

Privacy and Cookie Statement

This Privacy Statement was last updated in March 2026.

It sets out the data protection practices carried out through the use of the Internet and any other electronic communications networks by **BearingPoint Holding BV** and its associated companies (all together "**BearingPoint**"; "we", "us") and with respect to bearingpoint.com, hcube.io, ministerialkongress.de, ps.bearingpoint.com, bearingpointbill.com, bearingpoint.services, survey.bearingpoint.com, arcwide.com and other BearingPoint websites, applications and online services that link to this website privacy statement (together referred to as the "Site").

We may provide a separate privacy statement in connection with certain websites and applications that we offer, and where we do so, such privacy statement will apply to our collection and use of personal information collected through such websites and applications. A full list of our main offices can be found at <https://www.bearingpoint.com/en-gb/locations/> and at <https://www.arcwide.com/en/contact/>.

1. Personal Information Collected

1.1 BearingPoint collects personal information from you that you provide, such as your email address, job title or company name through the use of registration forms, for instance every time you sign up for an electronic newsletter, when you choose to send us an application to be considered for employment, when you register for an event, webinar or conference organized by BearingPoint, when you submit a request for proposal or for information, when you request the authorization of downloading a document, when you enter an online competition or when you send us a message via an email reply mechanism provided on the BearingPoint sites or when you choose to provide your information for surveys, quizzes, client satisfaction or benchmarking surveys.

We use a customer relation management system (the BearingPoint CRM) to store personal information about our business contacts. We collect and use business contact details for individuals associated with existing and potential BearingPoint clients to manage and maintain our relationship with those individuals.

1.2 BearingPoint collects information related to your person through public available sources or licenses data from B2B sales platforms. BearingPoint might have received your information through direct interaction at one of the various industry events in which we participate or through our Website as well. The information collected is limited to typical business card information, which may contain some or all of these categories of corporate organizational information: full name, company, office address, business phone number, business e-mail address, job title, job function, social media URL. The information collected is stored in our BearingPoint CRM system and processed to get in contact with you via phone or e-mail to establish a business relationship or to inform you about our events, products or services. BearingPoint processes your information in accordance with regulations on data protection and electronic communications as currently adopted. BearingPoint processes your information based on the legitimate interest. Please be informed that BearingPoint is a commercial enterprise and only addresses other commercial enterprises with regard to its products and services.

Licensed data is only processed according to the license agreements in place with the vendors. The vendors are typically acting as independent data controllers and are subject to the privacy regulations once they collect your information. BearingPoint is mainly licensing data from Cognism Platform (<https://www.cognism.com/en/privacy-policy>) and LinkedIn Sales Navigator (<https://www.linkedin.com/legal/privacy-policy>).

You have the right to ask BearingPoint for access, correction, or deletion of the data we process related to your person. You also have the right to object to processing. Please see sections 8 and 12 of this website privacy statement for more information related to your rights and contact details.

1.3 BearingPoint also uses Microsoft Bookings. Microsoft Bookings is a Microsoft 365 app supporting the scheduling and the managing of appointments; it includes a web-based booking calendar. The legal basis is the legitimate interest (Art. 6 (1) lit. f GDPR; we want to give you the opportunity to easily schedule an appointment with us.

The personal data required for an appointment via Microsoft Bookings (name and email address) as well as your additional, voluntary information (address, telephone number, notes) are processed and stored by us only to the extent that this is necessary for the processing of the appointment, but no longer than 120 days.

