

Data Protection Policy

KENDRIS-Group

Version 01.01.2026

Content

1	Contact	3
1.1	Responsibility	3
1.2	Data Protection Officer	3
1.3	EU-Representative	3
2	Data Protection at KENDRIS	3
2.1	Collection and processing of personal data	3
2.2	Purposes of data processing and legal basis	4
2.3	Data disclosure and data transfer abroad	5
2.4	Duration of data processing	6
2.5	Rights of the data subject	6
2.6	Data security	7
3	Video surveillance	7
4	Accessing our Website.....	7
4.1	Server log files	7
4.2	Cookies	8
4.3	Contact	8
4.4	Newsletter	9
4.5	Job application	9
	4.5.1 Job email service	10
4.6	eKENDRIS (user account registration)	10
4.7	Mapbox/OSM	10
4.8	Google Services	11
	4.8.4 Google Marketing Platform	13
	4.8.5 Google Floodlight	13
	4.8.6 YouTube	14
	4.8.7 Google Fonts	14
	4.8.8 Google reCAPTCHA	14
4.9	Font Awesome	15
4.10	Microsoft Clarity	15
4.11	Social Media presence	15

Data Protection Policy

In this Data Protection Policy, we, the companies of the KENDRIS-Group (hereinafter all together **KENDRIS, we or us**), explain how we collect and otherwise process personal data. This is not an exhaustive description; other data protection declarations or general terms and conditions, conditions of participation and similar documents may govern specific matters. Personal data refers to all information relating to an identified or identifiable person.

If you provide us with the personal data of other persons (e.g. family members, data of work colleagues), please ensure that these persons are aware of this Data Protection Policy and only provide us with their personal data if you are permitted to do so and if this personal data is correct.

Data protection is a high priority for us. Accordingly, we consider it a matter of course to comply with the Swiss Federal Data Protection Act (DSG), the associated Data Protection Ordinance (DPO) and other applicable data protection regulations, such as the EU General Data Protection Regulation (GDPR).

1 Contact

1.1 Responsibility

Responsible for all Group companies within the KENDRIS-Group in terms of data protection, unless otherwise specified in individual cases, is

KENDRIS Services AG

Gotthardstrasse 26

6300 Zug

Email: info@kendris.com

1.2 Data Protection Officer

If you have any data protection concerns regarding any of the companies in the KENDRIS-Group, you can direct them to the following contact address:

KENDRIS Services AG

Data Protection Officer

Gotthardstrasse 26

6300 Zug

Tel.: +41 (0)58 450 50 00

E-Mail: dataprotection@kendris.com

Website: www.kendris.com

1.3 EU-Representative

Our point of contact for supervisory authorities and data subjects with all questions in connection with EU data protection law is:

VGS Datenschutzpartner UG

Am Kaiserkai 69

20457 Hamburg

Deutschland

info@datenschutzpartner.eu

2 Data Protection at KENDRIS

2.1 Collection and processing of personal data

We process various kinds of personal data. The personal data contains in particular data

- which we receive from our clients and other business partners in the course of our business relationship with them and other persons involved;
- that we collect from users when operating our websites, apps and other applications;
- which we are legally or contractually obliged to collect.

To the extent permitted, we also obtain certain data from publicly accessible sources (e.g. debt

collection registers, land registers, commercial registers, media press, Internet) or receive such data from other entities within the KENDRIS-Group, from authorities and other third parties such as providers of background checks. Insofar as these third parties are themselves responsible in whole or in part for the processing of this data, their data protection provisions also apply (e.g. the data protection provisions of LexisNexis, available at <https://www.lexisnexus.com/global/privacy/en/article-14-bis.page>).

Depending on the type of relationship, we process personal data like the following:

- **Contact and identification information** such as surname, first name, address, email address, telephone number;
- **Personal data** such as age, gender, nationality, place of birth, residence status, marital status, language, family data, professional data (e.g. function and activity), tax residency;
- **Contract data** such as contract type, contract content, type of products and services, consumption groups, consumption types, applicable terms and conditions, start of contract, contract term, billing data, powers of attorney;
- **Health related data** such as diagnosis, examination and treatment data (in the form of text, images or sound);
- **Insurance data**, in particular social security, accident and health insurance
- **Financial data** such as account information, payment information, payment history, credit rating information, tax identification number (TIN);
- **Applicant data** such as letter of motivation, CV, references, certificates and other personal or qualification information provided with regard to a specific position or provided voluntarily by applicants;
- **Telecommunications data** such as telephone number, value-added service numbers, date, time and duration of the connection, connection type, location data, IP address, device identification numbers such as MAC address;
- **Interaction and usage data**, such as correspondence, preferences and target group information, end device type, device settings, operating system, software, information from the assertion of rights;
- **Website information**, such as IP address, cookie information, browser settings, frequency of visits to the website, date and duration of visits to the website, search terms, clicks on content, originating website, MAC address, location data;
- **Marketing data**, such as socio-demographic data, interests, information on subscribing to our newsletter;
- **Information on compliance with legal requirements** such as anti-money laundering and export restrictions.

