you do not wish plug-ins or tools to use local storage functions, you can control this in the settings of your respective browser. We would like to point out that this may result in functional restrictions.

Hosting

In the context of hosting our website, all data that arises in connection with the operation and use of the website is processed. This includes, in particular, content data, usage data, communication data, and technical data that are necessary for providing and securely operating the website.

The storage and processing of this data is necessary to enable access to the website, ensure the stability and security of the online offering, and to technically optimize the website.

To provide our online presence, we use the services of external web hosting providers. In this context, the data generated during the operation of the website is transmitted to these service providers or processed by them on our behalf. Processing is carried out exclusively in accordance with legal requirements and based on contractual agreements for data processing on behalf.

Further information on the handling of personal data in connection with hosting can be found in the privacy policy of this website.

Google Analytics

Provider: Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland, Email: support-de@google.com
Parent Company: Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA
Purpose: Web analytics, performance measurement, conversion tracking, collection of statistical data
Category: Statistics
Recipients: EU, USA
Data Processed: Information about website visits (see detailed list below), user data. The IP address is used only briefly for rough location determination and is not stored afterward (see below).
Data Subjects: Website visitors
Technology: JavaScript call (Google tag / gtag.js), cookies (details in the cookie list), local storage
Legal basis: Consent
Legal basis for data transfer: EU-U.S. Data Privacy Framework, Swiss-U.S. Data Privacy Framework, UK Extension to the EU-U.S. Data Privacy Framework
Further information:
https://policies.google.com/privacy
https://safety.google/intl/de/principles/
https://business.safety.google/privacy/
https://business.safety.google/adsprocessorterms/
https://policies.google.com/technologies/ads
https://www.google.com/about/company/user-consent-policy-help
Here you can find out exactly where Google data centers are located: https://www.google.com/about/datacenters/locations/

Web and app activities collected via Google Analytics can be viewed and deleted by signed-in Google users under “My Activity” (myaccount.google.com/data-and-privacy).

On our website, we use the features of the web analytics service Google Analytics 4 (GA4) to analyze user behavior and optimize our website.

Google Analytics uses cookies that enable the analysis of our website's usage. Full details (name, purpose, retention period) regarding these cookies can be found in our specific list of cookies used. As an alternative to cookies, GA4 may use local storage to store the client ID in order to track user behavior even without a traditional cookie.
Information about website usage—such as browser type and version, operating system used, the previously visited page, the time of the server request, and approximate location—is transmitted to Google and processed there. We have entered into a contract with Google for this purpose.

With regard to IP addresses, there is no traditional "anonymization" in the sense of truncation after transmission; rather, GA4 is designed from the ground up so that IP addresses are neither logged nor stored for visitors from the EU, Switzerland, and the UK. The IP address is used only briefly to determine a rough location (city, region, country) and is then irrevocably discarded before it is stored on Google's servers. This is a feature built into GA4 that cannot be disabled; it is not an optional setting.

On our behalf, Google will use this information to analyze the use of our website, compile reports on activity on our website, and provide us with other services related to the use of our website.
During a visit to the website, user behavior is recorded in the form of so-called events. These may include the following:

- Page views, a user's click path
- First-time visit to our website
- Websites visited
- Start of a session
- Interaction with our website
- User behavior (e.g., clicks, scrolling, time spent on page, bounce rates)
- File downloads
- Ads viewed/clicked (only if Google Ads is linked to this property and Google Signals is enabled)
- Interaction with videos
- Internal search queries

The following is also collected:

- Approximate location (region, derived from the IP address, without storing the IP address itself)
- Date and time of the visit
- Technical information about the browser or the devices used (e.g., language setting, screen resolution)
- Internet service provider
- Referrer URL (the website or advertising channel through which a user arrived at our website)

This data is primarily processed by Google for its own purposes, such as profiling (over which we have no control).

Data regarding the use of our website is deleted immediately upon expiration of the retention period we have set. By default, Google Analytics specifies a retention period of 2 months for user and event data, with a maximum retention period of 14 months. This retention period also applies to conversion data. For all other event data, the following options are available: 2 months, 14 months, 26 months (Google Analytics 360 only), 38 months (Google Analytics 360 only), 50 months (Google Analytics 360 only). We select the shortest retention period that meets our intended purpose. You may inquire with us at any time regarding the retention period currently set by us. Data for which the retention period has expired is automatically deleted once a month.

