Privacy policy

We, Dr. W. Meili + Partner AG, Zurich, Pannell Kerr Forster AG, Zurich (incl. Zug branch office), PKF Consulting AG, Zurich, and PKF Wirtschaftsprüfung AG, Zurich (collectively referred to as PKF Zurich) are responsible for the data processing specified in this privacy policy, unless stated otherwise.

Please take note of the information below to know what personal data we collect from you and for what purposes we use it. When it comes to data protection, we primarily adhere to the legal requirements of Swiss data protection law, in particular the Federal Act on Data Protection (FADP), as well as the GDPR, which may be applicable in individual cases.

If you have any questions or suggestions regarding data protection, you can mail our operations Data Protection Officer, Ms Dominique Kipfer to the following address at any time:

PKF Consulting AG
Data Protection Officer
Lavaterstrasse 40
CH-8002 Zürich

or send an email to: dominique.kipfer@pkf.ch

I. Scope and purpose of the collection, processing, and use of personal data

1. When visiting our website

When you visit our website, our servers temporarily store every access in a log file. With-out your intervention, the following data is processed and stored by us until automated deletion after 26 months:

- the IP address of the requesting computer
- the name of the owner of the IP address range (usually your Internet access provider)
- the date and time of access

- the website from which the access originated (referrer URL), possibly with the search term used
- the name and URL of the accessed file
- the status code (e.g., error message)
- the operating system of your computer
- the browser you are using (type, version, and language)
- the transmission protocol used (e.g., HTTP/1.1)
- your username from a registration/authentication

The collection and processing of this data are carried out for the purpose of enabling the use of our website (establishing a connection), ensuring the ongoing system security and stability, enabling the optimisation of our internet offering, and for internal statistical pur-poses. With regard to the aforementioned purposes, we have a legitimate interest in the data processing within the meaning of Art. 6(1)(f) GDPR. This data processing cannot be objected to, as we would not be able to provide you with the website otherwise.

Only in the event of an attack on the network infrastructure or a suspicion of other unau-thorised or abusive website use, the IP address will be analysed for investigation and de-fence purposes and, if necessary, used in the context of criminal proceedings for identifi-cation and civil or criminal action against the users concerned. Our legitimate interest in this data processing within the meaning of Art. 6(1)(f) GDPR lies in the purposes described above.

Lastly, we use cookies and other cookie-based applications when you visit our websites. Further information can be found in Section II "Cookies".

2. Contact form

You have the possibility to use our contact form to get in touch with us. The entry of the following personal data is required (* mandatory):

- Full Name*
- Email*
- Phone Number*
- Message*

We use this and other data voluntarily provided in the message (such as title, address, phone number, name of company, etc.) only to be able to answer your contact request in the best possible and personalised way. Any voluntary

information about how you be-came aware of our offer will also be used for internal statistical purposes. The pro-cessing of your contact request is our legitimate interest within the meaning of Art. 6(1)(f) GDPR. You can object to this data processing at any time if there are reasons relating to your particular situation that justify the objection to the data processing.

3. Contacting us via email

You have the possibility to contact us via email or phone to ask questions about our services. We only collect the personal data that you disclose to us. Therefore, you are responsible for the content of your communication and have control over the infor-mation you provide to us. We recommend that you do not submit sensitive information. To answer your questions, we may ask you to provide additional information (e.g., your address, phone number, etc.). We will only collect the personal data from you that is necessary to answer your questions or to provide the services you have requested.

For handling contact requests through the contact form, we use a software application provided by Umbraco, Denmark. Therefore, your data may be stored in a database of Umbraco, which may allow Umbraco to access your data if this is necessary for provid-ing the software and supporting its use. Information about data processing by third parties and any transfer abroad can be found in Section VII of this privacy policy.

The legal basis for the data processing is our legitimate interest within the meaning of Art. 6(1)(f) GDPR in responding to your request or, if your request is directed towards the conclusion or performance of a contract, the necessity for the implementation of the required measures within the meaning of Art. 6(1)(b) GDPR.

There is a possibility that Umbraco may want to use some of this data for its own purposes (e.g., for sending marketing emails or conducting statistical analysis). For these data processing activities, Umbraco is the data controller and must ensure compliance of these processing activities with data protection laws. Information about data processing by Umbraco can be found at https://umbraco.com/trust-center/.