BearingPoint conducts online surveys. The aim of the surveys is to improve our services. Participation in surveys is voluntary and anonymous unless otherwise described in the survey. All mandatory fields in surveys are marked with an *. If you would like to participate anonymously in the survey, we ask you not to enter any personal data (e.g. name, e-mail address) in free text fields. In some surveys there is the possibility to voluntarily enter personal data (e.g. name/pseudonym, business e-mail address, business phone number) so that we can contact you or to obtain more detailed survey data. If you provide us with your personal data, it will only be processed for survey purposes. By submitting the survey, you give us your consent to process the data you have provided (Art. 6 para. 1 lit. a GDPR). To ensure secure participation in the survey, data transmission is exclusively encrypted. In the process log data is collected (e.g. to prevent misuse of the survey forms). The log data collected will not be analysed or merged with other survey data. Survey data is deleted after finishing the survey and the internal evaluation of the results.

To prepare, conduct and evaluate the surveys we use Microsoft Forms.

We selected the Microsoft data centers in Europe for data storage. Since Microsoft Bookings and Microsoft Forms are Microsoft 365 services, Microsoft (One Microsoft Way, Redmond, WA 98052-6399, USA) also might receive access to the data you provide in the form. A Data Processing Agreement including the Standard Contractual Clauses is in place.

Further information on the handling and use of data by Microsoft can be found in Microsoft's privacy policy: <https://privacy.microsoft.com/en-us/privacystatement>.

2. Use of Personal Information

2.1 We process personal information collected via the BearingPoint sites for the purposes of:

- Providing our services
- Dealing with your enquiries and requests for Recruitment
- Proposing/inviting access to BearingPoint's social media accounts
- Proposing/inviting to informational events and conferences or to webinars
- Providing you with information about products and services
- Managing and maintaining our relationship with business contacts
- Participating in surveys, quizzes, or benchmarking surveys
- Replying to your data subject access requests

3. Information We Gather Automatically and How We Use It

3.1 When you visit one of the BearingPoint sites, we collect information automatically about those visits.

3.2 In particular, your browser automatically sends us certain Internet-related information, such as the Internet Protocol (IP) address of the computer you are using.

3.3 We also collect information through the use of cookies to better understand how visitors use the BearingPoint sites, to identify problems with our servers, prepare aggregate demographic information and other information regarding the use of the BearingPoint sites, and to improve the functions of the BearingPoint sites. Cookies do not collect any information that enables you to be identified as an individual.

3.4 BearingPoint uses "Google reCAPTCHA" (hereafter "reCAPTCHA") on its websites. Provider is Google LLC 1600 Amphitheater Parkway, Mountain View, CA 94043, USA ("Google"). With reCAPTCHA we want to check if the data entry on our websites (for example in a contact form) is done by a human or by an automated program. For this, reCAPTCHA analyzes the behavior of the site visitor based on various characteristics. This analysis begins automatically as soon as the website visitor enters the website. For analysis, reCAPTCHA evaluates various information (for example, the IP address, the time a site visitor spends on the website or mouse movements made by the user). The data collected during the analysis will be forwarded to Google. The reCAPTCHA analyzes are completely in the background. Site visitors are not advised that an analysis is taking place. Data processing takes place on the basis of Art. 6 para. 1 lit. f GDPR. BearingPoint has a legitimate interest in protecting its websites from abusive automated spying and SPAM. For more information about Google reCAPTCHA and Google's privacy policy, please visit the following links:

<https://www.google.com/intl/en/policies/privacy/> and <https://www.google.com/recaptcha/about/>.

3.5 LinkedIn

BearingPoint maintains an online presence on the LinkedIn platform operated by LinkedIn Ireland Unlimited Company, Wilton Place, Dublin 2, Ireland ("LinkedIn"), in order to communicate with LinkedIn members, promote our services, and collect leads through LinkedIn advertising tools.

For certain data processing BearingPoint and LinkedIn are joint controllers within the meaning of Art. 26 GDPR. LinkedIn's own privacy policy also applies to their collection and processing of LinkedIn member data.

[Please click here for LinkedIn's privacy policy.](#)

BearingPoint uses LinkedIn cookies on the BearingPoint website to measure the effectiveness of BearingPoint LinkedIn advertising campaigns and to retarget users who visited the BearingPoint website. These cookies collect data such as IP address, device information, browser type, and LinkedIn user ID (if logged in). The legal basis is consent.