Additional details can be found in the linked supplementary information. We recommend checking these links regularly for changes, as Google Analytics may update its features and privacy policies. Further information regarding your rights and our contact information can be found in the general section of this privacy policy.

Google Ad Manager (formerly DoubleClick for Publishers + DoubleClick Ad Exchange)

Provider: Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland
Parent Company: Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA
Purpose: Management, marketing, and display of advertising space on our website, including programmatic ad sales (real-time bidding) across multiple ad networks and exchanges

Recipients: EU, USA, and, where applicable, other third-party providers involved in the bidding process (demand-side platforms, ad networks)
Category: Marketing
Data processed: IP address (briefly for approximate location determination), cookie/device ID, information on page content and ad placements viewed, technical device information (browser, screen resolution)
Data subjects: Website visitors
Technology: JavaScript (Google Publisher Tag / gpt.js), cookies, and, if applicable, additional header bidding scripts from other providers participating in the bidding process
Legal basis: Consent
Legal basis for data transfer: EU-U.S. Data Privacy Framework, Swiss-U.S. Data Privacy Framework, UK Extension to the EU-U.S. Data Privacy Framework (Google LLC); for participating third-party providers without their own DPF certification, Standard Contractual Clauses (SCCs) apply
Website: https://www.google.com
Further information:
https://policies.google.com/privacy
https://safety.google/intl/de/principles/
https://business.safety.google/privacy/
https://business.safety.google/adsprocessorterms/
https://policies.google.com/technologies/ads
https://www.google.com/about/company/user-consent-policy-help
Here you can find out exactly where Google's data centers are located: https://www.google.com/about/datacenters/inside/locations/

This website uses the Google Ad Manager service to market and display our ad spaces. When a page containing an ad space is loaded, the browser sends a request to the Google ad server, whereupon the gpt.js script generates an ad request and forwards it to the server. The ad server checks the transmitted target values for the ad space (size, position, and, if applicable, targeting criteria) and delivers the appropriate ad. If ad spaces are sold programmatically via real-time bidding, multiple ad exchanges and third-party providers may participate in the auction simultaneously and process data in the process. In this case, granular consent is required that covers the individual providers involved, not just a blanket entry for "Google."

Google Tag Manager

Provider: Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland, Parent company: Google LLC (USA)
Purpose: Launching Tools and Plugins
Category: Technically Required
Recipients: EU, USA (possible)
Data processed: IP Address
Data subjects: User
Technology: JavaScript Call
Legal basis: legitimate interest
Legal basis for data transfer: EU-U.S. Data Privacy Framework, Swiss-U.S. Data Privacy Framework, UK Extension to the EU-U.S. Data Privacy Framework, https://www.dataprivacyframework.gov/s/participant-search/participant-detail?id=a2zt000000001L5AAI&status=Active
Website: https://www.google.com
Further information:
https://policies.google.com/privacy
https://safety.google/intl/en/principles/
https://business.safety.google/adsprocessorterms/
Here you can find out where exactly Google data centers are located: https://www.google.com/about/datacenters/locations/

The Google Tag Manager service is used on our website.

The Tag Manager is a service that allows us to manage website tags via an interface. This allows us to include code snippets such as tracking codes or conversion pixels on websites without interfering with the source code. In doing so, the data is only forwarded by the Tag Manager, but neither collected nor stored. The Tag Manager itself is a cookie-less domain and serves purely to manage other services in our online offering.

When the Google Tag Manager is started, the browser establishes a connection to Google's servers. These are mainly located in the U.S. Through this, Google obtains knowledge that our website was called up via the IP address of a user.

The Tag Manager ensures the resolution of other tags, which in turn may collect data. However, the Tag Manager does not access this data. If a deactivation has been made at the domain or cookie level, this remains in place for all tracking tags that are implemented with the Tag Manager.

jsDelivr

On our website, we use the open-source service jsDelivr to deliver content from our website as quickly as possible and in a technically flawless manner to various end user devices. The provider of this service is Prospect One sp. z o.o., Królewska 65A/1, PL-30-081 Kraków, Poland ("jsDelivr").

jsDelivr is a content delivery network (CDN) that mirrors the content on our website across different servers to ensure optimal accessibility worldwide. To make this possible, a CDN always uses servers that are geographically close to the respective user of our website. It can therefore be assumed that users within the EU are also provided with content by servers within the EU. In order to display content, jsDelivr uses user data such as the IP address.

