Data Protection Information under Art. 13 and Art. 14 GDPR

IMS Nanofabrication GmbH

Protecting your personal data is important to us. We strictly comply with the provisions of the EU General Data Protection Regulation (GDPR), the Austrian Data Protection Act, and all other applicable laws and regulations governing the protection, lawful processing, and confidentiality of personal data.

The following information explains how we process your personal data. If you have any questions, please contact us using the contact details provided.

1. Controller and data protection officer

Name and address of the entity responsible for processing personal data

Controller:
IMS Nanofabrication GmbH
Wolfholzgasse 20–24
2345 Brunn am Gebirge, Austria

External data protection officer:
Markus Dittrich | CASC – full service agentur GmbH
Address: Heigerleinstrasse 2/4–9, 1160 Vienna, Austria
https://www.casc.at
Tel. +43 1 924 05 28
Email: datenschutzbeauftragter@casc.at

2. Purposes and legal bases for processing personal data in connection with your use of our website

2.1 Logging of website activity (log files)

When you visit our website, we collect and store access data in log files (also known as access logs) to ensure the continued operation and functionality of our website. In this context, we process the following data:

- IP address
- Date and time of access
- Websites that directed you to our page (referrer URL)
- Operating system
- Internet service provider
- Browser name and version
- Amount of data transferred and page load time

We process these personal data on the basis of our legitimate interests pursuant to Art. 6(1)(f) GDPR. Our legitimate interests lie in ensuring the functionality, security, and availability of the

website for all visitors and, where applicable, in establishing, exercising, or defending legal claims.

You have the right to object to this processing of your data (the data subject's right to object to processing based on legitimate interests pursuant to Art. 21(1) GDPR). In that case, we will only continue to process your data if there are compelling legitimate grounds on our part for doing so.

These data cannot be attributed to you or otherwise used to identify you. They are automatically deleted once they are no longer necessary for the purposes specified above.

Data disclosures: As a rule, we only disclose data collected through your use of our website to the extent strictly necessary for the purposes described above (e.g. for the operation and maintenance of the website by external service providers). However, we may be required by law or by a public authority to disclose data to third parties (e.g. to law enforcement authorities).

Retention period: The retention period for log file data is 7 days from the end of your visit to our website.

2.2 Contact form

The contact form on our website provides you with an easy way to get in touch with us. When using the contact form, you will be asked to provide certain information so that we can process and respond to your inquiry.

We process the personal data you share solely for the purpose of responding to your inquiry and contacting you in connection with it. We use these personal data on the basis of our legitimate interests pursuant to Art. 6(1)(f) GDPR. Our legitimate interests lie in providing and using easily accessible electronic means of contact and communication and in maintaining a record of our communications. Where applicable, processing is also based on Art. 6(1)(b) GDPR where it is necessary for the performance of a contract. You have the right to object to this processing of your data (the data subject's right to object to processing based on legitimate interests pursuant to Art. 21(1) GDPR). In that case, we will only process your data if there are compelling legitimate grounds on our part for doing so.

Instead of using the contact form, you can also contact us by email, phone, or mail using the contact details provided.

Data disclosures: We disclose your personal data to third parties only to the extent necessary to communicate with you.

Retention period: Personal data you share via the online contact form are retained for 3 years from the end of the calendar year in which the communication took place.

2.3 Digital business partner onboarding

We work exclusively with suppliers that are not subject to sanctions. This ensures compliance with applicable legal and regulatory requirements.

Supplier master data is collected and created through our online self-registration process. Upon initial contact, you will receive an email containing a two-factor authentication code and a link to our online onboarding form.

You will be required to share your company information and personal data:

Data categories	Details
Company data	Registered company name
	Official website
	Company email
	Incoterm 2020
	Business registration number and commercial register number (company/commercial register no.)
	Extract from the business register (company register / commercial register)
	DUNS number
	Applicable NACE code(s)
	Value Added Tax Identification Number (VAT ID)
Address	Type of address
	Street address
	Address line 2
	Country
	Postcode
	City
	Region/Province
Bank details	Bank name
	Bank address
	Country
	Account number
	IBAN
	SWIFT code
	Bank code
	Preferred currency
Point of contact details	Name
	Function
	Department
	Email
	Telephone
Documents	Certifications, etc.

