PRIVERA
For spaces and people

Privacy Policy of Privera AG

Contents

1. What is this privacy policy about? 2
2. Who is responsible for processing your data? 2
3. What data do we process? 2
4. For what purposes do we process your data? 5
5. On what basis do we process your data? 7
6. What applies to profiling and automated decisions? 8
7. To whom do we disclose your data? 8
8. Does your personal data also go abroad? 9
9. How long do we process your data? 9
10. How do we protect your data? 9
11. What rights do you have? 10
12. Do we use online tracking and online advertising techniques? 10
13. What data do we process on our social network pages? 12
14. Can this privacy policy be changed? 13

1. What is this privacy policy about?

Privera AG (hereinafter also «we», «us») obtains and processes personal data concerning you or other persons (so-called «third parties»). We use the term «data» here synonymously with «personal data».

«Personal data» means data relating to an identified or identifiable person, i.e. data from which conclusions about that person's identity can be drawn, either from the data itself or with the help of corresponding additional data. «Sensitive personal data» is a category of personal data that is given special protection under applicable data protection law. Sensitive personal data includes, for example, data revealing racial or ethnic origin, health data, information on religious or philosophical beliefs, biometric data for identification purposes and information on trade union membership. Section 3 contains information on the data we process within the scope of this privacy policy. «Processing» means any handling of personal data, e.g. obtaining, storing, using, adapting, disclosing and deleting it.

In this privacy policy, we describe what we do with your data when you use our website https://www.privera.ch, obtain our services, are otherwise connected with us under a contract, communicate with us or otherwise deal with us. Where appropriate, we will inform you in good time and in writing of any additional processing activities not mentioned in this privacy policy. In addition, we may inform you separately about the processing of your data, e.g. in declarations of consent, contractual terms, additional privacy notices, forms and notices.

If you transmit or disclose to us data about other persons, such as family members, work colleagues etc., we assume that you are authorised to do so and that this data is accurate. By transmitting data about third parties, you confirm this. Please also make sure that these third parties have been informed of this privacy policy.

2. Who is responsible for processing your data?

Privera AG is a subsidiary of PHM Switzerland AG, based in Mägenwil (AG). Privera AG, based in Gümligen, is in principle the controller under data protection law for the data processing described in this privacy policy. Where we share data with other companies of the PHM Group for certain administrative activities, support services or in the context of using central IT infrastructures (such as the group-wide CRM system MS Dynamics), the respective companies remain independently responsible for their own processing, unless otherwise agreed or communicated in an individual case. Further details on intra-group data transfers can be found in section 7.

You can contact us regarding your data protection concerns and the exercise of your rights under section 11 as follows:

Privera AG
Worbstrasse 142
P.O. Box
3073 Gümligen
info@privera.ch

3. What data do we process?

We process various categories of data about you. The main categories are the following:

- Technical data: When you use our website or other electronic offerings (e.g. free WLAN), we collect the IP address of your device and other technical data in order to ensure the functionality and security of these offerings. This data also includes logs in which the use of our systems is recorded. We generally retain technical data for 3 months. This period may be longer where this is required to comply with legal or contractual requirements or for technical reasons. In order to ensure the functionality of these offerings, we may also assign an individual code to you or your device (e.g. in the form of a cookie, see section 12). On its own, technical data generally does not allow any conclusions to be drawn about your identity. However, in connection with user accounts, registrations, access controls or the performance of contracts, it may be linked to other categories of data (and thus possibly to you as a person).

Technical data includes, among other things, the IP address and information about the operating system of your device, the date, region and time of use and the type of browser you use to access our electronic offerings. This can help us to deliver the correct formatting of the website. Although the IP address tells us which provider you use to access our offerings (and thus also the region), we generally cannot use it to determine who you are.

- Registration data: Certain offerings and services (e.g. free WLAN access) can only be used with a user account or registration, which can be completed directly with us or via our external login service providers. In doing so, you must provide us with certain data, and we collect data about the use of the offering or service. Registration data may be generated in connection with access controls to certain facilities. We generally retain registration data for 12 months after the end of the use of the service or the closure of the user account. This period may be longer where this is required to comply with legal or contractual requirements or for technical reasons.

Registration data includes, among other things, the information you provide when you create an account on our website (e.g. user name, password, name, e-mail). Registration data also includes the data we may require from you before you can use certain free services, such as our WLAN service. You must also register if you wish to subscribe to our newsletter.