According to the provider, jsDelivr does not set cookies or use other tracking mechanisms, but is only necessary for the technical reasons mentioned above. The legal basis for the transmission of personal data is therefore our legitimate interest in processing your personal data.

jsDelivr keeps personal data, as long as it is necessary for the provision of the described service or for the fulfillment of legal obligations.

To prevent this service, you can install a JavaScript blocker. However, this may result in the website no longer functioning as usual.

For more information on the use of your data, please refer to the provider's privacy policy at https://www.jsdelivr.com/terms/privacy-policy-jsdelivr-net

Contact

Our website offers various options for contacting us, for example via contact forms or e-mail addresses provided. When contacting us, the personal data provided will be processed exclusively for the purpose of processing and responding to the respective inquiry. The processing takes place insofar as this is necessary to carry out pre-contractual measures or to fulfill a contract, or on the basis of legitimate interests, for example to maintain customer relationships or to document processes.

It may be necessary to provide certain data in order to fully process an inquiry. Without this information, it may not be possible to process the request, or only to a limited extent.

Personal data from contact requests may also be stored in a customer or prospective customer database on the basis of legitimate interests in order to optimize communication and support. Use for marketing purposes only takes place if separate consent has been obtained or a legitimate interest exists and there are no overriding interests of the data subject that require protection.

Personal data from contact inquiries will only be stored for as long as is necessary for the processing and handling of the inquiry or for as long as there are statutory retention obligations. After final processing of the inquiry and expiry of any legal deadlines, the data will be deleted or anonymized. As a rule, deletion takes place at the latest after three years without further contact, unless there are longer statutory or contractual retention obligations.

Additional information on the rights of data subjects and the relevant contact details are listed in the general section of this privacy policy.

LinkedIn Insight Tag

Provider: LinkedIn Ireland Unlimited Company, Wilton Place, Dublin 2, Ireland, Email: info@linkedin.com
Parent company: LinkedIn Corporation, 2029 Stierlin Court, Mountain View, CA 94043, USA
Purpose: Website analysis, conversion tracking and optimization of LinkedIn advertising campaigns

Category: Marketing
Recipient: EU, USA
Processed data: IP address, time of visit, pages visited, device information, browser type, operating system, demographic data (e.g. job title, company, industry)
Affected: Website visitors
Technology: Cookies (details in the cookie list), JavaScript
Legal basis: Consent (purpose)
Certifications: EU-US Data Privacy Framework, Swiss-US Data Privacy Framework, UK Extension to the EU-US Data Privacy Framework
Website: https://business.linkedin.com/marketing-solutions/insight-tag
Further information:
https://www.linkedin.com/legal/privacy-policy
https://www.linkedin.com/help/lms/answer/85787 https://www.linkedin.com/help/linkedin/answer/a1445756?lang=en-US
https://www.linkedin.com/legal/l/linkedin-pages-terms
https://www.linkedin.com/legal/l/page-joint-controller-addendum

We use the LinkedIn Insight Tag service on our website to analyze website visits, track conversions, and optimize LinkedIn advertising campaigns. The LinkedIn Insight Tag is a JavaScript code implemented on our website. When a visitor visits our website, the tag loads and collects various data about the visit.

The tool collects information such as IP address, time of visit, pages visited, device information, browser type, and operating system. Additionally, demographic data such as job title, company, and industry are collected if the visitor is logged into LinkedIn. This data is aggregated and anonymized to gain insights into our website visitors and measure the performance of our LinkedIn campaigns.

The LinkedIn Insight Tag uses cookies to identify visitors across multiple sessions and to attribute conversions. All details (name, purpose, storage duration) regarding the cookies can be found in our specific list of cookies used.

The collected data is stored for a period of up to 90 days before being aggregated and anonymized. After the expiration of the statutory retention periods, the data is deleted immediately.

Additional details can be found in the linked additional information. We recommend checking these links regularly for changes, as LinkedIn may update the functionality of the LinkedIn Insight Tag. Additional information on the rights of data subjects and the corresponding contact details are provided in the general section of this privacy policy.