After submitting the form, you will receive a confirmation email, and your information will be processed in our business partner application. For compliance purposes, we disclose your personal data to Dow Jones and Ripjar to screen your information against applicable sanctions lists. Following a successful review, your data will be processed in our ERP system, Sage.

In certain cases, we may conduct credit assessments through a specialized service provider.

The legal bases for this processing are Art. 6(1)(b) GDPR, where processing is necessary in connection with pre-contractual measures, the performance of a contract, or the fulfilment of post-contractual obligations; Art. 6(1)(c) GDPR, where processing is necessary for compliance with legal obligations, in particular anti-money laundering (AML) requirements, sanctions requirements, and statutory retention obligations; and Art. 6(1)(f) GDPR, based on our legitimate interests in ensuring the proper conduct of our business and assessing and

mitigating risks. Where applicable, our legitimate interests also include establishing, exercising, or defending legal claims and, in the case of credit checks, protecting our property and assets. You have the right to object to this processing of your data (the data subject's right to object to processing based on legitimate interests pursuant to Art. 21(1) GDPR). In that case, we will only process your data if there are compelling legitimate grounds on our part for doing so.

Source from which data originated pursuant to Art. 14 GDPR: We process the personal data you share with us. Beyond that, we receive data relating to you from the results of credit checks and compliance reviews performed by external service providers: Factiva Limited, The News Building, 7th floor, 1 London Bridge Street, London, UK, SE1 9GF ("Dow Jones") and Ripjar Ltd, Suite 404, Eagle Tower, Montpellier Drive, Cheltenham, Gloucestershire, UK, GL50 1TA ("Ripjar").

Data disclosures: We share the personal data collected with third parties where this is necessary for the performance of the contractual relationship. For compliance screening purposes, your data will be transferred to Factiva Limited, United Kingdom ("Dow Jones"), and Ripjar Ltd, United Kingdom ("Ripjar"), which act as joint controllers with IMS (Art. 26 GDPR). An adequacy decision has been adopted by the European Commission for the United Kingdom. In addition, we have entered into standard contractual clauses (SCCs). A corresponding agreement has been concluded, the provisions of which are summarized below:

"Dow Jones" acts internally as the controller with respect to the compilation and maintenance of the risk & compliance data and Factiva information in the Dow Jones substantive database; "Ripjar" acts internally as the controller with respect to the Ripjar technology, the data processed by Ripjar, and the processing of IMS queries for the generation of query results; "IMS" acts internally as the controller for any processing of queries before they are processed using the Ripjar technology and for the query results (including any onward transfers).

Dow Jones, Ripjar, and IMS fulfil their respective obligations with respect to data subject rights as controllers under the GDPR as follows:

IMS is responsible for:

a) Transparency. Informing the data subjects to whom compliance queries and query results relate, in accordance with applicable data protection law;
b) Compliance. Determining the scope of compliance screening queries and screening results, including determining and documenting the legal basis for processing, as well as any further use or transfer of the service results after receipt;
c) Data subject rights. Handling data subject rights requests relating to the processing of compliance screening requests and screening results after they have been delivered. Requests that fall within the responsibility of Dow Jones or Ripjar will be forwarded to the relevant party;
d) Security. Ensuring the security of the processing of compliance queries before they are transmitted and of the query results after they are made available;
e) Data transfer. Compliance with the requirements for data transfers in connection with the further processing of screening results. Where risk & compliance data are transferred across borders, IMS ensures that appropriate safeguards are implemented, unless an adequacy decision by the European Commission applies.