2.2 Purposes of data processing and legal basis

We primarily use the personal data we collect to conclude and process our **contracts** with our clients and business partners, in particular in the context of business consulting, legal and tax consulting, the provision of family office services, salary and HR consulting, trustee and board of directors mandates, investment reporting services, compliance services, trust & corporate administration, the automatic exchange of information and art management with our clients and the purchase of products and services from our suppliers and subcontractors, as well as to fulfill our **legal obligations** in Switzerland and abroad. If you work for such a client or business partner, your personal data may of course also be affected in this function.

In addition, we process personal data of you and other persons for the following purposes, where permitted and where deemed appropriate, in which we (and sometimes third parties) have a **legitimate interest** corresponding to the purpose:

- Offering and expanding our range, services and websites, apps and other platforms on which we are present;
- Communicating with third parties and processing their inquiries (e.g. applications);

- Examination and optimization of processes regarding analysis of needs for the purpose of direct client contact and collection of personal data from publicly accessible sources for client acquisition;
- Advertising and marketing (including the organization of events), provided you have not objected to the use of your data (if we send you advertising as an existing client, you can object to this at any time and we will then place you on a restricted list preventing further advertising mailings);
- Media monitoring;
- Assertion of legal claims and defense in connection with legal disputes and official proceedings;
- Conducting background checks and screening activities in connection with the client and the persons relevant to the fulfillment of the contract;
- Prevention and investigation of criminal offenses and other misconduct (e.g. conducting internal investigations, data analysis to combat fraud);
- Ensuring our operations, in particular IT, our websites, apps and other platforms;
- Video surveillance to safeguard domiciliary rights and other measures for IT, building and facility security and protection of our employees and other persons and assets belonging to or entrusted to us (e.g. access controls, visitor lists, network and mail scanners, telephone recordings);
- Purchase and sale of business units, companies or parts of companies and other corporate transactions and the associated transfer of personal data, as well as measures for business management and, to the extent necessary, compliance with national and international legal and regulatory obligations and internal regulations of KENDRIS.

If you have given us your **consent** to process your personal data for specific purposes (for example, when you register to receive newsletters), we will process your personal data within the scope of and based on this consent, unless we have another legal basis and require such. Consent that has been given can be revoked at any time, but this has no effect on data processing that has already taken place. You can send us your revocation by email or by post to the (email) address specified in section 1.2. Any consent given to cookies can be revoked independently by opening our cookie settings.

2.3 Data disclosure and data transfer abroad

Within the scope of our business activities and for the purposes mentioned above, we also disclose data to third parties, to the extent permitted and as we deem appropriate, either because they process it for us or because they wish to use it for their own purposes. This applies in particular to the following entities:

- Our service providers (within the KENDRIS-Group as well as external, like for example banks, insurance companies), including data processors (e.g. IT-Provider);
- registered agents in countries where these are required by law, provided that we are assisting you on your behalf in the relevant country with the formation and/or administration of an entity;
- retailers, suppliers, subcontractors, and other business partners;
- clients;
- domestic and foreign authorities, government agencies, or courts;
- media;
- the public, including visitors to websites and social media;
- competitors, industry organizations, associations, organizations, and other bodies;
- acquirers or parties interested in acquiring business areas, companies, or other parts of the KENDRIS-Group;
- other parties in potential or actual legal proceedings;
- other group companies of the KENDRIS-Group;

all together **recipients**.

Some of these recipients are located in Switzerland, but they may be anywhere in the world. In

particular, you must expect your data to be transferred to all countries in which the KENDRIS-Group is represented by group companies, branches, or other offices, as well as to other countries in Europe and the US where we are active on your behalf or where the service providers we use are located (such as LexisNexis). If we transfer data to a country without adequate legal data protection, we ensure that the recipient takes appropriate measures to protect personal data, namely by agreeing to the EU Standard Contractual Clauses (current version available [here](#)), by concluding Binding Corporate Rules, or by relying on the exceptions provided for by law, such as your consent. You can obtain a copy of the aforementioned contractual guarantees at any time from the contact person named in section 1.2, unless they are available at the link above. However, we reserve the right to redact copies for data protection or confidentiality reasons, or to provide only excerpts.

