

Privacy Notice for Job Applicants (m/f/d) pursuant to Articles 13 and 14 GDPR

Thank you for your interest in our company! At aigner business solutions GmbH, protecting your privacy is an important concern that we take very seriously. We would therefore like to explain which data we store and use, when we do so, and for what purposes.

Controller responsible for data processing pursuant to Article 4(7) GDPR

aigner business solutions GmbH

Rainer Aigner, Tobias Damasko

Goldener Steig 42

94116 Hutthurm

Germany

Tel.: +49 8505 91927-0

Email: info@aigner-business-solutions.com

Data Protection Officer

We have appointed a Data Protection Officer who acts on behalf of aigner business solutions GmbH pursuant to Articles 37 et seq. GDPR:

Ramona Höfler

aigner business solutions GmbH

Email: dsb@aigner-business-solutions.com

Scope

This privacy notice explains the nature, scope and purposes of the collection and use of personal data by the controller during the recruitment process, pursuant to Articles 13 and 14 GDPR.

Personal data

Personal data means information relating to an identified or identifiable natural person (data subject).

We generally collect information directly from the data subject. We receive personal data through the documents you provide during the recruitment process, telephone calls, and online and in-person interviews.

In particular, we process the following information about you to identify the most suitable candidates for vacant positions:

- **Basic personal details:** First name, surname, date of birth, place of birth, nationality, any photograph provided, and other information contained in your CV and cover letter, such as details of parents or legal guardians.
- **Contact details:** Address, telephone number, mobile phone number and email address.
- **Qualifications:** Educational certificates, employment references, diplomas, certificates, references and, where applicable, a copy of your certificate of conduct.
- **Additional information from the contact form:** A free-text field for individual details.
- **Where applicable, special categories of personal data pursuant to Article 9 GDPR:** Information concerning religious affiliation, trade union membership, health and severe disability.

The processing of these special categories of data serves solely to use your application documents to fill vacant positions. aigner business solutions GmbH will not take this information into account in its decisions unless legally required to do so. This means that we process these special categories of personal data pursuant to Article 9 GDPR only where required by law. If you do not wish this data to be processed, you are free to submit new application documents with this information removed. Doing so will not affect your prospects of success.

Obligation to provide data

You are under no statutory or contractual obligation to provide us with your data. However, providing your information is necessary for us to consider you for a vacant position.

You are under no obligation to consent to a longer retention period. Without this consent, however, we cannot consider your data beyond the recruitment process for a specific position.

Purposes and legal bases of data processing

The processing of your data during the recruitment process serves to fill a vacant position within our company.

Application for a specific advertised position

We publish vacancies within our company on our website and elsewhere. If you are interested in a vacancy, you can apply for that specific position. Your application data will then be used solely for the recruitment process and processed pursuant to Section 26 of the German Federal Data Protection Act (BDSG), in conjunction with Article 88 GDPR. If your application is unsuccessful, your data will be deleted within four months of the end of the recruitment process.

Unsolicited applications

You may submit an unsolicited application to our company without reference to a specific advertised position. These applications are also reviewed by our company and go through the recruitment process. Your application data will be used solely for the recruitment process and processed pursuant to Section 26 BDSG, in conjunction with Article 88 GDPR.

For unsolicited applications, we offer you the option of having your application data retained by us for a period of six months.

Talent pool

Regardless of whether you have applied for a specific position or submitted an unsolicited application, we offer you the option of joining our talent pool if you are interested. This enables us to match your documents against other positions, including potential future vacancies within our company. The legal basis for this processing is your declaration of consent pursuant to Article 6(1)(a) GDPR.

Based on your consent pursuant to Article 6(1)(a) GDPR, we retain your application for a longer period, up to a maximum of one year, so that you can be considered for vacancies within the company.

Matching your application against other vacancies

We also process your data pursuant to Article 6(1)(f) GDPR where this is necessary for our legitimate interests and your rights do not override those interests. Such a legitimate interest may, for example, justify considering your application for similar or comparable vacancies within our company.

Review of profiles on professional networks (LinkedIn / XING)

As part of the recruitment process, we process publicly available information from professional social networks, such as LinkedIn or XING, if you maintain a profile on these platforms. We review this information to verify your professional qualifications, career history and other information relevant to filling the position, and to supplement the overall picture provided by your application. Processing is based on Article 6(1)(b) GDPR, in conjunction with Section 26(1) BDSG, insofar as the processing is necessary to decide whether to establish an employment relationship.

Where, in an individual case, there is no direct connection with the decision to establish an employment relationship, processing is based on Article 6(1)(f) GDPR (legitimate interests). Our legitimate interest lies in conducting the recruitment process efficiently and appropriately.