Meta Pixel

Provider: Meta Platforms Ireland Limited, 4 Grand Canal Square, Grand Canal Harbour, Dublin 2, Ireland, e-mail: privacy@facebook.com
Parent company: Meta Platforms, Inc, 1601 Willow Road, Menlo Park, CA 94025, USA
Purpose: Web analysis, tracking (conversion)
Category: Marketing
Recipient: EU, USA
Processed data: Visitor data (e.g. IP address, location data), behavioral data (e.g. clicks, duration of visit, conversion data), device data (e.g. browser type, operating system), e-commerce data (e.g. order ID, product information)
Data subjects: Website visitors
Technology: JavaScript, cookies (details in the cookie list), tracking pixels
Legal basis: Consent (purpose)
Legal basis for data transfer: EU-U.S. Data Privacy Framework, Swiss-U.S. Data Privacy Framework, UK Extension to the EU-U.S. Data Privacy Framework
Website: https://www.facebook.com/business/tools/meta-pixel
Further information:
https://www.facebook.com/privacy/policy/
https://www.facebook.com/legal/terms

The Meta Pixel service of the social network Facebook is used on our website for the analysis, optimization and economic operation of our online offer.

With the help of Meta Pixel, it is possible for Meta to determine the visitors to our website as a target group for the display of personalized ads. Accordingly, we use Meta Pixel to display the advertisements placed by us only to those users who have also shown an interest in our online offering or who have certain characteristics (e.g. interests in certain topics or

products determined on the basis of the websites visited) that we transmit to Meta (so-called “custom audiences”). With the help of Meta Pixel, we also want to ensure that our meta ads correspond to the potential interest of users and are not annoying. With the help of Meta Pixel, we can also track the effectiveness of the Meta Ads for statistical and market research purposes by seeing whether users were redirected to our website after clicking on a meta ad (so-called “conversion”).

The actions of users are stored in one or more cookies. These cookies make it possible to match Meta user data (such as IP address, user ID) with the data of a Facebook account. The data collected is anonymous and not visible to us and can only be used in the context of advertisements. Users can prevent the link to their Facebook account by logging out before taking any action.

To set which types of ads are displayed within Facebook, users can go to the page set up by Meta and follow the instructions on the settings for usage-based advertising: https://www.facebook.com/settings?tab=ads

The settings are platform-independent, i.e. they are applied to all devices, such as desktop computers or mobile devices.

Additional details can be found in the linked further information. It is recommended that you check these links regularly for changes, as Meta may update its functions and privacy policy. Further information on rights and contact details can be found in the general section of this privacy policy.

Server-Logfiles

Category: General processing activity
Purpose: Technical security, stability, and error analysis
Data types: Technical connection data and access data
Data subjects: Visitors to the online offering
Recipients: Hosting providers or technical service providers
Technologies: Server logs
Legal basis: Legitimate interest (technical operation & security)

When you visit our website, so-called server log files are automatically created. These log files contain the following data, which is automatically transmitted by the browser:

- IP address
- Date and time of access
- File or page accessed
- Amount of data transferred
- Notification of successful retrieval
- Browser type and version used
- Operating system used
- Referrer URL (previously visited page)
- Host name of the accessing device

This data is processed to ensure the functionality, security, and stability of our website, in particular to defend against or track attacks (e.g., DDoS attacks), for error analysis, and for the technical provision of the website. The legal basis for this is a legitimate interest in the secure and error-free provision of the website.

The log file data is automatically deleted after a standard technical period – after 12 weeks at the latest– once it is no longer required for the aforementioned purposes. Longer storage may occur in individual cases if data is required for evidence purposes (e.g., to investigate security-related incidents). This data is not merged with other data sources.

SSL Encryption

Within your visit to our website, we use the widespread SSL procedure (Secure Socket Layer) in conjunction with the highest level of encryption supported by your browser. You can tell whether an individual page of our website is transmitted in encrypted form by the closed representation of the key or lock symbol in the lower status bar of your browser. We use this encryption procedure on the basis of our justified interest in the use of suitable encryption techniques.

We also make use of suitable technical and organisational security measures to protect your data against accidental or intentional manipulation, partial or complete loss, destruction or against unauthorised access by third parties. Our security measures are continuously improved in line with technological developments and kept state-of-the-art.

Webcare

Provider: DataReporter GmbH, Zeileisstraße 6, 4600 Wels, Austria.
Purpose: Consent Management
Category: technically required
Recipient: EU, AT
Data processed: IP Address, Consent Data
Data subjects: Users
Technology: JavaScript call, Cookies, Swarmcrawler
Legal basis: Legitimate interest, consent (swarmcrawler to evaluate search results)
Website: https://www.datareporter.eu/
Further information: https://www.datareporter.eu/company/info

On our website, we use the Webcare tool for consent management. Webcare records and stores the decision of each user of our website. Our Consent Banner ensures that statistical and marketing technologies such as cookies or external tools are only set or started if the user has expressly consented to their use.