We are entitled to transfer your data to a country without adequate legal data protection without taking any of the above measures if the data transfer is necessary for the conclusion or fulfillment of a contract between you and us or for the implementation of pre-contractual measures at your request. We are also entitled to transfer your data to a country without adequate legal data protection without taking the above measures if this is necessary for the conclusion or fulfillment of a contract concluded in your interest between us and another natural or legal person. If, in the cases mentioned, data of third parties, such as family members, also has to be transferred, you are responsible for obtaining any necessary consent from these third parties.

We would also like to point out that if KENDRIS and/or one of its group companies manages structures/companies or provides services for them which, according to the Automatic Exchange of Information under Common Reporting Standards (CRS), are classified as financial institutions (FI) and/or foreign financial institutions (FFI) under the Foreign Tax Account Tax Compliance Act (FATCA), certain information (e.g., account number/balance, tax identification number, name, address) about the relevant account holder and controlling persons may have to be reported to the competent tax authorities.

2.4 Duration of data processing

We process your personal data for as long as it is necessary to fulfill our contractual and national and international legal obligations or otherwise for the purposes pursued with the processing, i.e., for example, for the duration of the entire business relationship (from the initiation, execution, to the termination of a contract) and beyond that in accordance with the legal storage and documentation obligations. It is possible that personal data may be retained for the period during which claims can be asserted against us and insofar as we are otherwise legally obliged to do so or legitimate business interests require this (e.g. for evidence and documentation purposes). As soon as your personal data is no longer required for the above-mentioned purposes, it will be deleted or anonymized to the extent possible.

2.5 Rights of the data subject

Within the scope of the data protection law applicable to you and to the extent provided for therein, you have the right to information, correction, deletion, the right to restrict data processing and otherwise object to our data processing, as well as to the disclosure of certain personal data for the purpose of transfer to another location (so-called data portability).

Please note, however, that we reserve the right to assert the restrictions provided for by law, for example, if we are obliged to store or process certain data, have an overriding interest in doing so (insofar as we are permitted to invoke this), or need it to assert claims. We have already informed you about the possibility of revoking your consent in section **Error! Reference source not found.** Please note that exercising these rights may conflict with contractual agreements and may have consequences such as premature termination of the contract or cost implications. In this case, we will inform you in advance if this is not already regulated in the contract.

The exercise of such rights generally requires that you prove your identity (e.g., by providing a copy of your ID card/passport if your identity is otherwise unclear or cannot be verified). To assert your rights, you can contact us at the (email) address specified in section 1.2.

Every data subject also has the right to enforce their claims in court or to lodge a complaint with the competent data protection authority. The competent data protection authority in Switzerland is the [Federal Data Protection and Information Commissioner](#).

2.6 Data security

We take appropriate technical and organizational security measures to protect your personal data and continuously improve these in line with technological developments. This includes protection against accidental or intentional manipulation, loss, destruction, or unauthorized access, such as the use of recognized encryption methods (e.g., encryption using SSL/TLS).

The measures taken are designed to ensure the confidentiality and integrity of your data and to guarantee the long-term availability and resilience of our systems and services when processing your data. They are also intended to ensure the rapid restoration of the availability of your data and access to it in the event of a physical or technical incident.

Our employees and service providers engaged by us are bound to confidentiality and compliance with data protection regulations and only have access to your personal data when necessary.

3 Video surveillance

Based on our legitimate interests in protecting our property rights, safeguarding our employees and other persons, securing goods, data, and secrets belonging to us or entrusted to us, and preventing and punishing illegal behavior (such as theft or damage to property), we or our landlords use video surveillance systems and other measures for IT, building, and facility security at various locations, video surveillance systems and other measures for IT, building, and facility security, such as access controls, visitor lists, network and mail scanners, and telephone recordings.

The recordings will only be used if a criminal or civilly liable act is identified and the recordings are required for criminal prosecution, or if we need the recordings to enforce legitimate claims, in particular civil law claims.

If proceedings are initiated by a law enforcement agency, the records will also be retained until the proceedings have been legally concluded.

Outside of the aforementioned procedures, no copies of the records created will be made, and they will not be made accessible to unauthorized third parties.

4 Accessing our Website

4.1 Server log files

When you visit our website, our servers temporarily store each access in a log file, known as a server log file.