4. Applying for a position with us

You have the possibility to apply for open positions with us via email or postal mail. When you apply, we collect the data that you provide us with in your application docu-ments.

We need your application documents in order to review your application and to contact you in this context if necessary. The legal basis for the data processing is the imple-mentation of pre-contractual measures or the execution of a contract within the meaning of Art. 6(1)(b) GDPR, as well as our overriding legitimate interest within the meaning of Art. 6(1)(f) GDPR. You can object to this data processing at any time if there are rea-sons relating to your particular situation that justify the objection to the data processing. However, if you object, we will not be able to continue the application process.

Application documents of unsuccessful applicants will be deleted after the application process is completed, unless you explicitly consent to a longer retention period or we are legally obligated to retain them for a longer period.

5. Processing of personal data in the context of mandate relationships

We primarily process the personal data that we receive from our clients and other busi-ness partners in the context of our mandate relationships with them and other persons involved in these relationships:

- Personal data from publicly available sources:
  We obtain certain personal data (e.g., names, business-related information, etc.) from publicly available sources (e.g., debt enforcement registers, land registers, commercial registers, press, internet, etc.), media, and the internet (where applicable in the specific case, e.g., from press reviews, marketing/sales campaigns, etc.) to provide our services properly.

- Personal data related to contractual relationships:
  We process personal data (e.g., contact details, family circumstances, nationality, residence status, religion, employment status, payment data, information about income / assets / expenses / donations / inheritances, references, delivery address, powers of attorney, services according to the domicile agreement,

other contracts, or GTC, etc.) related to our clients, their employees, received from authorities (arbitration authorities), courts, and other third parties (e.g., counterparties, business partners and contracting partners of our clients), as well as information from banks, insurance companies, sales partners and other contracting partners of ours for the use or provision of services by you (e.g., payments and purchases made). This also includes information about third parties that you provide to us (e.g., information about your partner for tax assessment purposes). By providing us with such information, you ensure that any third parties have been adequately informed about this data transfer and, if necessary, have consented to it.

- Data from third parties:
  We also process personal data that is provided to us by third parties in the context of our services. This includes information about you provided to us by persons close to you (employers, family members, advisors, legal representatives, etc.), information we receive from third parties about you, in particular information from public registers, information which we learn about in connection with official and judicial procedures, information in connection with your professional roles and activities, information about you in correspondence and discussions with third parties, credit rating information (if we do business with you personally), information from banks, insurance companies, sales partners, and other contracting partners of ours for the use or provision of services by you (e.g., payments made, purchases made).

- Data for compliance with legal obligations:
  Information related to compliance with legal requirements, such as anti-money laundering and export restrictions.

- Sensitive personal data:
  We process sensitive personal data for the provision of our services, especially in the area of payroll administration and tax services. This data, usually, contained in documents, may also provide information about race or ethnic origin, religious beliefs, health status, political views and biometric data of private individuals or beneficial owners of legal entities. The sensitive data also includes negative information related to criminal offences or

criminal convictions of potential or existing customers and applicants. Although our website and services are not consciously tailored or targeted at children, we occasionally receive information about children, for example, as part of a service contract.

For the processing of personal data for the purposes mentioned above, in particular for the provision of our services, we rely on the implementation of pre-contractual measures or the execution of a contract within the meaning of Art. 6(1)(b) GDPR, our legitimate in-terest within the meaning of Art. 6(1)(F) GDPR and the fulfillment of legal obligations pur-suant to Art. 6(1)(c) GDPR. If the data processing is based on our legitimate interest, you can object to this data processing at any time if there are reasons relating to your particu-lar situation that justify the objection to the data processing. In the case of the processing of personal data in the context of the execution of a contract, you can also object to the processing, but we may then no longer be able to provide the service requested by you.

Sensitive personal data will only be processed with your consent pursuant to Art. 6(1)(a) GDPR, unless the data has been transferred to us indirectly and for legitimate purposes. In these cases, we rely on the legal bases listed above. You can withdraw your consent at any time with future effect.

6. Marketing

We use your personal data to provide you with information relevant to our services. For this purpose, we process the following data:

- your addresses, email addresses; and
- if applicable, interests (e.g., based on your income and wealth structure), and other socio-demographic data

We use this personal data to send you our newsletter or updates about our services. For this processing, we rely on your consent within the meaning of Art. 6(1)(a) GDPR. You can withdraw your consent at any time with future effect.