- Communication data: When you are in contact with us via the contact form, by e-mail, telephone, letter or other means of communication, we record the data exchanged between you and us, including your contact details and the metadata of the communication. If we want or need to establish your identity, e.g. in the case of a request for information you have made, we collect data to identify you (e.g. a copy of an ID document). We generally retain this data for 12 months from our last exchange with you. This period may be longer where this is required for evidentiary reasons, to comply with legal or contractual requirements or for technical reasons. E-mails and written correspondence are generally retained for at least 10 years.

Communication data comprises your name and contact details, the manner, place and time of the communication and usually also its content (i.e. the content of e-mails, letters etc.). This data may also contain information about third parties.

- Master data: We use the term master data for the basic data that, in addition to contract data (see below), we need to conduct our contractual and other business relationships or for marketing and advertising purposes, such as name, contact details and information, e.g. about your role and function, your bank details, your date of birth, customer history, powers of attorney, signing authorities and declarations of consent. We process your master data if you are a customer or other business contact or work for one (e.g. as a contact person of a business partner), or because we wish to address you for our own purposes or the purposes of a contractual partner (e.g. in the context of marketing and advertising, with invitations to events, with newsletters etc.). We receive master data from you (e.g. when the business relationship is established), from organisations you work for, or from third parties such as our contractual partners, associations, and from publicly accessible sources such as public registers or the internet (websites, social media etc.). We may also process information about third parties as part of master data. We generally retain this data for 10 years from our last exchange with you, but at least from the end of the contract. This period may be longer where this is required for evidentiary reasons, to comply with legal or contractual requirements or for technical reasons.

Master data includes, for example, data such as name, address, e-mail address, telephone number and other contact details, gender, date of birth, nationality, information about related persons, websites, photos and videos, copies of ID documents; also information about your relationship with us (customer, supplier, service recipient etc.), information about your status with us, allocations, classifications and mailing lists, information about our interactions with you (possibly a history thereof with corresponding entries), reports (e.g. from the media) or official documents (e.g. commercial register extracts, permits etc.) concerning you. As payment information, we collect, for example, your bank details and account number. Consent or

blocking notices also form part of master data, as does information about third parties, e.g. contact persons, recipients of services or representatives.

In the case of contact persons and representatives of our customers, suppliers and partners, we process as master data, for example, name and address, information on role, function in the company, qualifications and, where applicable, information about superiors, employees and subordinates and information about interactions with these persons.

Master data is not collected comprehensively for all contacts. Which data we collect in each individual case depends in particular on the purpose of the processing.

- Contract data: This is data generated in connection with the conclusion or performance of a contract, e.g. information about contracts and the services to be provided or already provided, as well as data from the run-up to the conclusion of a contract, the information required or used for performance and information about reactions (e.g. complaints or information on satisfaction etc.). We usually collect this data from you, from contractual partners and from third parties involved in the performance of the contract, but also from third-party sources (e.g. authorities, providers of credit data) and from publicly accessible sources. We generally retain this data for 10 years from the last contractual activity, but at least from the end of the contract. This period may be longer where this is required for evidentiary reasons, to comply with legal or contractual requirements or for technical reasons.

Contract data includes information about the conclusion of the contract and about your contracts, e.g. the type and date of conclusion of the contract, information from the application process (such as an application for our services) and information about the contract in question (e.g. its duration) and the performance and administration of the contracts (e.g. information in connection with invoicing and the enforcement of contractual claims). Contract data also includes information about defects, complaints and amendments to a contract, as well as information on customer satisfaction, which we may collect, for example, by means of surveys. Contract data further includes financial data such as information on creditworthiness (i.e. information that allows conclusions to be drawn about the likelihood that receivables will be paid), on reminders and on debt collection. We receive some of this data from you (e.g. when you make payments), but also from credit agencies, debt collection companies and publicly accessible sources (e.g. a commercial register).

- Other data: We also collect data from you in other situations. In connection with official or court proceedings, for example, data is generated (such as files, evidence etc.) that may also relate to you. We may also collect data for health protection reasons (e.g. as part of protection concepts). We may obtain or produce photos, videos and sound recordings in which you may be identifiable (e.g. at events etc.). The retention period for this data depends on its purpose and is limited to what is necessary.

You provide us with much of the data mentioned in this section 3 yourself (e.g. via forms, in the course of communication with us, in connection with contracts, when using the website etc.). You are not obliged to do so, subject to individual cases, e.g. in the context of binding protection concepts (legal obligations). If you wish to conclude contracts with us or use our services, you must also provide us with data as part of your contractual obligations under the relevant contract, in particular master, contract and registration data. When using our website, the processing of technical data is unavoidable.