LinkedIn uses various tracking and analytics technologies to understand user behavior, measure engagement. LinkedIn processes this data for its own legitimate business purposes, including analytics, marketing, and improvement of its platform. We do not have access to individual user data collected by LinkedIn through such technologies.

BearingPoint uses LinkedIn Lead Gen Forms for BearingPoint sponsored content, and sponsored LinkedIn InMails for recruitment and marketing campaigns. Once LinkedIn members click on BearingPoint advertisement, they will see a form that is pre-filled with information from their LinkedIn profile, such as their name, contact information, company name, seniority, job title and location. As soon as a LinkedIn member submits a lead form, BearingPoint receives the data to follow up with them.

3.6 When you visit or use our social media websites such as Facebook, we use Facebook Pixel, which allows us to display interest-based advertisements ("Facebook Ads") to users of the website when they visit the social network or other websites also using this tool. In this way, we pursue the interest in displaying advertisements that are of interest to you in order to make our website or offers more interesting for you. With the help of the Facebook Pixel, we can also track the effectiveness of Facebook ads for statistical and market research purposes by seeing whether users were redirected to our website after clicking on a Facebook ad ("conversion").

The processing of this data by Facebook takes place within the framework of Facebook's data policy: <https://www.facebook.com/policy.php>.

Special information and details about the Facebook pixel, the Conversions API and its functionality can also be found in the Facebook help area: <https://www.facebook.com/business/help/742478679120153?id=1205376682832142>.

We also use lead ads on Facebook, e.g. for recruiting purposes and promoting recruiting events. If you, as a platform user, click on an add, you will be prompted to fill out a lead ad forms. After submitting it, your leads data will be stored on Facebook's servers for no more than 90 days, and we may download your leads data from it. The downloaded data will be further stored in our recruitment system for no longer than 6 months. Facebook will use the information submitted by users through the lead ad, subject to its data policy: <https://www.facebook.com/policy>. Further details about how Lead ads work on Facebook can be found here: <https://www.facebook.com/business/help/1481110642181372?id=735435806665862>.

When operating with lead ads, BearingPoint together with Facebook Ireland Ltd, 4 Grand Canal Square, Grand Canal Harbour, Dublin 2, Ireland (Facebook) are Joint Controllers for the collection and transfer of data in this process. The following processes are therefore not covered by joint controllership:

- The process that takes place after the collection and transmission is within the sole responsibility of Facebook.
- The preparation of reports and analyses in aggregated and anonymized form is carried out as a Processor and is therefore within our responsibility.

We transfer the data within the scope of joint controllership based on the consent pursuant to Art. 6 (1) a GDPR. Further information on how Facebook processes personal data, including its legal basis and further information on the rights of data subjects can be found here: <https://www.facebook.com/about/privacy>.

3.7 Google Analytics 4.

BearingPoint also uses Google Analytics, a web analytics service provided by Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland, on its websites. In order to protect your data as best as possible, the version "Google Analytics 4" (GA4, anonymized tracking, cookieless tracking) and GA4 integrations are used. Thus, only anonymized aggregated data is transmitted to us, which we evaluate for web statistics and therefore want to improve our offer. No individual profiles are created, but rather user groups. A personal reference can no longer be established. The GA4 integration Google Signals collects session data from sites and apps that Google associates with users who have signed in to their Google accounts, and who have turned on Ads Personalization. This data is used to enable cross-device reporting, cross-device remarketing, and cross-device conversion export to Ads.

GA4 uses IP address anonymization by default, which cannot be deactivated. Lawful cookies have a duration of 2 months.

The legal basis for the use of GA4 and the resulting coverage measurement is the consent (Art. 6 (1) lit. a GDPR).