7. Use of Microsoft 365 for online meetings, phone communication, and data processing in connection with client-related tasks

7.1 Use of Microsoft 365 in general

For our daily work, we use Microsoft 365 and various applications contained therein. Mi-crosoft 365 is a software provided by Microsoft Corporation, One Microsoft Way Red-mond, WA 98052-6399, USA. However, our contractual partner is Microsoft Ireland Opera-tions Limited, One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, Ireland (Microsoft).

The office suite includes numerous services commonly used in office work, such as Word, PowerPoint, Excel, Outlook, and Teams. Microsoft 365 also offers additional online services. These include various cloud services, such as OneDrive and Exchange Online, where data is stored on Microsoft's servers instead of within our company. All data is stored in data centres in Switzerland. We use Office 365 E5.

A direct exchange of personal data between you and our Microsoft 365 applications pri-marily takes place during online meetings via the "Microsoft Teams" tool (see below) and in email communication. In most cases, you will not have direct interaction with the other functionalities of Microsoft 365. However, in exceptional situations, and with your con-sent, we may provide you access to specific features of Microsoft 365 if it is necessary or beneficial for the processing of your mandate.

If we should exceptionally grant you direct access to Microsoft 365, even if only for a limited period of time, your following data will be processed:

- IP address used to access Microsoft 365 applications
- your username (login credentials for Microsoft 365 applications), and data related to multi-factor authentication, which you have personally entered in your Microsoft account (e.g., optionally, your (private) mobile number)
- identification details: information about you as a user, sender, or recipient of data within Microsoft 365 applications. In particular, this includes the following master data: name, business contact data such as phone number, email address, business fax number, if provided by you. Additional data (such as a profile picture you have uploaded) can also be viewed in your profile at any time. This

information is visible to you at all times in your profile and in Outlook, where you can customise it as needed

- data required for authentication and licensing purposes. In Microsoft 365 applications, all user actions, such as time of access, date, type of access, indication of the data/files/documents accessed and all activities related to the use, such as creating, modifying, deleting a document, creating a team (and channels in Teams), making notes in a notebook, starting a chat, replying in a chat are processed

Otherwise, we process via Microsoft 365 all the data you provide to us by phone or email when you contact us. If the data processing takes place with regard to a mandate, we process the data listed in Section 5 above.

Currently, the following Microsoft 365 applications store data at rest in Switzerland: Ex-change Online, SharePoint, OneDrive, Teams, and Azure. However, data stored at rest in Switzerland may be transferred to other countries during the use of these applications. Microsoft 365 applications other than those mentioned above may also store data at rest outside of Switzerland. According to Microsoft, in such cases, the data is primarily stored on servers in the EU. For these data processing activities, we have entered into a data processing agreement with Microsoft in accordance with Art. 28 GDPR and Art. 9 and Art 16 et seq. FADP respectively. Accordingly, we have agreed with Microsoft on compre-hensive technical and organisational measures for Microsoft 365 that correspond to the current state of IT security technology, in particular with regard to access control and end-to-end encryption concepts for data transmission, databases, and servers. Microsoft has also added further protective provisions to the EU standard contractual clauses included in its contracts. Accordingly, Microsoft undertakes to take action against any request from a governmental authority and to compensate users in the event of governmental access. When data is transferred to third countries, Microsoft always uses state-of-the-art encryption and promises that the data will be returned to the internal storage location in the EU immediately after the processing.

The legal basis for the processing of personal data within Microsoft Teams is described below. The primary legal basis for all other data processing in Microsoft 365 is the imple-mentation of pre-contractual measures or the execution of a contract, i.e., the mandate relationship, within the meaning of Art. 6(1)(b) GDPR. If you contact us (by phone or email) outside of a mandate

relationship, the legal basis is our legitimate interest in cor-rectly responding to and managing your requests within the meaning of Art. 6(1)(f) GDPR. You can object to this data processing at any time. In this case, however, we may no longer be able to process your requests.