We store information on the extent to which the user has confirmed the use of cookies. The user's decision can be revoked at any time by accessing the cookie setting and managing the declaration of consent. Existing cookies are deleted after revocation of consent. For the storage of information about the status of the consent of the user, a cookie is also set, which is referred to in the cookie details. Furthermore, the IP address of the respective user(s) is transmitted to DataReporter's servers when this service is called up. The IP address is neither stored nor associated with any other data of the user, it is only used for the correct execution of the service.

With the help of Webcare, our website is regularly checked for technologies relevant to data protection. This investigation is only carried out for those users who have expressly given their consent (for statistical or marketing purposes). The search results of the users are evaluated by Webcare in an anonymous form and only in relation to technologies and used for the fulfillment of our information obligations. To start the Swarmcrawler technology, a request is sent to our servers and the IP address of the user is transmitted for the purpose of data transfer. Servers are selected which are geographically close to the respective location of the user. It can be assumed that for users within the EU, a server with a location within the EU will also be selected. The IP address of the user is not stored and is removed immediately after the end of the communication.

Webcare Consent Conserve

The WebCare Consent Conserve function enables us both to prove the consent of users of our website via our Consent Banner and to make the users' personal consent history transparent and traceable.

This function generates a unique Consent ID for each user and records every action concerning consent or revocation via our Consent Banner in connection with the Consent ID. The history of the user's decisions is stored in a protected memory area and can be viewed by the user at any time. For us as the website operator, an assignment of a history to a specific person can only take place after knowledge of the respective Consent ID.

Each action via the Consent Banner of a user is stored for 60 days and then automatically deleted. The storage location for the Consent ID is Frankfurt / Germany (EU). Only the Consent ID, the IP address and the data on the actions are saved.

The use of this function is based on our documentation and accountability obligations and our legitimate interest in this regard.

More information on this function can be found in the provider's help section at: https://help.datareporter.eu/docs/webcare/webcare_consent_conserve/

Further information on data protection can be found at: https://www.datareporter.eu/company/info

Webcare Statistics

The WebCare statistics function enables us to anonymously record the interactions of the users of our website with our Consent Banner. The statistics only record whether the Consent Banner was opened and which actions were carried out (purposes of consent, revocation). Only statistical data and no activities related to the specific user are stored. The visitor's IP address is only used for the purpose of the connection and is completely deleted after the connection is terminated.

The use of the WebCare statistics function is based on our legitimate interest in reviewing the performance of our Consent Banner and the related accessibility of our online offer.

The statistical data is stored for 30 days, older data is automatically deleted.

You can find more information about this function in the provider's help section at: https://help.datareporter.eu/docs/webcare/webcare_consent_statistic/

Further information on data protection can be found at: https://www.datareporter.eu/company/info

YouTube

Provider: Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland, parent company: Google LLC (USA)
Purpose: Integration of Video Content, Collection of Statistical Data
Category: Statistics
Recipients: EU, USA
Data processed: IP Address, Website Visit Details, User Data
Data subjects: Users
Technology: JavaScript Call, Cookies, Device Fingerprinting, Local Storage
Legal basis: Consent, Data Privacy Framework, https://www.dataprivacyframework.gov/s/participant-search/participant-detail?id=a2zt000000001L5AAI&status=Active
Website: https://www.youtube.com
Further information: https://www.youtube.com/intl/ALL_at/howyoutubeworks/user-settings/privacy/
https://policies.google.com/privacy
https://safety.google/intl/en/principles/
https://support.google.com/youtube/answer/10364219?hl=en

On our website, we use the YouTube service to embed videos.

We have activated the extended data protection mode on YouTube. According to YouTube, this mode means that YouTube does not store any information about visitors to this website before they watch a video. However, the disclosure of data to YouTube partners is not excluded by the extended data protection mode.

As soon as you start a YouTube video, a connection to YouTube's servers is established. This tells YouTube which of our pages you have visited. If you are logged into your YouTube account, you thereby enable YouTube to assign your surfing behaviour directly to your personal profile. This can be prevented by logging out of your account.