We only make certain services available to you if you provide us with registration data, because we or our contractual partners want to know who is using our services or has accepted an invitation to an event, because it is technically necessary or because we want to communicate with you. If you or a person you represent (e.g. your employer) wish to conclude or perform a contract with us, we must collect the corresponding master, contract and communication data from you, and we process technical data if you wish to use our website or other electronic offerings for this purpose. If you do not provide us with the data required for the conclusion and performance of the contract, you must expect that we may refuse to conclude the contract, that you may commit a breach of contract or that we may not perform the contract. Likewise, we can only send you a response to an inquiry if we process the data necessary for that purpose. It is also not possible to use our website without us receiving technical data.

Insofar as this is not impermissible, we also obtain data from publicly accessible sources (e.g. debt enforcement registers, land registers, commercial registers, the media or the internet including social media) or receive data from other companies within our group, from authorities and from other third parties.

The categories of personal data we receive about you from third parties include, in particular, information from public registers, information we learn in connection with official and court proceedings, information in connection with your professional functions and activities (so that we can, for example, conclude and conduct business with your employer with your help), information about you in correspondence and meetings with third parties, credit reports (insofar as we do business with you personally), information about you that people in your environment (family, advisors, legal representatives etc.) give us so that we can conclude or perform contracts with you or involving you (e.g. references, your delivery address, powers of attorney, information on compliance with legal requirements such as combating fraud, money laundering and terrorism and export restrictions), information from banks, insurance companies, sales partners and other contractual partners of ours on the use or provision of services by you (e.g. payments etc.), and information from the media and the internet about you (insofar as this is appropriate in the specific case, e.g. in the context of a job application, marketing, press review etc.).

4. For what purposes do we process your data?

We process your data for the purposes explained below. Further information for the online area can be found in sections 12 and 13. These purposes and the objectives underlying them represent legitimate interests of ours and, where applicable, of third parties. Further information on the legal bases of our processing can be found in section 5.

We process your data for purposes related to communication with you, in particular to respond to enquiries and in connection with the exercise of your rights (section 11) and to contact you in the event of queries. For this purpose, we primarily use communication data and master data, as well as data related to the offers and services you use. We retain this data to document our communication with you, for training purposes, for quality assurance and for follow-up enquiries.

This concerns all purposes in connection with which you and we communicate, whether in advisory services, for authentication when using the website, etc. We further process communication data so that we can communicate with you by e-mail and telephone as well as via social media, letter and fax. Communication with you usually takes place in connection with other processing purposes, e.g. so that we can provide services. Our data processing also serves as evidence of the communication and its content.

We process data for the establishment, administration and performance of contractual relationships.

We conclude contracts of all kinds with our business and private customers, with suppliers, subcontractors or other contractual partners such as partners in projects or with parties in legal disputes. In this process, we specifically handle master data, contract data, and communication data of the individuals to whom the client facilitates a service.

In the course of initiating business, personal data – in particular master data, contract data and communication data – is collected from potential customers or other contractual partners (e.g. in an order form or contract) or results from a communication. Also in connection with the conclusion of a contract, we process data to check creditworthiness and to open the customer relationship. Some of this information is checked to ensure compliance with legal requirements.

In the course of performing contractual relationships, we process data to manage the customer relationship, to provide and claim contractual services (which also includes involving third parties, such as banks and insurance companies), for advice and for customer care. The enforcement of legal claims arising from contracts (debt collection, court proceedings etc.) is also part of performance, as are accounting, termination of contracts and any public communication.

We process data for marketing purposes and relationship management, e.g. to send our customers and other contractual partners personalised advertising for our services or those of third parties affiliated with us.

This may take place, for example, in the form of newsletters and other regular contacts (electronically, by post, by telephone), via other channels for which we have contact information from you, but also in the context of individual marketing campaigns (e.g. events). You can refuse such contacts at any time (see the end of this section 4) or refuse or withdraw consent to being contacted for advertising purposes. With your consent, we can target our online advertising on the internet more specifically to you (see section 12).

For example, with your consent we send you information, advertising and service offers from us and from third parties within Privera AG, as printed matter, electronically or by telephone. For this purpose, we mainly process communication and registration data. Like most companies, we personalise communications so that we can send you individual information and make offers that match your needs and interests. To this end, we link data that we process about you, determine preference data and use this data as the basis for personalisation (see section 3).