The collected data may be transmitted to Google in Europe, or also to Google servers in the USA. BearingPoint has no influence on the data transfer to Google. Furthermore, BearingPoint has no influence on whether Google can draw conclusions about your person.

We are reviewing relevant rulings of the European Data Protection Agencies and/or other authorities which might impact the use of Google Analytics.

Further information on the handling of user data can be found in Google's privacy policy: <https://policies.google.com/privacy?hl=en&gl=de>.

3.8. Lead Forensics

BearingPoint uses Lead Forensics, a B2B sales and marketing enablement tool. It is operated by Lead Forensics. A Data Processing Agreement including the Standard Contractual Clauses is in place with Lead Forensics Limited, 3000 Lakeside, North Harbour, Western Road, Portsmouth, PO6 3EN, UK.

The Lead Forensics tool uses a tracking code for identifying businesses visiting our websites based on their business IP addresses. This is not the same as cookies. The Lead Forensics tracking code only provides information that is readily available in the public domain. It does not, and cannot, provide personal or sensitive data regarding who has visited our website. Under no circumstances will the data be used for the personal identification of an individual visitor. If IP addresses are collected, they will be anonymised immediately after collection. The information generated by the Lead Forensics tracking code is transmitted to the Lead Forensics tool and processed and stored in the UK within a secure environment.

The Lead Forensics tool does not provide us with the IP addresses. It provides us information on what companies have visited our website, the date and duration of their visit, and the web pages that they visit. This information allow us to analyse the use of our website and eventually contact those companies about their experience or for sales purposes.

More information can be found at <https://www.leadforensics.com/privacy-policy/>

3.9 CleanTalk anti-spam check

We use the "CleanTalk" service, which protects the Site from spam when a data entry on a Site is done (for example in a contact form). The legal basis is the legitimate interest (Art. 6 (1) lit. f GDPR).

For security reasons and as protection against spam, your data is processed in the CleanTalk Cloud Service and stored in log files for a maximum of 45 days. After expiry of the aforementioned period, this data will be completely deleted. CleanTalk may use information about spam activity from IP or email addresses to provide appropriate anti-spam protection to all websites connected to its service.

Further information on the handling and use of data by CleanTalk can be found in CleanTalk Inc's privacy policy: <https://cleantalk.org/publicoffer#privacy>.

3.10 Akismet

BearingPoint also uses the "Akismet" service which protects the site from spam when a data entry in a contact form is done by you. Provider of the Akismet service is Automattic Inc, 60 29th St, #343 San Francisco, CA 94110, United States.

The legal basis is the legitimate interest (Art. 6 (1) lit. f GDPR).

Automattic is processing your data in the USA; it is an active participant of the EU-US Data Privacy Framework, the Swiss-US Data Privacy Framework and the UK Extension to the EU-US Data Privacy Framework. Automattic may use your user IP, user agent, referrer, Site URL (along with other information directly provided by you in the contact forms such as your name, company address, job title, function and the comment itself). Automattic has retention periods between two weeks and ninety days for the vast majority of spamrelated data, at which point it is automatically deleted from Akismet's databases. A Data Processing Agreement including the Standard Contractual Clauses is in place.

Further information on the handling and use of data by using Akismet can be found in the Automattic privacy policy: <https://automattic.com/privacy/>

4. Cookie list

4.1 A cookie is a small piece of data (text file) that a website – when visited by a user – asks your browser to store on your device in order to remember information about you, such as your language preference or login information. Those cookies are set by us and called first-party cookies. We also use third-party cookies – which are cookies from a domain different than the domain of the website you are visiting – for our advertising and marketing efforts. More specifically, we use cookies and other tracking technologies for the following purposes:

Cookie list will automatically generated here and will replace this placeholder text

4.2 Microsoft Dynamics 365

We use cookies or tracking pixels from Microsoft Dynamics 365, which is provided by Microsoft Ireland Operations Limited, Ireland. Microsoft Dynamics uses the following cookies:

- **Long-term behavioral-analysis cookie:** This cookie is set and/or read on any webpage where we have placed a Dynamics 365 Marketing website behavioral-analysis script. It enables Dynamics 365 Marketing to score leads based on their level of interaction with a given website. The cookie contains no personal information but does uniquely identify a specific browser on a specific machine, and Dynamics 365 Marketing can use it to correlate this ID with an actual contact in our Dynamics 365 CRM. The cookie remains active for two years.
- **Short-term, single-visit cookie:** This cookie is also set and/or read on any webpage where we have placed a Dynamics 365 Marketing website behavioral-analysis script. By default, it expires after just 30 minutes. Dynamics 365 Marketing uses it to group all page loads by a given user that are recorded by the same behavioral-analysis script and that occur within the configured timeframe. It will consider all of these as part of a single "visit" to the website.

4.3 We use Microsoft Clarity and Microsoft Advertising services provided by Microsoft Ireland Operations Ltd, One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, Ireland to better understand the needs of our users and to optimise the offer on this website. The Clarity technology gives us a better understanding of our users' experiences (e.g. how much time users spend on which pages, which links they click on, what they like and dislike, etc.). This helps us to tailor our offering to our users' feedback. Clarity works with cookies and other technologies to collect information about the behaviour of our users and their devices (in particular IP address of the device (only stored in anonymised form), screen size, device type (unique device identifiers), information about the browser used, location (country only), preferred language for displaying our website). Microsoft Advertising is used to measure the effectiveness of our advertisements and to display relevant ads to users. For this purpose, the Microsoft Advertising Universal Event Tracking (UET) tag may be used on our website. This technology allows Microsoft to collect and process information about how users interact with our website after clicking on an advertisement, including visited pages, conversion actions, and interaction

data. This information may be used for remarketing purposes. The information collected through these services may be stored in pseudonymised user profiles. Neither we nor Microsoft use this information to directly identify individual users. The legal basis for data processing is your consent in accordance with Art. 6 (1) lit. a GDPR. Microsoft Corporation is committed to complying with the data processing principles of the Data Privacy Framework (DPF). On this basis, data transfer to the USA, which cannot be excluded, is possible. If you have any questions about data protection at Microsoft, you can contact them at <https://www.microsoft.com/en-us/concern/privacy>. You can find the Microsoft privacy policy at <https://privacy.microsoft.com/en-us/privacystatement>.

4.4 Furthermore, when browsing the BearingPoint website you may get access to embedded media and other external sources which may store cookies. As cookies from externally embedded media may be used or modified without BearingPoint's knowledge or consent, you are invited to consult the following links for further information.

Media	Link to their privacy statement
Twitter	https://twitter.com/en/privacy
YouTube	https://policies.google.com/privacy
LinkedIn	https://www.linkedin.com/legal/privacy-policy
Facebook	https://www.facebook.com/policy.php
Xing	https://privacy.xing.com/en/privacy-policy
Instagram	https://privacycenter.instagram.com/policy

4.5 You have the right to choose whether or not to accept cookies. You can exercise this right by amending or setting the controls on your browser to reflect your cookie preferences. However, please note that if you choose to refuse cookies you may not be able to use the full functionality of the BearingPoint sites.

4.6 The "help" portion of the toolbar on most Internet browsers will tell you how to change your browser cookie settings, including how to have the browser notify you when you receive a new cookie, and how to disable cookies altogether. For further information about cookies and how to control their use, please visit the following third-party educational resources: <https://www.allaboutcookies.org/> and <https://www.youronlinechoices.eu/>.

5. Information We Share

5.1 We will only disclose personal information to other companies within our group of companies, business partners, government bodies and law enforcement agencies, successors in title to our business and suppliers we engage to process data on our behalf. In these circumstances we will share your personal information for purposes such as our legitimate business purposes and to comply with legal obligations.