For this purpose, your IP address, the date and time of your visit, the name of the file accessed, the access status (successful, partially successful, unsuccessful, etc.), the web browser and operating system used, information about your internet service provider, and other similar information are recorded.

The data collected in this way will not be merged with other data and will not be evaluated in relation to individuals.

This information is processed on the basis of our legitimate interests and for the purpose of correctly displaying our website and its content and offers to you, ensuring data traffic, optimizing our website, content, and offers, permanently ensuring the stability and security of our website and systems, and enabling the investigation, defense, and prosecution of cyberattacks, spam, and other illegal activities in relation to our website and systems, and to enforce related claims.

We delete your personal data as soon as it is no longer required for the purpose for which it was collected. In the case of data collection for the provision of our website, deletion generally takes place when the respective session has ended, at the latest after seven days. If we store the data for longer, it is anonymized so that no conclusions can be drawn about you.

We may use third-party services in Switzerland and abroad to host the website, which carry out the above-mentioned processes on our behalf. Currently, our website is hosted exclusively by Swiss hosting providers and on servers in Switzerland.

4.2 Cookies

KENDRIS' website uses cookies. Cookies are text files that are stored on your device (notebook, computer, smartphone, etc.) with the help of your browser. They serve to make our websites more user-friendly and effective overall and to make your visit to our websites as pleasant as possible. Cookies do not cause any damage to your device and cannot execute programs or contain viruses.

Most of the cookies we use are so-called session cookies. These are automatically deleted when you log out or close your browser. Other cookies remain stored on your device beyond the respective usage process and enable us or our partner companies (third-party cookies) to recognize your browser the next time you visit. If other cookies (e.g., cookies for analyzing your surfing behavior) are stored, these are treated separately in this Data Protection Policy.

The basis on which we process your personal data using cookies depends on whether we ask for your consent. If this applies and you consent to the use of cookies, the basis for processing your data is your consent. Otherwise, the personal data processed using cookies is processed on the basis of our legitimate interests (e.g., to guarantee the security of our website) or, if the use of cookies is necessary, to fulfill our contractual obligations.

Regardless of whether processing is based on consent or legal permission, you have the option at any time to revoke your consent or object to the processing of your data by cookie technologies. You can adjust your browser to inform you about the setting of cookies and only allow the acceptance of cookies in specific cases or exclude them altogether. If you generally exclude the setting of cookies, we would like to point out that in this case you may not be able to use all the functions of our website to their full extent. Furthermore, you can activate the automatic deletion of cookies when closing your browser and delete cookies that have already been set at any time in your browser or other software programs.

You can also opt out of cookies used for reach measurement and advertising purposes via the [Network Advertising Initiative's opt-out page](#) and additionally on the US website [YourAdChoices](#) or the European website [Your Online Choices](#).

4.3 Contact

You can contact us via an online form and/or by email on our website. If you contact us using the online form, the information you provide on the form, including the contact details you provide there, will be stored by us for the purpose of processing your request and in case of follow-up questions, and will not be passed on to unauthorized third parties without your consent. This also applies, of course, to requests that you send us by post.

The basis for processing your personal data is our legitimate interest in processing your request. If the purpose of contacting you is to fulfill a contract to which you are a party or to take pre-contractual measures, this constitutes an additional basis for processing your personal data.

You may object to this data processing at any time. Please send your objection to the email address specified in section 1.2 and we will review your request. In such a case, your request will not be processed further.

Your personal data will be deleted as soon as your request has been processed. This is the case when it can be inferred from the circumstances that the matter in question has been conclusively

clarified and there are no legal retention obligations that prevent deletion.

4.4 Newsletter

You can subscribe to various free newsletters on our website. To do so, fill out the form with the required information, such as your email address, and select one or more topics that interest you (e.g., fiduciary services). We require this mandatory information in order to send you the newsletter(s) and address you personally. With our newsletters, we inform you several times per year about current topics, offers, important news in the industry, and regulatory changes.

Registration for the newsletter is carried out using a double opt-in procedure and is therefore based on your consent. This means that after registering, you will receive an email in which you must click on a link to confirm your registration.

You can unsubscribe from the newsletter free of charge at any time and revoke your consent. To do so, click on the corresponding button in the newsletter you have received.

Our newsletters may contain graphics and/or web links that collect personal data, if permitted, on whether, when, and how often an individual newsletter has been opened in an email application and which web links have been clicked on. Such graphics and/or web links collect data on the use of newsletters in order to ensure quality and enable improvements to the newsletter. You can block the setting of such graphics and/or web links in your email application.