Dow Jones is responsible for:

a) Transparency. Informing data subjects, in accordance with applicable data protection law, about how their personal data contained in the risk & compliance data and/or Factiva information forming part of the Dow Jones substantive database are processed;
b) Compliance. Ensuring compliance with the requirements applicable to the Dow Jones substantive database, including identifying and documenting the legal basis for processing the risk & compliance data and Factiva information;
c) Data subject rights. Handling data subject rights requests relating to the processing of the risk & compliance data and Factiva information in the Dow Jones substantive database, before such data are ingested into the Ripjar technology. If Dow Jones receives requests that fall within the responsibility of IMS (e.g. regarding the scope of a compliance screening request or decisions based on screening results) or Ripjar (e.g. regarding data processed by Ripjar, including Ripjar risk data, or the logic of data processing and search functions), Dow Jones will forward such requests to the relevant party.
d) Security. Ensuring appropriate security of processing within the Dow Jones substantive database;
e) Data transfer. Compliance with the requirements applicable to data transfers in connection with processing in the Dow Jones substantive database.

Ripjar is responsible for:

a) Transparency. Informing data subjects about the processing of their personal data contained in the data processed by Ripjar, in accordance with applicable data protection law;
b) Compliance. Adherence to the requirements applicable to Ripjar technology, the data processed by Ripjar, and the service results, including the determination and documentation of the respective legal bases and the processing of IMS compliance screening requests;
c) Data subject rights. Handling data subject rights requests relating to personal data processed by Ripjar using its technology and the processing of IMS compliance screening requests (including the logic applied for purposes such as risk classification or search functions). Should Ripjar receive any requests that fall within the responsibility of IMS or Dow Jones, it will forward these to the relevant party;
d) Security. Ensuring an appropriate level of security for the processing and for the handling of IMS compliance screening requests using Ripjar technology;
e) Data transfer. To the extent that IMS's access to query results constitutes an international data transfer that is not covered by an adequacy decision (a "relevant transfer"), the agreed standard contractual clauses prevail. Ripjar is responsible for ensuring compliance with the requirements applicable to data transfers in connection with Ripjar technology.

As set out in Section 7, however, data subjects may exercise their rights under the GDPR in respect of and against each controller individually, irrespective of the above.

Furthermore, we process your data in our ERP system, for which reason we also transfer your data to our processor: Sage, Stella-Klein-Löw-Weg 15, 1020 Vienna (Art. 28 GDPR). A corresponding data processing agreement has been concluded for this purpose.
In addition, we conduct credit checks through a specialized service provider and therefore disclose your personal data to that provider.

Retention period: Your data will generally only be stored for as long as necessary to fulfil the purpose for which it was collected, and beyond this period only for as long as we are subject to statutory obligations to retain or maintain such data. We are legally required to retain tax-related and accounting records and documents for seven years from the end of the calendar year to which they pertain. Data relating to rejected suppliers will be retained for 90 days from the date on which you are notified of the rejection.

2.4 Job newsletter

On our website, you can subscribe to our regular job newsletter featuring current vacancies that match the information you provide.

When you sign up, you will be asked to provide certain information on the registration form. We process your personal data to send you our job newsletter, conduct statistical analyses, and measure the effectiveness of our communications (e.g. whether the job newsletters have been opened or links contained in them have been clicked).

We use your personal data for the purposes described above on the basis of your consent pursuant to Art. 6(1)(a) GDPR. You give your consent by selecting the relevant checkbox and confirming your selection. You may withdraw your consent at any time with effect for the future. To withdraw your consent, you can use the unsubscribe link included in each job newsletter or contact us by mail or email (see the controller's contact details). The withdrawal of consent does not affect the lawfulness of any processing carried out on the basis of that consent before it was withdrawn. You are not obliged to give us your consent or provide us with your personal data for the purposes described above. However, if you do not give your consent or provide the required personal data, we will not be able to send you our job newsletter. Your personal data will be retained for as long as you subscribe to the job newsletter.

When you sign up for the job newsletter, your IP address and the date and time of registration are collected and stored. This serves to prevent misuse of the services or of the data subject's email address. The legal basis for the processing/retention of these data is our legitimate interest pursuant to Art. 6(1)(f) GDPR. You have the right to object to this processing of your data (the data subject's right to object to processing based on legitimate interests pursuant to Art. 21(1) GDPR). In that case, we will only process your data if there are compelling legitimate grounds on our part for doing so.