In connection with the use of Microsoft 365, Microsoft also processes certain data as an independent controller and not as a processor on our behalf. This poses a data protection risk for the data subjects whose data is processed in Microsoft 365. We have entered into data protection agreements and EU standard contractual clauses with Microsoft to guar-antee a minimum level of data protection. Please note that we have no control over Mi-crosoft's data processing. To the extent that Microsoft processes personal data in con-nection with the use of Microsoft 365, Microsoft is an independent data controller for that use and, as such, is responsible for compliance with all applicable laws and obligations of a data controller. For more information about the purpose and scope of these data processing activities, please see Microsoft's privacy policy here. There you will also find further information about your rights in this regard.

Microsoft collects and processes, in particular, diagnostic data in order to keep Microsoft 365 secure and up-to-date, address issues, and make product improvements. By using Windows Restricted Traffic Limited Functionality, we restrict Microsoft 365 applications' connections to Microsoft. This minimises the diagnostic data shared with Microsoft.

7.2 Microsoft Teams

We use the Microsoft Teams application to conduct conference calls, online meetings, video conferences and/or webinars (Online Meetings). Microsoft Teams is part of Microsoft 365.

When using Microsoft Teams, various types of data are processed. The scope of the data processing also depends on the information you provide before or during your participation in an online meeting.

The following personal data may be subject to processing:

- user details: e.g., display name, email address (if applicable), profile picture (optional), preferred language

- meeting metadata: e.g., date, time, meeting ID, phone numbers, location, text, audio, and video data
- authentication data
- protocol log files
- contents of the online meeting (if you personally participate and make contributions)
- you may have the option to use the chat function in an online meeting. In this case, the text entries you make will be processed to display them in the online meeting. To enable the display of video and playback of audio, data from your device's microphone and, if available, the device's video camera will be processed during the meeting. You can turn off or mute the camera or microphone yourself using the Microsoft Teams application
- when dialling in with phone: information about the incoming and outgoing phone number, country name, start and end times. Additional connection data such as the IP address of the device may be stored if necessary.

If we intend to record online meetings, we will transparently communicate this to you before the online meeting and, if necessary, ask for your consent. If it is necessary for the purpose of documenting the results of an online meeting, we will log the chat contents. However, this will generally not be the case.

The legal basis for this data processing is the implementation of pre-contractual measures or the execution of a contract within the meaning of Art. 6(1)(b) GDPR, provided that the meetings or phone communications take place within the framework of the customer relationship. Outside the customer relationship, the legal basis is our legitimate interest within the meaning of Art. 6(1)(f) GDPR, namely, in responding optimally to your contact request by phone or via a meeting. If our legal basis is our legitimate interest, you can object to this data processing at any time.

Note: when you access the Microsoft Teams website, Microsoft is responsible for data processing. Accessing the website is only necessary for downloading the software to use Teams. You can also use Teams by entering the respective meeting ID and, if necessary, other access data for the meeting directly in the Teams app or by clicking on the link to the meeting provided to you.

Microsoft reserves the right to process the personal data collected through Microsoft Teams for its own business purposes, provided that Microsoft has access to such data at all. This poses a data protection risk for users of Microsoft Teams. We have entered into data protection agreements and EU standard

contractual clauses with Microsoft to guarantee a minimum level of data protection. Please note that we have no control over Microsoft's data processing. To the extent that Microsoft Teams processes personal data in connection with Microsoft's legitimate business activities, Microsoft is an independent data controller for this use and is responsible for complying with all applicable laws and obligations of a data controller. For more information on the purpose and scope of data collection and processing by Microsoft Teams, please refer to Microsoft's privacy policy available here. The information on data processing specific to Microsoft Teams is available here. There you can also find additional information about your rights in this regard. In addition, Microsoft may process your personal data in the US (for more information, please see Section VIII below).

8. Registration for events / data collection related to events

We regularly organise events, including physical events on specific topics, general corporate events, webinars, etc., for which customers, business partners, and other interested parties can register. As part of the registration process, we collect various information about the participants. During the registration process, you will be informed about the specific information that we require from you. We collect, among others, the following information:

- first name
- last name
- company name
- country
- street/address
- postal code
- place/city
- canton
- phone number
- email address
- consent to the GTC and the privacy policy
- for paid events, the payment information
- additional information depending on the event (e.g., dietary preferences, etc.)

We need this information to ensure your participation in the respective events and to organise the events efficiently. The legal basis for this data processing is

the implementation of pre-contractual measures or the execution of a contract within the meaning of Art. 6(1)(b) GDPR.