As legal bases we rely on contractual obligation, legitimate interest or your consent.

6. Links to Other Sites

6.1 This Privacy Statement applies only to information collected by a BearingPoint site.

6.2 BearingPoint sites contain links to other sites that are not owned or administered by BearingPoint. Please be aware that BearingPoint is not responsible for the privacy practices of such other third party sites. We encourage you to read the privacy statements of every Website you visit.

7. Security

7.1 We maintain safeguards to protect against unauthorized disclosure, use, alteration, or destruction of the personal information you provide to us through the BearingPoint sites. Please note, however, that perfect security does not exist on the Internet. Therefore, while we endeavor to protect your personal data, when data is transferred over the Internet it may potentially be accessed and used by unauthorized parties.

8. Your Privacy Rights

All personal data BearingPoint as a controller stores or processes should be accurate and up to date. You may have certain rights related to your personal data, depending on your location and the applicable data protection laws. Subject to any applicable exceptions or limitations, these rights may include:

- The right to access your personal data;
- The right to have your personal data deleted;
- The right to have your personal information rectified, corrected, or updated;
- The right to know what personal information of yours is collected and for what purpose;
- The right to object to the processing of your personal data;
- The right to restrict processing of your personal data;
- The right to withdraw consent you provided for storage and processing of your personal data (to the extent processing is based on your consent).

Data subject rights requests can be made to BearingPoint by completing a short questionnaire through Microsoft Form (a service provided by our data processor Microsoft Ireland Operations Ltd.) available via the following link: <https://forms.cloud.microsoft/e/9JggvbKEfX>

If you prefer not to use the online form, you can also file a paper request which should be mailed to:

BearingPoint Data Protection Department
Group Compliance Officer
BearingPoint Berlin
Invalidenstraße 73
10557 Berlin
Fax: +49 30- 880041040

To ensure the security and confidentiality of personal data, providing identity verification information may be required to process any data subject request.

The data provided when completing the Data Subject Request Form is retained in accordance with applicable statutory retention periods and as long as it is necessary to fulfil the purpose for which it was provided.

9. Hosting

Design and maintenance of our websites by RYZE Digital GmbH, Mombacher Str. 4, 55122 Mainz, Germany. The webserver is hosted by aiticon GmbH Stephanstraße 1, 60313 Frankfurt, Germany.

10. Internet-based Transfers

10.1 Given that the Internet is a global environment, using the Internet to collect and process personal data necessarily involves the transmission of data on an international basis. Therefore, by browsing the BearingPoint sites and communicating electronically with us, you acknowledge our processing of personal data in this way. However, we will endeavor to protect all personal information collected through the BearingPoint sites in accordance with strict data protection standards.

11. Changes to the Privacy Statement

We reserve the right to amend this Statement at any time without advance notice in order to address future developments of **BearingPoint**, the Website or changes in industry or legal trends. We will post the revised Statement on the Website or announce the change on the home page of the Website. You can determine when the Statement was revised by referring to the "Last Updated" date on the top of this Statement. Any changes will become effective upon the posting of the revised Statement on the Website. By continuing to use the Website following such changes, you will be deemed to have agreed to such changes. If you do not agree with the terms of this Statement, in whole or part, you can choose to not continue to use the Website.

12. Data protection information for data subjects in California (CCPA/CPRA)

California Consumer Privacy Act (CCPA)

Notice at Collection

This California Consumer Privacy Act Notice at Collection is addressed to California residents only, and is provided by BearingPoint Holding BV and its associated companies (all together "BearingPoint; "we", "us").

This Notice explains what personal information we collect, how we use, share, disclose, and retain it, as well as the rights of California residents and how they can exercise those rights.

The CCPA Notice at Collection only applies to California residents.

Categories of Personal Information Collected

We collect personal information as defined under the CCPA, **Cal. Civ. Code § 1798.140(v)**, which includes information that identifies, relates to, describes, or could reasonably be linked with a particular consumer or household.