To protect your personal data, we use a double opt-in process when you sign up for the job newsletter online. Your subscription to the job newsletter will only be confirmed once you click the confirmation link we send to your email address.

Data disclosures: We disclose your personal data to our processor, rapidmail GmbH. We have entered into a data processing agreement with rapidmail GmbH for this purpose.

To learn more about rapidmail, go to https://www.rapidmail.at/datenschutz.

Retention period: Personal data you share via the registration form is retained for as long as your consent remains in effect.

2.5 Jobs/applications

You can find current job vacancies on our website. We process personal data that you share with us via

- email,
- LinkedIn, or
- the online form

for the purpose of managing the recruitment process, assessing your suitability for the position in question, and, where applicable, taking the necessary steps to establish an employment relationship (commencement of employment). In individual cases, we may also retain applicant data in our talent pool (where the applicant is unsuccessful or no suitable vacancy is currently available, provided that the applicant has consented to the retention of their data for this purpose). The same applies to speculative applications.

You can share the link to an advertised vacancy via LinkedIn, Facebook, X, Xing, WeChat, or by email.

As a general rule, the legal basis for this processing is Art. 6(1)(b) GDPR (performance of a contract or steps taken prior to entering into a contract). Where applicants consent to the retention of their data in our talent pool, the legal basis for this processing is Art. 6(1)(a) GDPR. After one year, we will send you an email asking whether you would like your data to remain in our talent pool or be deleted. In individual cases, we may also process personal data on the basis of our legitimate interests pursuant to Art. 6(1)(f) GDPR (e.g. for the establishment, exercise, or defense of legal claims).

We process special categories of personal data (such as health data, religious beliefs, or degree of disability) only where the applicant has consented to such processing or where processing is otherwise permitted by law (Art. 9(2)(a) and/or (b) GDPR).

Data disclosures: When you use the online form, your personal data are processed by SmartRecruiters GmbH, Wilhelmstrasse 118, 10963 Berlin, Germany. We have entered into a data processing agreement with SmartRecruiters for this purpose.

In case of job applications via LinkedIn: We have entered into a joint controllership agreement pursuant to Art. 26 GDPR with LinkedIn Inc./Microsoft, 1000 W Maude Ave, Sunnyvale, CA 94085, United States. This agreement sets out the respective responsibilities of each party with regard to the processing of personal data. LinkedIn Inc./Microsoft uses the personal data and information collected for its own purposes and may also disclose them to third parties (in the United States and other third countries).

For more information about how LinkedIn Inc./Microsoft processes personal data, please refer to the company's privacy policy: https://de.linkedin.com/legal/privacy-policy.

Please note that we cannot rule out the possibility that your personal data may be transferred to the United States. In this context, the European Commission's adequacy decision for the EU-U.S. Data Privacy Framework applies.

Retention period: Personal data provided to us are retained for 7 months after the end of the recruitment process (i.e. the hiring decision). Where you have consented to your data being retained in our talent pool, they will be retained beyond this period.

2.6 Contact via the internal whistleblowing channel

The footer on our website contains a link to our whistleblowing system, which provides a way to submit reports in accordance with the EU Whistleblower Protection Directive and applicable national law (in Austria, the Whistleblower Protection Act).

Reports may be submitted anonymously, and all cases are handled confidentially, whether or not names are provided.

We process the data and information provided solely for the purposes of reviewing incoming reports, conducting investigations, responding to inquiries, and contacting you, as provided for by the EU Whistleblower Protection Directive and applicable national law. In addition, we are subject to statutory documentation and record-keeping requirements.

The legal bases for this processing are Art. 6(1)(c) GDPR, where processing is necessary for compliance with a legal obligation, and Art. 6(1)(f) GDPR, based on our legitimate interests in carrying out internal administrative activities across affiliated business units, investigating potential compliance issues, and establishing, exercising, or defending legal claims.

You have the right to object to this processing of your data (the data subject's right to object to processing based on legitimate interests pursuant to Art. 21(1) GDPR). In that case, we will only process your data if there are compelling legitimate grounds on our part for doing so.