Furthermore, YouTube can save various cookies on your end device after starting a video or use comparable technologies (e.g. device fingerprinting). YouTube also uses the local storage on your end device. In this way, YouTube can obtain information about visitors to this website. This information is used, among other things, to collect video statistics, improve the user experience and prevent fraud attempts

The Hotels Network

Provider: THE HOTELS NETWORK, S.L.P, Avda. Diagonal, 439, 3º-1ª, 08036 Barcelona, Spain, e-mail: privacy@thehotelsnetwork.com
Purpose: To improve the online booking experience and increase direct bookings for hotels
Category: Marketing
Recipient: EU
Processed data: User behaviour on hotel websites, booking data, personalized offers, price comparisons, reviews
Data subjects: Website visitors
Technology: Cookies (details in the cookie list), JavaScript, Locals Storage
Legal basis: Consent (purpose)
Website: https://www.thehotelsnetwork.com/
Further information: https://thehotelsnetwork.com/en/privacy-policy https://thehotelsnetwork.com/en/instant-privacy-

policy
https://info.thehotelsnetwork.com/en/thn-terms

On our website, we use The Hotels Network service to improve the online booking experience for our guests and increase direct bookings. The tool offers a range of integrated functions to personalize and optimize the hotel website.

The Hotels Network collects anonymized data about user behavior on hotel websites, including pages visited, searches, rates displayed and bookings made. This data is used to create personalized offers and content for each visitor. The tool uses artificial intelligence and machine learning to predict user behavior and adapt the website accordingly.
Key features include price comparisons, review summaries and personalized messaging options. The Hotels Network also uses predictive personalization to automatically tailor messaging and offers to each user. The Hotels Network's BenchDirect tool also provides hotels with competitive data on the performance of their direct sales channel.

Data is collected via JavaScript and cookies implemented on the hotel website. All relevant information about the cookies, including name, purpose and storage duration, is included in our detailed list of cookies used. The Hotels Network uses the browser's local storage.

The storage period of the collected data is based on the statutory retention obligations. Once these periods have expired, the data is deleted immediately. Additional details can be found in the linked further information. We recommend that you check these links regularly for changes in order to stay informed about the current practices of The Hotels Network. Additional information on the rights of data subjects and the relevant contact details can be found in the general section of this privacy policy.

General information on data protection

The following provisions in its principles apply not only to the data collection on our website, but also in general to other processing of personal data.

Personal data

Personal data is information that can be assigned to you individually. Examples include your address, your name as well as your postal address, email address or telephone number. Information such as the number of users who visit a website is not personal data because it is not assigned to a person.

Legal basis for the processing of personal data

Unless more specific information is provided in this Privacy Policy (e.g. in the case of the technologies used), we may process personal data from you on the basis of the following legal principles:

- **consent in accordance with Art. 6 paragraph 1 lit. a of the GDPR** - The data subject has given his or her consent to the processing of his or her personal data for one or more specific purposes.
- **Fulfillment of a contract and pre-contractual measures pursuant to Art. 6 paragraph 1 lit. b of the GDPR** - Processing is necessary for the fulfillment of a contract to which the data subject is a party or for the implementation of pre-contractual measures.
- **Legal obligation pursuant to Art. 6 paragraph 1 lit. c of the GDPR** - Processing is necessary for the performance of a legal obligation.
- **Protection of vital interests pursuant to Art. 6 paragraph 1 lit. d of the GDPR** - Processing is necessary to protect the vital interests of the data subject or of another natural person.
- **Reasonable interests pursuant to Art. 6 paragraph 1 lit. f of the GDPR** - The processing is necessary to protect the legitimate interests of the controller or of a third party unless the interests or fundamental rights and freedoms of the data subject prevail.

Please note that in addition to the provisions of the GDPR, national data protection regulations may apply in your or our home country.

Transfer of personal data

Your personal data will not be transferred to third parties for purposes other than those listed in this Privacy Policy.

We will only transfer your personal data to third parties if:

- you have given your express **consent** in accordance with **Art. 6 paragraph 1 lit. a of the GDPR** ,
- the transfer pursuant to **Art. 6 paragraph 1 lit. f of the GDPR** is necessary to safeguard **reasonable interests,** as well as to assert, exercise or defend legal claims and there is no reason to assume that you have a prevailing interest worthy of protection by not disclosing your data,
- there is a **legal obligation** to transfer the data in accordance with **Art. 6 paragraph 1 lit. c of the GDPR,** as well as this is legally permissible and / or
- it is required according to **Art. 6 paragraph 1 lit. b of the GDPR** for the **processing of contractual relationships** with you.

Cooperation with processors

We carefully select our service providers who process personal data on our behalf. If we commission third parties to process personal data on the basis of a data processing agreement, this is done in accordance with **Art. 28 of the GDPR** .