During our own events and events organised by other entities, we may also receive information from you, e.g., when you provide us with your business card or connect with us or our employees on LinkedIn for business purposes. You voluntarily provide us with this information. We will include this information, along with other personal data mentioned in this privacy policy, in our central electronic data processing system, and use it for managing our business relationships (see Section 9 below). The legal basis for this data processing is the implementation of pre-contractual measures or the execution of a contract within the meaning of Art. 6(1)(b) GDPR, or our legitimate interest within the meaning of Art. 6(1)(f) GDPR to efficiently and purposefully manage contacts and business relationships. You can object to this data processing at any time. However, this may affect our ability to provide you with certain requested services.

9. Central customer database

We store the personal data affected by and mentioned in this privacy policy in a central electronic data processing system. For this purpose, we work with the software platform provided by Abacus Research AG, Abacus-Platz 1, 9300 Wittenbach, Switzerland.

In addition to the aforementioned processing purposes, we also use this personal data to organise and manage our business relationships with you. For this purpose, we assign various characteristics to you in our central data processing system (e.g., topics you have shown interest in, etc.). We derive these characteristics from the information provided by you or the data collected about you as mentioned above. However, we do not carry out comprehensive profiling for these purposes. The following personal data are particularly relevant in this regard:

- name, title, age, year of birth
- gender
- contact details
- professional data (e.g., function, position; your business website, business email; professional qualifications, education, and specialisation)

- information about interactions with us, such as topics covered, questions asked about our company and products, events you have attended; your feedback on events, etc.

This processing is based on our legitimate interest within the meaning of Art. 6(1)(f) GDPR for the customer-friendly and efficient management of customer data. The processing is also carried out to possibly display interest-based content on the website or in our communication with you. The legal basis for this processing is the contract fulfilment within the meaning of Art. 6(1)(b) GDPR. You can object to this data processing at any time.

After consultation with and approval by us, customers can access and modify certain personal data directly in the Abacus solution. For these data processing activities, customers are considered data controllers under data protection law. We assume no liability for damages related to these data processing activities. The customer must ensure that only those persons (employees or contractual partners of the customer) who have received the appropriate authorisation from the customer can access the personal and financial data. The customer is responsible for all actions and data processing carried out via their granted access to the Abacus solution.

II. Cookies / tracking tools (e.g., Google Analytics / DoubleClick / web analytics services etc.)

1. Cookies

Cookies are information files that your web browser stores on the hard drive or in the memory of your computer when you visit our Website. Cookies are assigned identification numbers that enable your browser to be identified, and allow the information contained in the cookie to be read.

Cookies are used to make your visit to our website easier, more enjoyable, and more meaningful. We use cookies for various purposes that are necessary for the desired use of the website, i.e., "technically necessary." For example, we use cookies to identify you as a registered user after logging in, so you don't have to log in again when navigating to different subpages. Furthermore, cookies perform other technical functions necessary for the operation of the website, such as load balancing, which distributes the workload of the site across various web servers to relieve the servers. Cookies are also used for security purposes, such as preventing the unauthorised posting of content. Finally, we use cookies

in the design and programming of our website, for example, to enable the uploading of scripts or codes.

In addition to cookies which are only used during a session and are deleted after your visit to the website ("session cookies"), cookies can also be used to store user settings and other information for a certain period of time (e.g. two years) ("permanent cookies"). However, you can set your browser to reject cookies, save them for one session only, or otherwise delete them prematurely. Most browsers are set by default to accept cookies automatically. We use permanent cookies to better understand how you use our offerings and content. In general, cookies can also be blocked by you - although this can cause functions such as language selection, location etc. to stop working.

The legal basis for this data processing is our legitimate interest within the meaning of Article 6(1)(f) GDPR in providing a user-friendly and up-to-date website.

On the following pages, you will find explanations on how to configure cookie settings in the most popular browsers:

- Microsoft Windows Internet Explorer
- Microsoft Windows Internet Explorer Mobile
- Mozilla Firefox
- Google Chrome for Desktop
- Google Chrome for Mobile
- Apple Safari for Desktop
- Apple Safari for Mobile

Disabling cookies may prevent you from using all the features of our Website.