Data disclosures: When you use the whistleblowing channel to submit a non-anonymous report, your personal data are automatically processed by Whistleblower Software ApS, which handles the technical operation of the whistleblowing system on our behalf. We have entered into a data processing agreement with Whistleblower Software ApS for this purpose.

We also share the data with the IMS Group location in question. The IMS Group operates internationally and has locations in various countries both within and outside the European Union. The stored data may only be accessed by persons within the Group who are specifically authorized for this purpose. To the extent necessary for the purpose specified above, specifically authorized persons at our subsidiaries may also be granted access to the data, with the subsidiaries acting as joint controllers. This applies in particular where your report is investigated in the relevant country. All persons authorized to access the data are expressly required to maintain confidentiality.

For the purpose specified above, we may also need to disclose your personal data to third parties, such as law firms, law enforcement authorities, or competition authorities, within or outside the European Union.

Where we disclose your personal data within the Group or to third parties, internal data protection policies and/or appropriate contractual arrangements ensure an equivalent level of data protection. In all cases, responsibility for the processing of personal data remains with the company. Transfers of personal data to our locations in the United States, Japan, and South Korea are based on the applicable adequacy decisions. For our locations in Taiwan, we have entered into standard contractual clauses.

We have entered into a joint controllership agreement with our locations. The locations listed in the table below act as controllers within the meaning of the GDPR:

USA – California	IMS Nanofabrication LLC Mission Towers 1 3975 Freedom Circle, Suite 830, Santa Clara, CA 95054, USA 1-408-582-3103
USA – Oregon	Office Hillsboro 7235 N.E. Evergreen Parkway, Suite 800 OR 97124 Hillsboro USA
USA – Idaho	Columbus Business Park B 2141 E Summersweet Drive Boise, ID 83716 USA 1-408-582-3103
Taiwan – Tainan	No. 8, Daye 1st Road, Southern Taiwan Science Park, Xinshi Dist., Tainan City 741, Taiwan R.O.C +886 (06) 5050585
Taiwan – Hsinchu	No. 6-1, 3rd Floor, Du Sing Road, Hsinchu Science Park East District, 300 Hsinchu City Taiwan R.O.C
Taiwan – Taichung	F16, No. 847, Sec. 4, Taiwan Blvd., Xitun Dist., Taichung City Taiwan R.O.C

Korea – Dongtan	B2334, 27, Dongtan Cheomdansaneop 1-ro, Hwaseong-si 18469 Republic of Korea 경기도 화성시 동탄첨단산업1로 27, B동, 2334호 (금강펜테리움IX타워), 18469 +82 31 8015 3039
Korea – Cheongju	706 Terra Square, 288-6, Bokdae-dong, Heungdeok-gu, Cheongju-si, Chungcheongbuk-do, 28424, Korea
Japan	Level 32, Shinjuku Nomura Building 1-26-2 Nishi-Shinjuku Shinjuku-ku, Tokyo 163-0590 Japan
Austria – Brunn am Gebirge	Rennweg 83 2345 Brunn am Gebirge, Austria
Austria – Vienna	Dresdner Strasse 47 1200 Vienna, Austria +43 1 214 48 94

Contact details for the whistleblowing system at all locations:

Controller:

IMS Nanofabrication GmbH
Wolfholzgasse 20–24
2345 Brunn am Gebirge, Austria

Contact:

Maria LEPUSCHITZ
Tel.: +43 2236 37310 393
Email: maria.lepuschitz@ims.co.at

In our joint controllership agreement pursuant to Art. 26 GDPR, we have set out the following:

- As a data subject, your primary point of contact is IMS Nanofabrication GmbH. You can therefore contact IMS Nanofabrication GmbH with any inquiries relating to the joint controllership.
- IMS Nanofabrication GmbH is responsible for providing the information required under Art. 13 and 14 GDPR and for handling requests relating to data subject rights under the GDPR.
- In the case of processing activities carried out under joint controllership, IMS Nanofabrication GmbH and the locations listed above exchange personal data with each other and synchronize the data.
- All processing activities carried out under joint controllership are subject to an equivalent level of data protection and security.