Transfer to third countries

If we process data to a third country or if this is done in the context of using the services of third parties or disclosure or transfer of data to other persons or companies, this is only done on the legal basis described above for the transfer of data.

Subject to express consent or contractual necessity, we process or allow data to be processed only in third countries in accordance with **Art. 44 - 49 of the GDPR** with a recognized level of data protection or on the basis of special guarantees, such as contractual obligations through so-called standard contractual clauses of the EU Commission, the existence of certifications or binding corporate rules.

Data transfer to the U.S.

We would like to explicitly point out that as of July 10, 2023, the EU Commission has issued an adequacy decision on the EU-US data protection framework (Data Privacy Framework) pursuant to Art. 45 paragraph 1 GDPR. Accordingly, organizations or companies (as data importers) in the US that are registered in a public list as part of the self-certification of the Data Privacy Framework provide an adequate level of protection for data transfers. Whether the specific provider of a service is already certified can be found here: https://www.dataprivacyframework.gov/s/participant-search

The Data Privacy Framework provides a valid legal basis for the transfer of personal data to the USA. This creates binding guarantees to comply with all ECJ requirements; for example, it provides that access by U.S. intelligence services to EU data is limited to a necessary and proportionate level and that a data protection review court is created to which individuals in the EU also have access.

If a transfer of data by us to the US takes place at all or if a service provider based in the US is used by us, we refer to this explicitly in this Privacy Policy (see in particular the description of the technologies used on our website).

It should be noted that aside from significant improvements, the Data Privacy Framework is only partial and only applies to data transfers to those data importers in the U.S. that appear on the public list of certified organizations/companies.

What can the transfer of personal data to the US mean for you as a user and what risks are involved?

Risks for you as a user as far as data importers in the USA are concerned, which are not covered by the Data Privacy Framework, are in any case the powers of the US secret services and the legal situation in the U.S., which currently, according to the European Court of Justice, no longer ensure an adequate level of data protection. Among others, these are the following:

- Section 702 of the Foreign Intelligence Surveillance Act (FISA) does not provide for any restrictions on the surveillance measures of the secret services or guarantees for non-US citizens.
- Presidential Policy Directive 28 (PPD-28) does not provide effective remedies for those affected against actions by U.S. authorities and does not provide barriers to ensuring proportionate measures.

- The ombudsman provided for in the Privacy Shield does not have sufficient independence from the executive; he cannot issue binding orders to the U.S. secret services.

Legally compliant transfer of data to the U.S. on the basis of the standard contractual clauses for data importers not covered by the Data Privacy Framework?

In June 2021, the European Commission adopted new Standard Contractual Clauses (SCC) in Decision 2021/914/EU. These create a new legal basis for data transfers where the level of data protection is not the same as in the EU.

Legally compliant transfer of data to the U.S. based on consent?

If a data transfer to a service provider based in the U.S. takes place that is not covered by the Data Privacy Framework and this data transfer is based on explicit consent, we provide explicit information about this in this privacy policy, in particular in the description of the technologies used on our website.

What measures do we take to ensure that data transfers to the U.S. are legally compliant?

Where US providers offer the option, we choose to process data on EU servers. This should technically ensure that the data is located within the European Union and that access by US authorities is not possible.

Storage periods in general

If no explicit storage period is specified during the collection of data (e.g. in the context of a declaration of consent), we are obliged to delete personal data in accordance with **Art. 5 paragraph 1 lit. e of the GDPR** as soon as the purpose for processing has been fulfilled. In this context, we would like to point out that legal storage obligations represent a legitimate purpose for the further processing of affected personal data.

Personal data will be stored and retained by us in principle until the termination of a business relationship or until the expiry of any applicable guarantee, warranty or limitation periods, in addition, until the end of any legal disputes in which the data is required as evidence, or in any event until the expiry of the third year following the last contact with a business partner.

Storage periods in particular

As part of the description of individual technologies on our website, there are specific references to the storage period of data. In our cookie table, you will be informed about the storage period of individual cookies. In addition, you always have the possibility to ask us directly about the specific storage period of data. To do so, please use the contact data listed in this Privacy Policy.