We use Aivie as a marketing automation tool to send out newsletters, campaigns, and automated communication channels. Aivie processes personal data on our behalf and exclusively in accordance with our instructions. Details on data protection, data security, subcontractors, and the data processing agreement are described here: <https://aivie.ch/en/privacy-at-aivie/>.

4.5 Job application

When you apply for a job with us, we process the personal data that we receive from you during the application process or that you enter or upload in the application form. In addition to your personal details, education, work experience, and skills, this includes the usual contact details such as your email address and telephone number. In addition, all documents submitted by you in connection with the application, such as your resume and references, will be processed. This data will be stored, evaluated, processed, or forwarded internally exclusively in the context of your application. It may also be processed for statistical purposes (e.g., reporting). In this case, no conclusions can be drawn about individual persons.

Our online application form is provided by Refline AG (“Refline”), based in Switzerland. The form is embedded in our website via an iframe, which means that the information you provide and your application documents are stored on Refline's servers.

Your applicant data is processed in order to fulfill our (pre)contractual obligations within the scope of the application process.

You may object to this data processing at any time and withdraw your application. Please send your objection to the contact person named in the job advertisement or to the (email) address specified in section 1.2.

If we conclude an employment contract with you, the data transmitted will be stored for the purpose of processing the employment relationship in compliance with legal regulations. If the application process ends without employment, your personal data will be stored for six months for documentation purposes and then deleted from Refline, unless you have given us your consent to store your details for a certain period of time for further application processes.

Further information on data protection and data security at Refline can be found in their [Terms and Conditions](#) and [Privacy Policy](#).

4.5.1 Job email service

If you would like to receive regular updates about new job vacancies at KENDRIS, you can sign up for our job email service.

You can create a personalized job search profile. Simply select the desired business unit and work location. If you do not enter any information, you will receive an overview of all our open positions at all our locations.

In order for us to send you the information, you must provide us with a valid email address, choose a name for your job email service, and specify the frequency in which you would like to receive job emails. Registration for our job newsletter is based on a double opt-in procedure and therefore requires your consent. This means that after registering, you will receive an email in which you must click on a link to confirm your registration.

The job newsletters we send may contain small, “invisible” files (beacons) that enable us to perform various analyses to improve our services. The beacons record your IP address, the browser you are using, the time you accessed and opened the job email, and your clicking behavior on links contained in the emails. The data is stored and evaluated in order to better tailor the job emails to individual interests in the future. We do not pass this information on to third parties.

Our job emails are also sent by Refline (see section **Error! Reference source not found.** above).

You can revoke your consent to the storage of your data and its use for sending job emails at any time, for example via the “Unsubscribe” link at the end of each newsletter or in the job email management section. If you wish to prevent the use of web beacons, please set your email program so that HTML is not displayed in messages. The following links provide explanations on how to configure this setting in the most common email programs: [Microsoft Outlook](#) and [Mail on Mac](#).

4.6 eKENDRIS (user account registration)

We offer our clients the opportunity to register for our eKENDRIS portal. Within the portal, we provide you with personal information and financial data relating to the respective client (eInvestment Reporting, etc.).

User registration is necessary in order to provide certain content and services on the KENDRIS website. User registration is required for the fulfillment of a contract with the user or for the implementation of pre-contractual measures. To register for eKENDRIS, please contact the responsible account manager.

The basis for processing your personal data is your consent. If the registration serves to fulfill a contract to which you are a party or to implement pre-contractual measures, this is an additional basis for processing your personal data.

All rights and obligations in connection with the use of the eKENDRIS portal and the information contained therein arise from the specific agreement and the eKENDRIS GTC.

4.7 Mapbox/OSM

On the basis of your consent, we use Mapbox, a service provided by Mapbox Inc., based in the USA (“Mapbox”), in conjunction with OpenStreetMap, a service provided by the OpenStreetMap Foundation, based in the United Kingdom (“OSM”), to integrate interactive maps on our website.

When you visit one of our websites where we use Mapbox/OSM, certain data (in particular your IP address, data about your browser, and similar information, as well as your approximate location, if applicable) will be transmitted to the two providers and stored there, i.e., in the USA or the United Kingdom.

To protect your privacy, we have entered into an [order processing agreement](#) with Mapbox, including EU standard contractual clauses. In addition, Mapbox is certified under the [EU-U.S. and](#)

[Swiss-U.S. Data Privacy Framework](#) and therefore offers adequate protection when transferring data to the United States.

OSM considers itself to be independently responsible, which is why we were unable to conclude such an agreement.