For managing cookies on our website, we use the services offered by Cookiebot. Cookiebot is provided by Usercentrics A/S, Havnegade 39, 1058 Copenhagen, DK. Cookiebot helps us manage and organise the cookies we use, including, for example, to create cookie banners. The use of these functions may result in the transmission of personal data to Cookiebot. If you allow cookies in your browser or on your device, the following information will be transmitted to Cookiebot: IP address (in hashed form), date and time of your consent to cookies, technical browser data, and cookies which you have allowed. According to the Cookiebot, this information is stored and processed within Europe. All information is deleted by Cookiebot no later than 12 months after the consent has been given.

You can prevent the transmission of information by rejecting cookies in the cookie banner or by disabling them in your browser, as described above. The legal basis for the use of Cookiebot lies in our legitimate interest in the lawful use of cookies within the meaning of Art. 6(1)(f) GDPR and, if applicable, your consent to cookies within the meaning of Art. 6(1)(a) GDPR. Further information regarding Cookiebot's data processing can be found at https://www.cookiebot.com/en/privacy-policy/.

2. Tracking and web analytics tools

2.1 General information about tracking

For the purpose of customising and continuously optimising our Website, we use the web analytics services listed below. In this context, pseudonymised usage profiles are created, and cookies are used (please see Section 1 above). The information generated by the cookie regarding your use of our Website is usually transmitted to a server of the service provider, where it is stored and processed, together with the Log File Data mentioned in Section I para. 1. This may also result in a transfer to servers abroad, e.g., the USA (see Section VIII below).

By processing the data, we obtain, among others, the following information:

- navigation path followed by a visitor on the site (including content viewed, products selected or purchased, or services booked);
- time spent on the Website or specific page;
- the specific page from which the Website is left;
- the country, region, or city from where an access is made;
- end device (type, version, colour depth, resolution, width, and height of the browser window); and
- returning or new visitor.

The provider, on our behalf, will use this information to evaluate the use of the Website, in particular to compile Website activity reports and provide further services related to Website usage and internet usage for the purposes of market research and the customisation of the Website. For these processing activities, we and the providers may be considered joint controllers in terms of data protection to a certain extent.

The legal basis for this data processing with the following services is your consent within the meaning of Article 6(1)(a) GDPR. You can withdraw your consent or oppose to processing at any time by rejecting or deactivating the relevant cookies in the settings of your web browser (see Section 1 above) or by using the service-specific options described below.

Regarding the further processing of the data by the respective provider as the (sole) controller, including any potential disclosure of this information to third parties, such as authorities due to national legal regulations, please refer to the respective privacy policy of the provider.

2.2 Google Analytics

We use the web analytics service Google Analytics provided by Google Ireland Limited, Gordon House, 4 Barrow St, Dublin, D04 E5W5, Ireland, or Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA (Google).

Contrary to the description in Section 2.1, IP addresses are not logged or stored in Google Analytics (in the version used here, "Google Analytics 4"). For accesses originating from the EU, IP address data is only used to derive location data and is immediately deleted thereafter. When collecting measurement data in Google Analytics, all IP searches take place on EU-based servers before the traffic is forwarded to Analytics servers for processing. Google Analytics utilises regional data centres. When connecting to the nearest available Google data centre in Google Analytics, the measurement data is sent to Analytics via an encrypted HTTPS connection. In these centres, the data is further encrypted before being forwarded to Analytics' processing servers and made available on the platform. The most suitable local data centre is determined based on the IP addresses. This may also result in a transfer of data to servers abroad, e.g., the USA (see Section VIII below).

You can prevent the collection of data generated by cookies related to your use of the websites (including your IP address) as well as the processing of this data by Google by downloading and installing the browser plugin available at the following link:

https://tools.google.com/dlpage/gaoptout?hl=en-GB

An opt-out cookie is stored on your device. If you delete cookies, the link must be clicked again.

III. Social media

On our website, you will find the links to the social media networks. These are not plugins provided by the provider that transmit data to the provider without the user's influence when the page is loaded. Behind the buttons for the social media networks, there is simply a link to the respective social media network, which involves transferring the website for sharing. No user data is transmitted from the website to the social media network.