Rights of data subjects

Data subject have the right:

- (i) **in accordance with Art. 15 of the GDPR, to request information** about your personal data processed by us. In particular, you may request information on the purposes of processing, the category of personal data, the categories of recipients to whom your data has been or will be disclosed, the planned duration of storage, the existence of a right of rectification, deletion, restriction of processing or opposition, the existence of a right of appeal, the origin of your data, if not collected by us, as well as the existence of automated decision making including profiling and, where applicable, meaningful information on the details thereof;
- (ii) **in accordance with Art. 16 of the GDPR,** to demand without delay the **correction** of incorrect or incomplete personal data stored by us;
- (iii) **in accordance with Art. 17 of the GDPR, under specific circumstances** to demand the **deletion** of your personal data stored with us, unless the processing is necessary to exercise the right to freedom of expression and information, to fulfill a legal obligation, for reasons of public interest or to assert, exercise or defend legal claims;
- (iv) **in accordance with Art. 18 of the GDPR,** to demand the (temporary) **restriction of the processing** of your personal data, insofar as the accuracy of the data is disputed by you, the processing is unlawful, but you refuse to delete it and we no longer require the data, but you require it for the assertion, exercise or defense of legal claims or you have lodged an objection to the processing in accordance with Art. 21 of the GDPR;

- (v) **in accordance with Art. 20 of the GDPR,** to receive your personal data that you have provided to us in a structured, common and machine-readable format or to request that it be transferred to another controller; However, this only covers those of your personal data that we process with the help of automated processes after your consent or on the basis of a contract with you;
- (vi) **in accordance with Art. 21 of the GDPR,** if your personal data are processed on the basis of our legitimate interest, **to object** to the processing of your personal data for reasons arising from your specific situation or if the objection is directed against direct advertising. In the latter case, you have a general right of objection, which we will implement without indicating a specific situation.
- (vii) **in accordance with Art. 7 paragraph 3 of the GDPR,** you may at any time **revoke your consent** to us. As a result, we may no longer continue the data processing based on this consent in the future. Among other things, you have the option of revoking your consent to the use of cookies on our website with effect for the future by calling up our **Cookie Settings.**
- (viii) **in accordance with Art. 77 of the GDPR** to **complain** to a data protection authority regarding the illegal processing of your data by us. As a rule, you can contact the data protection authority at your usual place of residence or workplace or at the headquarters of our company.

The responsible data protection authority for VAYA Holding II GmbH is:

Österreichische Datenschutzbehörde
Barichgasse 40-42, 1030 Wien, Österreich
Tel.: +43 1 52 152-0, dsb@dsb.gv.at

Assertion of rights of data subjects

You yourself decide on the use of your personal data. Should you therefore wish to exercise one of your above-mentioned rights towards us, you are welcome to contact us by email at datenschutz@vayagroup.at or by post, as well as by telephone.

Please assist us in specifying your request by answering questions from our responsible employees regarding the specific processing of your personal data. If there are reasonable doubts about your identity, we may request a copy of your identification.

For questions regarding data protection, you can reach us at datenschutz@vayagroup.at or at the other contact details stated in this Privacy Policy.

Privacy Notice – CCTV Surveillance

Data Controller

VAYA Holding II GmbH, Dr.-Helmut-Marsoner-Weg 3C, 6175 Kematen in Tirol, Austria, together with the operating company of the respective VAYA resort (collectively referred to as "VAYA").

CCTV cameras are in operation on the premises and record video footage to help prevent and investigate criminal offences and other exceptional incidents. The system does not use facial recognition or any other form of automated identification.

The processing of CCTV footage is based on VAYA's legitimate interest in protecting people, property and company assets.

Footage is generally retained for 72 hours. If required for the investigation of an incident or for legal proceedings, the relevant recordings will be kept for as long as necessary to complete the process.

Where necessary, footage may be disclosed to competent public authorities or courts (for use as evidence in criminal or civil proceedings), law enforcement authorities, employees, witnesses and affected persons (for the establishment, exercise or defence of legal claims), insurance companies (solely for handling insurance claims), legal advisers and other competent authorities where required for the enforcement or defence of legal rights.

CCTV footage may also be processed by service providers acting on behalf of VAYA. These processors act only on VAYA's instructions, may not use the data for their own purposes and are contractually bound to comply with the requirements of the General Data Protection Regulation (GDPR).

Personal data will not be transferred to recipients outside the European Union or to international organisations. No automated decision-making, including profiling, takes place.

You have the right to request access to your personal data, to have inaccurate data corrected and, where applicable, to request its deletion. You also have the right to request restriction of processing, to object to the processing of your personal data and to lodge a complaint with the competent data protection supervisory authority.

Kematen in Tirol , on November 15, 2026

Download as PDF