Relationship management also includes addressing existing customers and their contacts – where applicable personalised on the basis of behavioural and preference data. As part of relationship management, we may also operate a customer relationship management system («CRM») in which we store the data on customers, suppliers and other business partners required for relationship management, e.g. about contact persons, the relationship history (e.g. about services obtained, interactions etc.), interests, wishes, marketing measures (newsletters, invitations to events etc.) and other information. This CRM may be operated on a group-wide platform, as a result of which other companies of the PHM Group (including our parent company in Finland) obtain access to this data exclusively for technical support and administrative purposes.

We further process your data for market research and to improve our services and our operations.

We strive to continuously improve our services (including our website) and to be able to respond quickly to changing needs. We therefore analyse, for example, how you navigate through our website or which services are used by which groups of people and in what way, and how new services can be designed (for further details see section 12). This gives us indications of the market acceptance of existing services and the market potential of new ones. For this purpose, we process in particular master, behavioural and preference data, but also communication data and information from customer surveys, polls and studies and other information, e.g. from the media, social media, the internet and other public sources. Where possible, we use pseudonymised or anonymised information for these purposes. We may also use media monitoring services or carry out media monitoring ourselves and process personal data in the process, in order to carry out media work or to understand and respond to current developments and trends.

We may also process your data for security purposes and for access control.

We continuously review and improve the appropriate security of our IT and our other infrastructure (e.g. buildings). Like all companies, we cannot rule out data security breaches with absolute certainty, but we do our utmost to reduce the risks. We therefore process data, for example, for monitoring, checks, analyses and tests of our networks and IT infrastructures, for system and error checks, for documentation purposes and in the context of backup copies. Access controls include, on the one hand, controlling access to electronic systems (e.g. logging in to user accounts) and, on the other hand, physical access control (e.g. access to buildings). For security purposes (preventive and to investigate incidents), we also keep access logs or visitor lists and use surveillance systems (e.g. security cameras).

We process personal data to comply with laws, directives and recommendations from authorities and internal regulations («compliance»).

This includes, for example, the legally regulated fight against money laundering and terrorist financing. In certain cases, we may be obliged to carry out certain clarifications about customers («Know Your Customer») or to make reports to authorities. The fulfilment of obligations to provide information or to report, e.g. in connection with supervisory and tax law obligations, also requires or entails data processing, e.g. the fulfilment of archiving obligations and the prevention, detection and investigation of criminal offences and other violations. This also includes receiving and processing complaints and other reports, monitoring communications, internal investigations or disclosing documents to an authority if we have sufficient reason to do so or are legally obliged to do so. Your personal data may also be processed in the course of external

investigations, e.g. by a law enforcement or supervisory authority or a mandated private body. For all these purposes, we process in particular your master data, your contract data and communication data, but under certain circumstances also behavioural data and data from the category of other data. The legal obligations may be Swiss law, but also foreign provisions to which we are subject, as well as self-regulation, industry standards, our own «corporate governance» and official instructions and requests.

We also process data for the purposes of our risk management and as part of prudent corporate governance, including business organisation and corporate development.

For these purposes, we process in particular master data, contract data, registration data and technical data, but also behavioural and communication data. For example, as part of our financial management, we must monitor our debtors and creditors, and we must avoid becoming the victim of offences and abuse, which may require the analysis of data for corresponding patterns. For these purposes and to protect you and us against criminal or abusive activities, we may also carry out profiling and create and process profiles. In planning our resources and organising our operations, we must evaluate and process data on the use of our services and other offerings or exchange information about this with others (e.g. outsourcing partners), which may also include your data. The same applies with regard to services provided to us by third parties. As part of corporate development, we may sell businesses, parts of businesses or companies to others or acquire them from others or enter into partnerships, which may also lead to the exchange and processing of data (including yours, e.g. as a customer or supplier or as a supplier representative).

We may process your data for further purposes, e.g. as part of our internal processes and administration.

These further purposes include, for example, administrative purposes (such as the management of master data, accounting and data archiving and the testing, management and ongoing improvement of IT infrastructure), the protection of our rights (e.g. to enforce claims in court, before or out of court and before authorities in Switzerland and abroad or to defend ourselves against claims, for example by preserving evidence, legal clarifications and participation in court or official proceedings) and the evaluation and improvement of internal processes. The safeguarding of other legitimate interests is also among the further purposes, which cannot be listed exhaustively.