In the past 12 months, we may have collected the following categories:

Category	Examples
Identifiers	Full name, Social Media URL, Address, Email Address, business phone number, and IP Address

Personal Information	Address, Telephone Number, and Notes
Internet or Network Activity	IP Address, Interactions with our website, advertisements, and applications,
Professional or Employment-related Information	Job Title, Job Function, Company Name, Business Contact Details, Office Address, Business Phone Number, Employment Application, and Business Email Address.

Use of Personal Information

We use personal information for business or commercial purposes such as:

- Providing our services
- Dealing with your enquiries and requests for Recruitment
- Proposing/inviting access to BearingPoint's social media accounts
- Proposing/inviting to informational events and conferences or to webinars
- Providing you with information about products and services
- Managing and maintaining our relationship with business contacts
- Participating in surveys, quizzes, or benchmarking surveys
- Replying to your data subject access requests
- To better understand how visitors use BearingPoint sites
- To improve the functions of the BearingPoint sites
- To identify problems with our servers
- To prepare aggregate demographic information and information regarding the use of the BearingPoint sites

Sources of Personal Information

We collect personal information from the following sources:

- Directly from consumers (e.g., registration forms, inquiries, requests, email replies, surveys, quizzes, events)
- Automatically from interactions with our websites or services
- Through the use of cookies
- Third-party data B2B platforms
- Third-party data providers or public sources

Sharing of Personal Information

We will only disclose personal information to:

- Companies within our group of companies
- Business Partners
- Government Bodies

- Law Enforcement Agencies
- Successors in title to our business
- Suppliers we engage to process data on our behalf

We do not sell personal information as defined under **Cal. Civ. Code §§ 1798,140(ad) and (ah)**.

Your Rights Under The CCPA

Under the California Consumer Privacy Act, California residents have the following rights:

Your Right	What You Can Request From Us
Right To Know	Categories and specific data we collected Sources of data Our business purposes for the collection and use of data Categories of third parties we have disclosed data
Right to Delete	Deletion of your personal data (unless retention is necessary)
Right to Correct	You can request that we correct inaccurate personal information we maintain
Right To Opt-Out	You can request to opt out of the sale or sharing of your personal information
Right To Limit	You may restrict the use of your sensitive personal information to only necessary business purposes

We will not discriminate against you for exercising your rights.

How To Exercise Your Rights

You or your authorized agent may submit a verifiable request to privacy@bearingpoint.com

Data Retention

- We use a customer relation management system (the BearingPoint CRM) to store personal information about business contacts.
- We store personal data required for an appointment via Microsoft Bookings only to the extent that is necessary for the processing of the appointment. We store this data for no longer than 120 days.
- Downloaded data regarding recruitment and promoting recruiting events will be stored in our recruitment system for no longer than 6 months.

We retain data only as long as reasonably necessary for business/legal purposes, and we implement reasonable administrative, technical, and physical safeguards to protect consumer data.

Do Not Track notice

Some browsers offer the option of sending a "Do Not Track" signal, which indicates that you do not wish to be tracked across different websites. Our website does not currently respond to such signals as there is no uniform standard for implementation.

BearingPoint Privacy Policy

Link to BearingPoint's Privacy Policy

Privacy Policy: <https://www.bearingpoint.com/en-us/privacy-statement/>

13. Contact Us

If you have any general questions or concerns about how we process personal information please contact us at privacy@bearingpoint.com.

People's Republic of China

These terms are additional to the present privacy notice, as required by the China Personal Information Protection Law.

These terms should apply to the processing of the personal information of natural persons within the territory of the People's Republic of China.

These terms shall also apply to the activities carried out outside the territory of the People's Republic of China to process the personal information of natural persons within the territory of the People's Republic of China under any of the following circumstances:

- (I) where the purpose is to provide products or services to domestic natural persons;
- (II) where the purpose is to analyze and evaluate the activities of domestic natural persons; and
- (III) other circumstances provided by laws and administrative regulations.