We have no influence on the data processing by Mapbox/OSM and cannot rule out the possibility that Mapbox and/or OSM may pass on the data collected about you to third parties, if this is required by law or if third parties process this data on their behalf.

We do not store any personal data that is collected when using the maps on our website. Regarding the retention period at Mapbox/OSM, please refer to their documentation. This and further information on data protection at Mapbox/OSM can be found in the [Privacy Policy](#), the [FAQ “Services and tile users privacy”](#), the [Terms of Use](#) of the OpenStreetMap Foundation, and the [“Mapbox Legal Portal”](#).

4.8 Google Services

On the basis of your consent, we use various services provided by Google LLC, based in the USA, or, if you are a resident of the European Economic Area (EEA) or Switzerland, Google Ireland Ltd., based in Ireland (“Google”), on our website. Google LLC is always responsible for the processing of personal data when using YouTube. We use the following Google services on our website:

- Google Tag Manager
- Google Analytics
- Google Ads
- Google Marketing Platform
- Google Floodlight
- YouTube
- Google Fonts
- Google reCAPTCHA

More detailed information on the individual services can be found below.

Google uses technologies such as cookies, web storage in the browser, and tracking pixels, which enable an analysis of your use of our website. The information generated about your use of our website may be transmitted to a Google server in the USA or other countries and stored there. Information about the locations of Google's data centers can be found [here](#).

We use tools provided by Google which, according to Google, may process personal data in countries where Google or its [subprocessors](#) have facilities. In its [“Data Processing Addendum for Products where Google is a Data Processor”](#), Google promises to ensure an adequate level of data protection by relying on the EU Standard Contractual Clauses.

Google is also certified under the [EU-U.S. and Swiss-U.S. Data Privacy Framework](#).

For more information about Google's processing of data and privacy settings, please refer to Google's [Privacy Policy](#) and [privacy settings](#).

4.8.1 Google Tag Manager

Our website uses Google Tag Manager. Google Tag Manager allows website tags to be managed efficiently. Website tags are placeholders that are stored in the source code of the respective website in order to record the integration of frequently used website elements, such as code for web analysis services. Google Tag Manager does not use cookies and triggers other tags, which in turn may collect data. Google Tag Manager does not access this data. If deactivation has been carried out at the domain or cookie level, this remains in effect for all tracking tags implemented with Google Tag Manager.

For more information, please refer to the [Google Tag Manager Terms of Service](#).

4.8.2 Google Analytics

We use the web analytics service Google Analytics 4 (“Google Analytics”) for the purpose of analyzing our website and its visitors, as well as for marketing and advertising purposes.

Google Analytics uses cookies that are stored on your device (laptop, tablet, smartphone, etc.) and enable an analysis of your use of our website. This allows us to evaluate usage behavior on our website and use the statistics/reports obtained to make our offering more interesting.

IP address anonymization is enabled by default in Google Analytics. This means that your IP address is truncated by Google within Switzerland or the EU/EEA before it is transmitted. Only in exceptional cases is the full IP address transmitted to a Google server and shortened there.

Google uses this information to evaluate your pseudonymous use of our website, to compile reports on website activity, and to provide us with other services related to website and internet usage. According to Google, the IP address transmitted by your browser as part of Google Analytics is not merged with other Google data. When you visit our website, your user behavior is recorded in the form of events (such as website views, interaction with the website, or your “click path”) as well as other data such as your approximate location (country and city), technical information about your browser and the devices you use, or the referrer URL, i.e., which website/advertisement brought you to our website.

You can prevent the collection and transmission of data generated by the cookie and related to your use of our website (including your IP address) to Google, as well as the processing of this data by Google, by downloading and installing the [browser add-on to deactivate Google Analytics](#). If you wish to object to interest-based advertising by Google, you can use the [settings and opt-out options](#) provided by Google.

Your personal data will be deleted or anonymized after 14 months.

An overview of data usage in Google Analytics and the measures taken by Google to protect your data can be found in the [Google Analytics Help Center](#).

Further information on the [Google Analytics Terms of Service](#) and [Google Privacy Policy](#) can be found in the respective documents.

4.8.3 Google Ads

Our website uses Google Ads, an online advertising program belonging to Google Marketing Services, to draw attention to our offers with the help of advertising material on external websites. We can determine how successful the individual advertising measures are in relation to the data from the advertising campaigns.

Google Ads places a cookie on your computer (“conversion cookie”) if you have accessed our website via a Google ad. These cookies usually expire after 30 days and are not intended to identify you personally.