5. On what basis do we process your data?

Where we ask for your consent for certain processing, we will inform you separately about the corresponding purposes of the processing. You may withdraw your consent at any time with effect for the future by written notice (by post) or, unless otherwise stated or agreed, by e-mail to us; our contact details can be found in section 2. For the withdrawal of your consent to online tracking, see section 12. As soon as we have received notification of the withdrawal of your consent, we will no longer process your data for the purposes to which you originally consented, unless we have another legal basis for doing so. The withdrawal of your consent does not affect the lawfulness of the processing carried out on the basis of the consent until its withdrawal.

Where we do not ask for your consent for processing, we base the processing of your personal data on the fact that the processing is necessary for the initiation or performance of a contract with you (or the organisation you represent) or that we or third parties have a legitimate interest in it, in particular in order to pursue the purposes described above in section 4 and the associated objectives and to be able to implement corresponding measures. Our legitimate interests also include compliance with legal provisions, insofar as this is not already recognised as a legal basis by the applicable data protection law (e.g. in the case of the GDPR, the law in the EEA and in Switzerland). This also includes the marketing of our services, the interest in better understanding our markets and in managing and further developing our company, including its operations, safely and efficiently.

If we receive sensitive data (e.g. health data, information on political, religious or philosophical views or biometric data for identification purposes), we may also process your data on the basis of other legal grounds, e.g. in the event of disputes due to the necessity of processing for possible litigation or the enforcement or defence of legal claims. In individual cases, other legal grounds may apply, which we will communicate to you separately where necessary.

6. What applies to profiling and automated decisions?

We may automatically evaluate certain of your personal characteristics on the basis of your data («profiling») in order to provide you with targeted information about our services or to identify risks of abuse and security risks. This concerns in particular the analysis of usage and interaction data in connection with our newsletter or our web presence. We do not make any fully automated individual decisions that have legal consequences or significant disadvantages for you.

7. To whom do we disclose your data?

In connection with our contracts, the website, our services, our legal obligations or otherwise to protect our legitimate interests and for the other purposes listed in section 4, we also transfer your personal data to third parties, in particular to the following categories of recipients:

- Group companies

We may disclose data to other companies of the PHM Group. An overview of the companies involved in Switzerland and abroad can be found at www.phmgroup.ch/unserefirmen. The disclosure serves the performance of cross-group contracts, central administration (e.g. in shared IT systems such as the group-wide CRM system) and internal support and controlling purposes on the basis of our legitimate interests. Only those departments and persons who are authorised to do so in accordance with authorisation rules have access to the data.

- Service providers: We work with service providers in Switzerland and abroad who process data about you on our behalf or under joint responsibility with us, or who receive data about you from us under their own responsibility (e.g. IT providers, banks, insurance companies).

In order to provide our services efficiently and to be able to concentrate on our core competencies, we obtain services from third parties in numerous areas. These services concern, for example, IT services, the dispatch of information, marketing, sales, communication or printing services, facility management, building security and cleaning, the organisation and holding of events and receptions, debt collection, credit agencies, address verification services (e.g. to update address records in the event of relocations), fraud prevention measures and services provided by consulting firms, lawyers, banks, insurers and telecommunications companies. We disclose to these service providers the data required for their services, which may also concern you. In addition, we conclude contracts with these service providers that include provisions on data protection, insofar as such protection does not arise from the law.

- Contractual partners including customers: This refers to our customers and other contractual partners, because this data transfer results from these contracts. If you yourself work for such a contractual partner, we may also transfer data about you to that partner in this context.

If you act as an employee for a company with which we have concluded a contract, the performance of this contract may result in us informing the company, for example, how you have used our service.

- Authorities: We may disclose personal data to offices, courts and other authorities in Switzerland and abroad if we are legally obliged or entitled to do so or if this appears necessary to protect our interests. The authorities process data about you that they receive from us under their own responsibility.

Examples include criminal investigations, police measures (e.g. health protection concepts, combating violence etc.), regulatory requirements and investigations, court proceedings, reporting obligations and pre-trial and out-of-court proceedings, as well as statutory obligations to provide information and cooperate. Data may also be disclosed if we wish to obtain information from public bodies, e.g. to justify an interest in information or because we have to state about whom we require information (e.g. from a register).

- Other persons: This refers to other cases where the involvement of third parties results from the purposes set out in section 4 (e.g. service recipients).