Retention period: In this context, we retain personal data for 5 years from the date of the most recent processing or disclosure. Where administrative or judicial proceedings or an investigation have already been initiated, the data will be retained beyond this period for as long as necessary until those proceedings or investigations have been concluded. The personal data will be deleted thereafter.

Log data relating to processing activities are retained from the date of the most recent processing or disclosure until 3 years after the aforementioned retention obligation ceases to apply.

3. General provisions regarding data disclosure and recipients

We only disclose personal data to the extent strictly necessary for the purposes described above. Whenever we disclose personal data, we ensure that only the information strictly necessary is disclosed and that all applicable data protection requirements are met (e.g. processors are subject to strict instructions under data processing agreements pursuant to Art. 28 GDPR, obligations of secrecy and confidentiality apply, and an adequate level of protection is maintained at all times when personal data are processed).

However, in some cases, we may be required by law or by a public authority to disclose data to third parties (e.g. to law enforcement authorities or courts).

Details of data disclosures and recipients can be found in the information on the individual purposes of processing.

Data transfers within the IMS Group:

Within the IMS Group, your personal data are shared where necessary for any of the purposes set out in the privacy notice or where necessary for internal administrative activities across related divisions on the basis of our legitimate interests pursuant to Art. 6(1)(f) GDPR. Our organizational structure ensures that IMS Group companies meet the level of data protection required in the European Union.

You have the right to object to this processing of your data (the data subject's right to object to processing based on legitimate interests pursuant to Art. 21(1) GDPR). In that case, we will only process your data if there are compelling legitimate grounds on our part for doing so.

4. General provisions regarding data retention

Your personal data are retained only for as long as technically and organizationally necessary to fulfil the purposes specified above and to comply with our legal obligations. In some cases, we also retain your personal data for specific periods on the basis of our legitimate interests (e.g. for the establishment, exercise, or defense of legal claims). When determining these retention periods, we ensure that your rights and freedoms are not infringed. Once it is no longer necessary to retain your personal data, we will delete them without delay.

Detailed information on the applicable retention period can be found under the respective purpose of processing.

5. Profiling and automated decision-making

We do not engage in profiling (the evaluation of certain personal aspects relating to a natural person, in particular to analyze or predict aspects concerning work performance, economic situation, health, personal preferences, interests, reliability, behavior, location, or movements), nor do we make decisions based on such information.

6. Cookies

Please note: The following information regarding cookies applies exclusively to IMS's general corporate website (www.ims.co.at). The digital business partner onboarding form does not use cookies when accessed by business partners. Only the browser's session storage and local storage are used for strictly necessary session management within the onboarding form. This information remains on the user's device and is not shared.

We use cookies on our website. Cookies are small files that are stored either temporarily in your browser for the duration of your browsing session (session cookies) or on your device for a specified period of time (persistent cookies). Cookies enable us to recognize you when you return to our website, allowing us to provide you more quickly and effectively with content tailored to your needs and preferences.

As a rule, we use a cookie banner to obtain your explicit consent to the use of cookies (legal basis Art. 6(1)(a) GDPR). You can use the cookie banner to manage your cookie preferences. Cookies that are necessary to ensure the proper functioning of our website cannot be deselected. The legal basis for the use of these cookies is our legitimate interest in accordance with Art. 6(1)(f) GDPR.

The cookies we use:

6.1 Cookies

Strictly necessary cookies

Borlabs Cookie:

Name: Borlabs Cookie
Purpose: This cookie stores information about the user's consent preferences for service groups and individual services.
Retention period: 60 days
Technical name(s): borlabs-cookie

Analytics cookies

Google Analytics:
Name: Google Analytics
Purpose: Google Analytics is a web analytics service provided by Google that tracks and analyzes traffic to our website. It provides insights into how users interact with our website, helping us to better understand our audience and optimize our online activities.
Retention period: 2 years according to Technologies – Privacy & Terms – Google

Technical name(s):
_ga
_ga_J1SL5NSSTY

6.2 Google Analytics

This website uses Google Analytics, a web analytics service provided by Google LLC. As a company based in the European Union, we work with Google's subsidiary Google Ireland Limited (herein "Google").