The links lead to the following networks:

- Instagram LLC, 1601 Willow Rd, Menlo Park CA 94025, USA
- Meta, 1601 S. California Ave, Palo Alto, CA 94304, USA
- X International Unlimited Company, One Cumberland Place, Fenian Street Dublin 2, D02 AX07, Ireland
- LinkedIn Unlimited Company, Wilton Place, Dublin 2, Ireland

When you click on a link to our social media profile, a direct connection is established between your browser and the server of the respective social network. This provides the network with the information that you have visited our website with your IP address and clicked on the link. If you click on a link to a network while logged into your account with that network, the content of our site may be linked to your profile with the network, meaning that the network can directly associate your visit to our website with your user account. If you want to prevent this, you should log out before clicking on the respective links. An association is made in any case if you log in to the respective network after clicking on the link.

We may operate pages and other online presences on social networks and other platforms operated by third parties ("fan pages", "channels", "profiles", etc.) and collect data about you there. We receive this data from you and the platforms when you interact with us through our online presence (e.g., when you communicate with us, comment on our content, or visit our presences). At the same time, the platforms analyse your use of our online presences and link this data with other data about you known to the platforms (e.g., your behaviour and preferences). The platforms also process this data for their own purposes and in 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 display to you). The content published by you (e.g., comments on announcements) may be further distributed by us (e.g., in our

advertising on the platform or elsewhere). We or the platform operators may also delete or restrict content from or about you in accordance with the usage policies (e.g., inappropriate comments). For further information on the processing by the platform operators, please refer to the privacy policies of the respective platforms; concerning LinkedIn, see here. There you will also find information on the countries in which they process your data, what rights of access, deletion, and other data subject rights you have, and how you can exercise these rights or obtain further information.

We process this data to tailor and continuously optimise our online presences, enabling us to engage with our (potential) customers in a personalised and individualised manner, providing them with optimal and individual solutions. We also process the data to answer inquiries and to communicate directly with users via our online presences. We also use the data to control online advertising in our online presences and thereby reduce wastage.

The legal basis for data processing through our online presences is, firstly, the consent of the users of the online presences (Art. 6(1)(a) GDPR) and, also, our legitimate interest in data processing for the following purposes pursuant to Art. 6(1)(f) GDPR.

IV. How long will your data be kept?

We only store personal data for as long as it is necessary to carry out the processing described in this privacy policy within the scope of our legitimate interests. For contractual data, the storage is stipulated by statutory retention obligations. The requirements that oblige us to retain data arise, for example, from the accounting, audit and tax law regulations. According to these regulations, business communication, concluded contracts, and accounting documents must be retained for up to 10 years. If we no longer need this data to provide services for you, the data will be blocked. This means that the data may then only be used if this is necessary to fulfil the retention obligations or to defend and enforce our legal interests. The data will be deleted as soon as there is no longer any legal obligation to retain it and no legitimate interest in its retention exists.

V. What are your rights in respect to your personal data?

If the legal requirements are met, as a data subject, you have the following rights with respect to data processing:

Right of access: You have the right to request access to your personal data stored by us at any time and free of charge if we process such data. This gives you the opportunity to check what personal data concerning you we process and whether we process it in accordance with applicable data protection regulations.

Right to rectification: You have the right to have inaccurate or incomplete personal data rectified and to be informed about the rectification. In this case, we will also inform the recipients of the data concerned about the adaptations we have made, unless this is impossible or involves dis-proportionate effort.

Right to erasure: You have the right to obtain the erasure of your personal data under certain circumstances. In individual cases, particularly in the case of statutory retention obligations, the right to erasure may be excluded. In this case, the erasure may be replaced by a blocking of the data if the requirements are met.

Right to restriction of processing: You have the right to request that the processing of your per-sonal data be restricted.

Right to data portability: You have the right to receive from us, free of charge, the personal data you have provided to us in a readable format.

Right to object: You have the right to object at any time to data processing, especially with regard to data processing related to direct marketing (e.g., marketing emails).

Right to withdraw consent: You have the right to withdraw your consent at any time. However, processing activities based on your consent in the past will not become unlawful due to your withdrawal.

To exercise your rights, send a letter by mail to:

PKF Consulting AG
Data Protection Officer
Lavaterstrasse 40
CH-8002 Zurich

or send an email to: dominique.kipfer@pkf.ch.

Right of complaint: You have the right to lodge a complaint with a competent supervisory authority, e.g., against the manner in which your personal data is processed.

VI. Will your data be disclosed to third parties?

We will only disclose your personal data if you have expressly consented to it, if there is a legal obligation to do so, or if it is necessary to enforce our rights, especially to assert claims arising from the contractual relationship. Furthermore, we may share your data with third parties to the extent necessary for the use of the website and contract processing. The use of the data provided to third parties for this purpose is strictly limited to the purposes mentioned. The data recipients are contractually obligated to protect the data entrusted to them.