Other recipients include, for example, delivery addressees or third-party payment recipients specified by you, other third parties, including in the context of representation relationships (e.g. when we send your data to your lawyer or your bank), or persons involved in official or court proceedings. As part of corporate development, we may sell or acquire businesses, parts of businesses, assets or companies or enter into partnerships, which may also result in the disclosure of data (including yours, e.g. as a customer or supplier or as a supplier representative) to the persons involved in these transactions.

All these categories of recipients may in turn involve third parties, so that your data may also become accessible to them. We can restrict processing by certain third parties (e.g. IT providers), but not by others (e.g. authorities, banks etc.).

8. Does your personal data also go abroad?

As explained in section 7, we also disclose data to other parties. These are not only located in Switzerland. Your data may therefore also be processed in Europe (e.g. at the headquarters of our parent company in Finland); in exceptional cases, however, in any country in the world (such as South Africa).

If a recipient is located in a country without adequate statutory data protection, we contractually oblige the recipient to comply with the applicable data protection (for this purpose we use the revised standard contractual clauses of the European Commission, which are available here: https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj), unless the recipient is already subject to a legally recognised set of rules to ensure data protection and we cannot rely on an exemption. An exception may apply in particular in the case of legal proceedings abroad, but also in cases of overriding public interest or if the performance of a contract requires such disclosure, if you have consented or if the data concerned has been made generally accessible by you and you have not objected to its processing.

Many countries outside Switzerland, the EU and the EEA do not currently have laws that guarantee an adequate level of data protection from the perspective of the FADP or the GDPR. The contractual arrangements mentioned can partially compensate for this weaker or missing legal protection. However, contractual arrangements cannot eliminate all risks (in particular of government access abroad). You should be aware of these residual risks, even if the risk may be low in an individual case and we take further measures (e.g. pseudonymisation or anonymisation) to minimise it.

Please also note that data exchanged via the internet is often routed through third countries. Your data may therefore end up abroad even if the sender and recipient are located in the same country.

9. How long do we process your data?

We process your data for as long as our processing purposes, the statutory retention periods and our legitimate interests in processing for documentation and evidence purposes require, or for as long as storage is technically necessary. Further information on the respective storage and processing periods can be found under the individual data categories in section 3 and under the cookie categories in section 12. Unless legal or contractual obligations prevent this, we will delete or anonymise your data after the storage or processing period has expired as part of our usual processes.

Documentation and evidence purposes include our interest in documenting processes, interactions and other facts in the event of legal claims, discrepancies, IT and infrastructure security purposes and proof of good corporate governance and compliance. Retention may be technically necessary if certain data cannot be separated from other data and we therefore have to retain it together with that data (e.g. in the case of backups or document management systems).

10. How do we protect your data?

We take appropriate security measures to maintain the confidentiality, integrity and availability of your personal data, to protect it against unauthorised or unlawful processing and to counter the risks of loss, unintentional alteration, unwanted disclosure or unauthorised access.

Technical and organisational security measures may include, for example, encryption and pseudonymisation of data, logging, access restrictions, storage of backup copies, instructions to our employees, confidentiality

agreements and checks. We protect your data transmitted via our website in transit by means of suitable encryption mechanisms. However, we can only secure areas that we control. We also oblige our processors to take appropriate security measures. However, security risks can generally not be ruled out entirely; residual risks are unavoidable.

11. What rights do you have?

Under certain circumstances, the applicable data protection law grants you the right to object to the processing of your data, in particular processing for direct marketing purposes and for other legitimate interests in the processing.

To make it easier for you to control the processing of your personal data, you also have the following rights in connection with our data processing, depending on the applicable data protection law:

- The right to request information from us as to whether and which data we process about you;
- the right to have us correct data if it is inaccurate;
- the right to request the deletion of data;
- the right to request that we hand over certain personal data in a commonly used electronic format or transfer it to another controller;
- the right to withdraw consent, insofar as our processing is based on your consent;
- the right to obtain, on request, further information necessary for the exercise of these rights.

If you wish to exercise the above rights against us, please contact us in writing, on site or, unless otherwise stated or agreed, by e-mail; our contact details can be found in section 2. To rule out misuse, we must identify you (e.g. with a copy of your ID, unless this is otherwise possible).

Please note that these rights are subject to conditions, exceptions or restrictions under the applicable data protection law (e.g. to protect third parties or trade secrets). We will inform you accordingly where applicable.