Job interviews via Microsoft Teams

In individual cases, job interviews may be conducted using the Microsoft Teams video conferencing service, particularly where attending in person is not possible or would involve considerable effort due to geographical distance. The interview serves to assess your professional qualifications, personal suitability and other aspects relevant to filling the advertised position. The processing of your personal data during such a video interview is based on Article 6(1)(f) GDPR. Our legitimate interest lies in conducting the recruitment process efficiently and promptly.

Verification of applicants' identity using an identity card

At the beginning of the interview, we carry out an identity check for both in-person interviews and interviews conducted via Microsoft Teams. For this purpose, we ask you to present your identity card or briefly show it during the video interview. We do not make a copy or scan of your identity card. The check is conducted solely by visual inspection. Internally, we only document that an identity check has been carried out, recording the name, date and signature of the person performing the check.

The identity check is based on our legitimate interest pursuant to Article 6(1)(f) GDPR. Our legitimate interest is to ensure that the interview is being conducted with the person who applied for the position concerned.

Video surveillance by the landlord

When attending an in-person interview at our premises, you may enter areas of the building that are subject to video surveillance, such as entrance areas or publicly accessible areas. The video surveillance is not carried out by our company, but by the building's landlord, who is the controller for this processing within the meaning of the GDPR. In particular, the purposes of the video surveillance are to exercise the right to control access to and use of the premises, protect people and property, and prevent and investigate criminal offences.

Disclosure of data by our company

Only those departments and employees who require access to your data to fulfil the purposes stated above will receive access. These are generally the managers of the department in which the vacancy is to be filled.

Our company may disclose data to comply with legal obligations pursuant to Article 6(1)(c) GDPR, for example to public authorities or the police. Personal data may also be disclosed on the basis of our legitimate interests pursuant to Article 6(1)(f) GDPR, for example to lawyers in connection with legal disputes.

Apart from this, we do not receive your information from any other sources and generally do not disclose it to others. Should any other disclosure of your information become necessary, you will be informed in advance.

Deletion of your personal data

If your application is unsuccessful, your data will be deleted within four months of the end of the recruitment process. If you are employed by aigner business solutions GmbH, all your documents will be transferred to your employment records and retained for the duration of the employment relationship.

Transfer of personal data to a third country

As a general rule, personal data is not transferred to a third country. If such a transfer nevertheless takes place, it is governed by an adequacy decision, for example for Canada, consent, Binding Corporate Rules or agreed EU Standard Contractual Clauses. An exception applies to the transfer of data to LinkedIn.de if you choose to apply by submitting your application documents stored on LinkedIn.de.

Your rights as a data subject

Right of access

Pursuant to Article 15 GDPR, you have the right to obtain confirmation from the controller as to whether personal data concerning you is being processed.

For this purpose, aigner business solutions GmbH provides an overview of the purposes of processing, the categories of personal data processed, the respective recipients or categories of recipients, and a copy of the stored data.

Rights to rectification, erasure and restriction of processing

Pursuant to Article 16 GDPR, you have the right to request the rectification of inaccurate personal data concerning you without undue delay. Taking into account the purposes of processing, you also have the right to have incomplete personal data completed.

Pursuant to Article 17 GDPR, you have the right to request that aigner business solutions GmbH erase personal data concerning you without undue delay, provided that no other legal requirement prevents its erasure.

Pursuant to Article 18 GDPR, you have the right to request restriction of processing where:

- You contest the accuracy of your personal data.
- The processing is unlawful and the data subject opposes the erasure of the personal data and requests restriction of its use instead.
- The controller no longer needs the personal data for the purposes of processing, but the data subject requires it for the establishment, exercise or defence of legal claims.
- You object to processing pursuant to Article 21 GDPR.

Right to withdraw consent

You have the right to withdraw your consent at any time, in whole or in part, with effect for the future. Withdrawal of consent does not affect the lawfulness of processing based on consent before its withdrawal. However, if you withdraw your consent, your application may no longer be considered at all or may no longer be considered to the same extent. No further placement activities will take place after you withdraw your consent. Statutory retention obligations may nevertheless require us to continue storing your data.

Right to object

You have the right to object at any time to the processing of your personal data based on Article 6(1)(e) or Article 6(1)(f) GDPR. aigner business solutions GmbH will then cease processing the personal data unless it can demonstrate compelling legitimate grounds that override the interests, rights and freedoms of the data subject.

Right to lodge a complaint

You have the right to lodge a complaint with the competent supervisory authority if you believe that the processing of personal data concerning you infringes statutory provisions. The supervisory authority responsible for aigner business solutions GmbH is the Bavarian State Office for Data Protection Supervision (Bayerisches Landesamt für Datenschutzaufsicht).

Updates to this privacy notice

Ongoing developments require us to adapt our data protection principles from time to time. We reserve the right to make corresponding changes at any time.