Personal information refers to various kinds of information related to identified or identifiable natural persons recorded by electronic or other means, excluding the information processed anonymously.

Processing of personal information includes the collection, storage, use, processing, transmission, provision, publication, and erasure of personal information.

Processing personal information shall be for a definite and reasonable purpose, shall be directly related to the purpose of processing, and shall be processed in a manner that has the least impact on individual rights and interests.

Collection of personal information shall be limited to the minimum scope for the purpose of processing and excessive collection of personal information shall not be allowed.

Sensitive personal information refers to the personal information that can easily lead to the infringement of the personal dignity or natural persons or the harm of personal or property safety once leaked or illegally used, including such information as biometrics, religious belief, specific identities, medical health, financial accounts, and whereabouts, and the personal information of minors under the age of 14.

Personal information processors can process sensitive personal information only when they have a specific purpose and sufficient necessity and take strict protective measures.

Cross-Border data transfer

Where a personal information processor needs to provide personal information outside the territory of the People's Republic of China due to business or other needs, it shall meet any of the following conditions:

(I) where it has passed the security assessment organized by the State cyberspace administration;

(II) where it has been certified by a specialized in accordance with the provisions of the State cyberspace administration in respect of the protection of personal information;

(III) where it has concluded a contract with an overseas recipient according to the standard contract formulated by the State cyberspace administration, specifying the rights and obligations of both parties;

or

(IV) where it has satisfied other conditions prescribed by laws, administrative regulations, or the State cyberspace administration.

Data Subject Rights

- the right to know and make decisions on the processing of your personal information;
- the right to restrict or refuse others to process your personal information, unless otherwise provided for by laws and administrative regulations.
- The right to consult or copy your personal information from a personal information processor, except for the circumstances as prescribed in Paragraph 1 of Article 18 and Article 35.
- The right to withdraw consent;
- The right to request to make corrections or supplements.
- The right to request deletion:

(I) where the purpose of processing has been achieved, unable to achieve, or is no longer necessary to achieve;

(II) where the personal information processor stops providing products or services, or the agreed storage period has expired;

(III) where the individual withdraws his/her consent;

(IV) where the personal information processor processes personal information in violation of laws, administrative regulations, or the agreement; or

(V) any other circumstance as prescribed by laws and administrative regulations.

Where the storage period as prescribed by laws and administrative regulations does not expire, or the deletion of personal information is difficult to be realized technically, the personal information processor shall stop processing personal information other than storage and taking necessary security measures.

Data Sharing

In addition to the data sharing activities as described in the main notice, we may also share your personal information with other independent personal information handlers. We will notify you of the data to be shared, its processing purpose and means as well as other items as required by applicable data protection laws and will obtain your separate consent where this is required.

Contacting Us

Personal Information Handler: the company (or companies) of the BearingPoint Group (including BearingPoint (Shanghai,) Enterprise Management Consulting Co. Ltd.) is responsible for the processing of your personal information as described here and in the main notice.

China Contact Details:

BearingPoint (Shanghai) Enterprise Management Consulting Co. Ltd. 55/F, Wheelock Square
1717 Nanjing West Road
CN-200000 Jing'an District, Shanghai, China

Phone: +86 21 6288 7866

marketing.cn@bearingpoint.com

BearingPoint Hong Kong Limited

Office 4 10/F, Kwan Chart Tower, No.6 Tonnochy Road

HKG Wanchai, Hong Kong, China

Phone: +852 5621 4776

Fax: +852 3753 0021

marketing.cn@bearingpoint.com

Foreign Data Recipient Contact Details

BearingPoint Holding B.V.

De Entree 89 NL-1101 BH Amsterdam

Phone: +31 20 504 90 00

compliance@bearingpoint.com