In particular, we may need to continue processing and storing your personal data in order to perform a contract with you, to protect our own legitimate interests, such as the assertion, exercise or defence of legal claims, or to comply with legal obligations. To the extent permitted by law, in particular to protect the rights and freedoms of other data subjects and to safeguard legitimate interests, we may therefore also reject a data subject request in whole or in part (e.g. by redacting certain content concerning third parties or our trade secrets).

If you do not agree with how we handle your rights or with our data protection practices, please let us know (section 2). In particular, if you are located in the EEA, the United Kingdom or Switzerland, you also have the right to lodge a complaint with the data protection supervisory authority in your country.

12. Do we use online tracking and online advertising techniques?

On our website, we use various techniques with which we and third parties engaged by us can recognise you during your use and possibly also track you across several visits. In this section, we inform you about this.

Essentially, the aim is for us to be able to distinguish your access (via your system) from access by other users so that we can ensure the functionality of the website and carry out analyses and personalisation. We do not intend to infer your identity, even if we are able to do so insofar as we or third parties engaged by us can identify you by combination with registration data. Even without registration data, however, the techniques used are designed in such a way that you are recognised as an individual visitor each time you access a page, for example by our server (or the servers of third parties) assigning a specific identification number to you or your browser (a so-called «cookie»).

Cookies are individual codes (e.g. a serial number) that our server or a server of our service providers or advertising partners transmits to your system when you connect to our website and that your system (browser, mobile) accepts and stores until the programmed expiry date. With each subsequent access, your system transmits these codes to our server or the server of the third party. In this way, you are recognised even if your identity is unknown.

Other techniques may also be used to recognise you with a greater or lesser degree of probability (i.e. to distinguish you from other users), e.g. «fingerprinting». Fingerprinting combines your IP address, the browser you use, the screen resolution, the language selection and other information that your system communicates to every server, which results in a more or less unique fingerprint. This makes it possible to dispense with cookies.
Whenever you access a server (e.g. when using a website or an app or because an image is visibly or invisibly embedded in an e-mail), your visits can therefore be «tracked». If we integrate offerings from an advertising partner or provider of an analysis tool on our website, that provider can track you in the same way, even if you cannot be identified in the individual case.

We use such techniques on our website and allow certain third parties to do so as well. You can program your browser to block or deceive certain cookies or alternative techniques, or to delete existing cookies. You can also add software to your browser that blocks tracking by certain third parties. You can find more information on this on the help pages of your browser (usually under the keyword «privacy») or on the websites of the third parties listed below.

A distinction is made between the following cookies (techniques with comparable functionality, such as fingerprinting, are also included here):

- Necessary cookies: Some cookies are necessary for the functioning of the website as such or for certain functions. For example, they ensure that you can switch between pages without losing information entered in a form. They also ensure that you remain logged in. These cookies exist only temporarily («session cookies»). If you block them, the website may not work. Other cookies are necessary so that the server can store decisions or entries you have made beyond one session (i.e. one visit to the website) if you use this function (e.g. selected language, consent given, the function for automatic login etc.). These cookies have an expiry date of up to 24 months.

- Performance and Marketing cookies: In order to optimise our website and the related offerings and to better adapt them to users' needs, we use cookies to record and analyse the use of our website, possibly also beyond the session. We do this by using third-party analytics services. Marketing cookies are also used to measure the success of our advertising campaigns and to display interest-based advertisements. We have listed these services below. These cookies also have an expiration period of up to 24 months. Details can be found on the websites of the third-party providers.

We currently use offerings from the following service providers and advertising partners (insofar as they use data from you or cookies set on your device for advertising control):

- Google Analytics: Google Ireland (based in Ireland) is the provider of the «Google Analytics» service and acts as our processor. For this purpose, Google Ireland relies on Google LLC (based in the USA) as its processor (both «Google»). Google uses performance cookies (see above) to track the behaviour of visitors to our website (duration, frequency of pages viewed, geographical origin of access etc.) and on this basis prepares reports for us on the use of our website. We have configured the service so that the IP addresses of visitors are truncated by Google in Europe before being forwarded to the USA and therefore cannot be traced. We have switched off the «data sharing» and «signals» settings. Although we may assume that the information we share with Google is not personal data for Google, it is possible that Google may use this data for its own purposes to draw conclusions about the identity of visitors, create personal profiles and link this data to the Google accounts of these individuals. If you consent to the use of Google Analytics, you expressly consent to such processing, which also includes the transfer of personal data (in particular usage data for the website and app, device information and individual IDs) to the USA and other countries. Information on data protection at Google Analytics can be found here [https://support.google.com/analytics/answer/6004245] and, if you have a Google account, further information on processing by Google can be found here [https://policies.google.com/technologies/partner-sites?hl=en].