These cookies enable Google to recognize your internet browser. If you visit certain websites belonging to us and the cookie has not yet expired, Google and we can recognize that you clicked on the ad and were thus redirected to our website. Each Google Ads customer is assigned a different cookie. Cookies cannot therefore be tracked through the websites of Google Ads customers. We ourselves do not collect or process any personal data in the advertising measures mentioned. We only receive statistical evaluations from Google. Based on these evaluations, we can identify which of the advertising measures used are particularly effective. We do not receive any further data from the use of the advertising material; in particular, we cannot identify you based on this information.

Based on the information collected, categories relevant to your interests are assigned to your browser. These categories are used to display interest-based advertising.

By using Google Ads, we can reach users who have already visited our website. This allows us to present our advertising to target groups who are already interested in our products or services.

You can prevent participation in this tracking process in various ways, including:

- by adjusting your browser software settings accordingly; in particular, suppressing third-party cookies means that you will not receive any third-party advertisements;
- by disabling cookies for conversion tracking by adjusting the relevant [settings for personalized advertising from Google](#);
- by deactivating interest-based ads from providers who are part of the “[YourAdChoices](#)” self-regulation campaign.

For more information on how this works and data protection, please refer to the [Google Ads Privacy Policy and Terms of Use](#).

4.8.4 Google Marketing Platform

The online marketing tool Google Marketing Platform (“GMP”) uses cookies to display relevant ads to website visitors, improve campaign performance reports, or prevent website visitors from seeing the same ads multiple times. Google uses a cookie ID to track which ads are displayed in which browser, thereby preventing them from being displayed multiple times.

In addition, GMP can use cookie IDs to track conversions, i.e., whether a website visitor sees a GMP ad and later visits the advertiser's website and, for example, makes a purchase there. According to Google, GMP cookies do not contain any personal information.

Your browser automatically establishes a direct connection to Google's server. We have no influence on the scope and further use of the data collected by Google through the use of this service. According to Google, the integration of GMP provides Google with the information that you have accessed the corresponding part of our website or clicked on one of our ads. If you are registered with a Google service, Google can assign the visit to your user account. Even if you are not registered with Google or have not logged in, it is possible that the provider may collect and store your IP address.

For more information about GMP, visit the [Google Marketing Platform](#) website.

4.8.5 Google Floodlight

To measure the success of our advertising campaigns and to show you only those advertisements that may be of interest to you, we use the web analytics and conversion tracking service Google Floodlight (“Floodlight”) on our website.

The use of Floodlight establishes a connection to Google's servers, which may transmit information about your use of our website to Google. Floodlight stores and collects various information about you, such as the advertisements you click on or your behavior on other websites.

Google uses a cookie ID to track which ads are displayed in which browsers, thereby preventing multiple displays. Furthermore, Google can use cookie IDs to track conversions, i.e., whether a user sees a Google ad and later visits the advertiser's website and makes a purchase or signs up for a newsletter. These cookies do not contain any personal information (e.g., your name or email address).

By integrating Floodlight tags, Google receives information that you have visited our website or clicked on one of our advertisements.

In addition, the Floodlight tags we use enable us to understand whether you perform certain actions on our website after viewing or clicking on one of our advertisements on other platforms (“conversion tracking”).

We store the information we collect with Floodlight for as long as necessary for the purpose for

which it was collected, e.g., for the duration of a specific advertising campaign. Reports are available for up to 60 days and are then only aggregated.

For more information on how Floodlight works, please refer to the relevant [Google Help](#) section.

4.8.6 YouTube

We use the services of YouTube LLC, based in the USA (“YouTube”), a subsidiary of Google LLC (“Google”), to embed videos on our website.

When you start a YouTube video on our website, a connection to YouTube's servers is established. This connection tells the YouTube server which of our websites you have visited. This information (including your IP address) may be transmitted to a Google server in the USA and stored there. If you are logged into your YouTube account at the same time, you enable YouTube to assign your surfing behavior directly to your personal profile. You can prevent this by logging out of your YouTube account before visiting our website.

We use YouTube's extended data protection mode. According to YouTube, this mode ensures that YouTube does not store any data about you as a visitor of our website before you view or play the video. However, the extended data protection mode does not necessarily prevent data from being passed on to YouTube partners.

Further information can be found in YouTube's [Terms of Service](#) and Google's [Privacy Policy](#).

4.8.7 Google Fonts

In order to display our content correctly and in a graphically appealing manner across all browsers, we may use script and font libraries on our website to display fonts. Google Fonts are transferred to your browser's cache to avoid multiple loading. If your browser does not support Google Fonts or prevents access, our website content will be displayed in a standard font.