Various third-party service providers are explicitly mentioned in this privacy policy. The other data recipients belong to the following categories:

- member companies of the PKF network (available at: https://www.pkf.ch/netzwerk/), for any administrative purposes (e.g. hosting and support of IT applications, conducting of customer conflict investigations), as well as providing professional services to our customers (e.g. consulting services by PKF member companies in different regions);
- third parties who assist us in the provision of services and products (e.g., telecommunications system providers, post office management, IT system support, document creation services, cloud-based software services). This includes, in particular, All Consulting AG, St. Gallen, and UMB AG, Cham, from which we obtain SaaS and hosting services. The personal data is hosted on servers located in Switzerland;
- our professional advisers, including lawyers, accountants and insurers;
- insurance brokers;
- providers of payment services;
- providers of marketing services;

- law enforcement agencies or other governmental and regulatory authorities (e.g., Federal Audit Oversight Authority of Switzerland (FAOA), Swiss Financial Market Supervisory Authority (FINMA)) as well as other third parties if this serves to comply with applicable laws and regulations (e.g., tax authorities); and
- the company that hosts our website.

VII. Will your personal data be transmitted abroad?

We have the right to transfer your personal data to third parties located abroad, in particular to member companies of the PKF network, if this is necessary to carry out the data processing described in this privacy policy. Specific data transfers have been mentioned above in Sections I and VI.

When making such transfers, we will ensure compliance with the applicable legal requirements for disclosing personal data to third parties. The countries to which data is transmitted include those that, according to the decision of the Federal Council and the European Commission, have an adequate level of data protection (such as the member states of the EEA or, from the EU's perspective, Switzerland), as well as those countries (such as the USA) whose level of data protection is not considered adequate (see Annex 1 of the Data Protection Ordinance (DPO) and the website of the European Commission). If the country in question does not have an adequate level of data protection, appropriate measures will be implemented, unless an exception is specified for the individual data processing in each case (see Art. 49 GDPR or Art. 17 FADP). Unless otherwise specified, these safeguards may be provided for by standard contractual clauses as referred to in Art. 46(2)(c) GDPR or Art. 16(2)(d) FADP), which can be found on the websites of the Federal Data Protection and Information Commissioner (FDPIC) and the EU Commission. If you have any questions regarding the implemented measures, please reach out to our data protection contact person (see Section V).

VIII. Information on data transfers to the USA

Some of the third-party service providers mentioned in this privacy policy are based in the USA. For the sake of completeness, we would like to inform users residing or based in Switzerland or the EU that certain third-party service providers mentioned in this privacy policy are located in the USA. It is important to note that there are surveillance measures by US authorities in place that generally allow for the storage of all personal data of individuals whose data has

been transmitted from Switzerland or the EU to the United States. This occurs without differentiation, limitation, or exception based on the purpose for which the data is being collected and without an objective criterion that would restrict US authorities' access to the data and its subsequent use to specific, strictly limited purposes that can justify the interference associated with accessing and using the data. Furthermore, we would like to point out that affected individuals from Switzerland or the EU do not have legal remedies or effective judicial protection against general access rights of US authorities, which would allow them to access the data concerning them and to rectify or delete it. We explicitly highlight this legal and factual situation to enable you to make an informed decision regarding your consent to the use of your data.

In cases where we have mentioned in this privacy policy that the data recipients (such as Google) are based in the USA, we will take appropriate measures to adequately protect your data with our third-party service providers.

IX. Data security

We use appropriate technical and organisational security measures to protect your stored personal data against manipulation, partial or complete loss, as well as against unauthorised access by third persons. Our security measures are constantly being improved in line with technological advances.

We also take internal company data protection very seriously. Our employees and the external service providers commissioned by us, are committed to secrecy and observing the data protection provisions.

We take reasonable precautionary measures to protect your data. However, the transmission of information via the Internet and other electronic means / devises, always carries certain security risks and we cannot guarantee the security of information transmitted in this way.

X. Changes to this privacy policy

We reserve the right to amend and supplement this policy at any time. Please refer to this policy regularly. The current version updated on our website shall apply.

This privacy policy was last updated in November 2023.