- Google Ads: Google Ireland (based in Ireland) is the provider of the «Google Ads» service. For

this purpose, Google Ireland relies on Google LLC (based in the USA) as its processor. Google uses marketing cookies (see above) to track the actions of visitors to our website (e.g. purchases or contact requests) in order to measure the success of our advertising campaigns and to show you tailored advertising in the Google advertising network based on your previous browsing behaviour. Google may link this information to your Google account and create user profiles for its own purposes. By giving your consent, you agree to this processing and to the transfer of data to the USA and other countries. Information on data protection at Google in connection with advertising can be found here [https://policies.google.com/technologies/ads?hl=en].

- LinkedIn Insight Tag: LinkedIn Ireland Unlimited Company (based in Ireland) is the provider of the «LinkedIn Insight Tag» service. LinkedIn uses marketing and performance cookies (see above) to track the behaviour of visitors to our website (e.g. pages viewed, clicks, job-related characteristics) and prepares reports for us on the effectiveness of our advertisements and on the target groups of our website. Although we can assume that the information visible to us does not allow any direct conclusions to be drawn about your identity, LinkedIn may assign this data to your LinkedIn account, use it for its own advertising purposes and link it to profiles on other LinkedIn platforms. If you consent to the use of the LinkedIn Insight Tag, you expressly consent to this processing and to the possible transfer of data to the USA. Information on data protection at LinkedIn can be found here [https://www.linkedin.com/legal/privacy-policy].

- Meta Pixel: Meta Platforms Ireland Ltd. (based in Ireland) is the provider of the «Meta Pixel» service (covering Facebook and Instagram). Meta uses marketing cookies (see above) to track the interactions of visitors to our website after they have seen or clicked on an advertisement on Facebook or Instagram (conversion tracking). This enables us to measure the effectiveness of our advertising measures and to display personalised advertising. Meta may link this data to your Facebook or Instagram account and use it for its own advertising purposes. By giving your consent, you agree to this processing and to the transfer of data to Meta Platforms Inc. in the USA. Information on data protection at Meta can be found here [https://www.facebook.com/about/privacy/].

13. What data do we process on our social network pages?

We may operate pages and other online presences («fan pages», «channels», «profiles» etc.) on social networks and other platforms operated by third parties and collect the data about you described in section 3 and below. We receive this data from you and the platforms when you come into contact with us via our online presence (e.g. when you communicate with us, comment on our content or visit our presence). At the same time, the platforms evaluate your use of our online presences and link this data with other data about you known to the platforms (e.g. about your behaviour and preferences). They also process this data for their own purposes under their own responsibility, in particular for marketing and market research purposes (e.g. to personalise advertising) and to control their platforms (e.g. which content they show you).

We receive data about you when you communicate with us via online presences or view our content on the corresponding platforms, visit our online presences or are active on them (e.g. publish content, post comments). These platforms also collect from you or about you, among other things, technical data, registration data, communication data, behavioural and preference data (for definitions of these terms, see section 3). These platforms regularly evaluate statistically the way in which you interact with us and how you use our online presences, our content or other parts of the platform (what you look at, comment on, «like», share etc.) and link this data with other information about you (e.g. information on age and gender and other demographic information). In this way, they also create profiles about you and statistics on the use of our online presences. They use this data and profiles to show you our or other advertising and other content on the platform in a personalised manner and to control the behaviour of the platform, but also for market and user research and to provide us and other parties with information about you and the use of our online presence. We can partially control the analyses that these platforms create regarding the use of our online presences.

We process this data for the purposes described in section 4, in particular for communication, for marketing purposes (including advertising on these platforms, see section 12) and for market research. Information on the corresponding legal bases can be found in section 5. We may ourselves redistribute

content published by you (e.g. comments on an announcement) (e.g. in our advertising on the platform or elsewhere). We or the operators of the platforms may also delete or restrict content from or about you in accordance with the terms of use (e.g. inappropriate comments).
For further information on the processing carried out by the platform operators, please refer to the platforms' privacy notices. There you will also find out in which countries they process their data, which rights of access, deletion and other data subject rights you have and how you can exercise them or obtain further information.

14. Can this privacy policy be changed?

This privacy policy does not form part of any contract with you. We may amend this privacy policy at any time. The version published on this website is the current version.

Last updated: 22.10.2026