Calling up script or script libraries automatically triggers a connection to the library operator. In theory, it is possible—although it is currently unclear whether and, if so, for what purposes—that the operator, in this case Google, collects data.

We do not collect any personal data through the integration of Google Fonts.

You can object to data processing by Google Fonts by deactivating JavaScript in your browser or installing a JavaScript blocker. Please note that this may result in functional restrictions on the website.

For more information about Google Fonts, please refer to the [Google Fonts FAQ](#) and Google's [Privacy Policy](#).

4.8.8 Google reCAPTCHA

We use the reCAPTCHA function to distinguish whether an entry (e.g., in a contact form) is made by a human or automatically by a computer program (so-called [bots](#)). In this way, we want to ensure the security of our website and protect it in particular from automated entries (or attacks) and spam. This is also our legitimate interest in processing.

To do this, reCAPTCHA analyzes the behavior of the website visitor based on various characteristics. These analyses run completely in the background and start automatically as soon as you visit our website. To distinguish between humans and bots, Google analyzes various information, such as the IP address of the device used, the length of time spent on the website, the browser and operating system used, and the mouse movements made by the website visitor.

Further information on how Google uses the data collected in this way can be found in Google's [Privacy Policy](#) and [Terms of Service](#).

4.9 Font Awesome

On the basis of your consent, we use web fonts (specifically icons) from Fonticons Inc., based in the USA (“Font Awesome”), on our website in addition to Google Fonts in order to display our content correctly and in a graphically appealing manner across all browsers.

The icons are loaded via the Font Awesome Content Delivery Network (CDN). CDNs are networks of servers distributed worldwide, enabling files to be loaded quickly from the nearest server. In order for the icons to be loaded, the browser you are using automatically connects to the Font Awesome servers. This provides Font Awesome with information about your IP address and which icon you loaded and when. This information is stored on the respective CDN server, including in the USA.

According to [Font Awesome's Privacy Policy](#), Font Awesome processes this data about your use of its CDN for purposes including optimizing its CDN, diagnosing and fixing technical errors, protecting the CDN from misuse and attacks, and compiling statistics.

We do not collect any personal data through the integration of Font Awesome.

For more information about Font Awesome, please refer to [Font Awesome's Privacy Policy](#) and [Support + FAQ page](#).

4.10 Microsoft Clarity

On the basis of your consent, we use Microsoft Clarity, an analytics service provided by Microsoft Corporation, based in the United States, or, if you are a resident of the European Economic Area (EEA) or Switzerland, Microsoft Ireland Operations Limited, based in Ireland (“Clarity”), on our website.

Clarity enables us to better understand the needs of our website visitors and is particularly useful for optimization and marketing purposes, as well as for designing our website in line with user interests. With the help of Clarity, movements on our website can be tracked (so-called “heat maps”) and, by displaying animations (so-called “session recordings”), all these user interactions, including individual sessions, can be traced. Clarity uses cookies for this purpose.

The information collected using cookies includes, in particular, interaction (e.g. clicks, scrolling and mouse-overs) and diagnostic data (e.g. script and image errors). You can find out which information is processed by Clarity [here](#).

The data generated using Microsoft Clarity can be stored for up to 12 months and will then be deleted.

For more information about how Clarity works, see the [Clarity website](#), the [Clarity Documentation](#), and the [Clarity FAQ](#).

Further information about data protection and how Microsoft handles your data can be found in the [Microsoft Privacy Statement](#).

4.11 Social Media presence

We maintain social media profiles on Instagram, YouTube, LinkedIn and Kununu.

The data you enter on our social media profiles will be published by the Social Media platform and will not be used or processed by us for any other purposes at any time. However, we reserve the right to delete content if necessary. If need be, we will communicate with you via the social media platform.

The basis is your and our legitimate interest in exchanging ideas with each other in this way.

Be aware that the operator of the social media platform uses web tracking methods. Web tracking, over which we have no influence, can also take place regardless of whether you are logged in or registered with the social media platform.

More detailed information on data processing by the provider of the social media platform can be found in the data protection declaration of the respective provider:

Soziales Netzwerk	Anbieter	Datenschutzerklärung
Instagram	Meta Platforms Inc. (USA)/Meta Platforms Ireland Ltd. (Ireland)	Privacy Policy
YouTube	YouTube LLC (USA)	Privacy Policy
LinkedIn	LinkedIn Corporation (USA)/LinkedIn Ireland Unlimited Company (Ireland)	Privacy Policy
Kununu	New Work SE (Germany)	Privacy at XING