The information generated by the cookie about your use of the website is transmitted to and stored on Google's servers.

Google uses this information on our behalf to evaluate your use of our website, compile reports on website activity, and provide us with other services relating to website and internet usage. The data transmitted may be used to create usage profiles of visitors to our website.

Please note that we cannot rule out the possibility that your personal data may be transferred to the United States. In this context, the European Commission's adequacy decision for the EU-U.S. Data Privacy Framework applies.

The analysis of your use of our website is based on your consent pursuant to Art. 6(1)(a) GDPR. For more information about the Google Analytics Terms of Service and Google's privacy practices, please go to:

Terms of Service | Google Analytics – Google or Privacy Policy – Privacy & Terms – Google

You may withdraw your consent at any time with effect for the future. To do so, you can access the settings in the bottom-left corner of our website or use the opt-out link below:

You can disable Google Analytics on our website. You can do this either via our Privacy Policy at https://www.ims.co.at/en/data-protection/, under section 6.2, or via the settings in the cookie window. You will find this at the bottom left of the screen.

7. Your rights as a data subject

As a data subject, you have a number of rights regarding the personal data we process about you. You may exercise any of these rights free of charge and without any formal requirements, by email, telephone, or mail, using the contact details provided below. Where necessary, we may ask you to provide proof of your identity.

In the case of joint controllers pursuant to Art. 26 GDPR, the following applies:
Regardless of the arrangement between the controllers, data subjects may exercise their rights under the GDPR with and against each controller individually. This applies to data processing activities in connection with the internal whistleblowing system and with digital business partner onboarding.

Your rights in detail:

Right of access: You may request information about the personal data we process about you at any time, without any formal requirements. In response to your request, we will provide you with written information about the personal data we hold about you, the purposes for which we use them, the categories of recipient to whom we disclose them, and how long we intend to retain them. We will respond to your request for access without undue delay and, in any event, within one month.

Right to erasure: You have the right to request the erasure of the personal data we process about you at any time, without any formal requirements. We will comply with your request where your personal data are no longer necessary for the purposes for which they were collected, where you withdraw any consent you may have given, where the data have been processed unlawfully, or where erasure is necessary for compliance with a legal obligation.

Right to rectification: If any personal data we process about you are inaccurate or incomplete, we will rectify them accordingly. To request rectification, simply contact us; no particular form is required.

Right to restriction of processing: If your personal data cannot be erased or you do not wish to have them erased, but you object to their processing beyond mere storage, we will restrict any further processing of your personal data at your request.

Right to data portability: At your request, we will provide you, free of charge, with the personal data we hold about you or that we have received on the basis of a contract or your consent, in a structured, commonly used and machine-readable format. No particular form is required for your request. You may use these data for your own purposes and pass them on to future contractual partners. At your request, and where technically feasible, we will also transmit your personal data directly to a recipient designated by you. In this case, we will notify you once the data have been transmitted. We will respond to your request without undue delay and, in any event, within one month.

Right to withdraw consent: You may withdraw your consent to the processing of your personal data at any time with effect for the future. In this case, we will cease processing your personal data. The withdrawal of consent does not affect the lawfulness of any processing carried out on the basis of your consent before its withdrawal.

Right to object: Where we process your personal data on the basis of our legitimate interests, you have the right under the GDPR to object to the further processing of your personal data. If you exercise this right, we will no longer process your personal data for the purpose to which you have objected, unless we can demonstrate compelling legitimate grounds for the processing that override your interests, rights, and freedoms, or the processing is necessary for the establishment, exercise, or defense of legal claims.

8. Right to lodge a complaint

The GDPR and the Austrian Data Protection Act guarantee you the rights set out above. If you believe that we have infringed any of these rights, you have the right to lodge a complaint with a data protection supervisory authority.

The data protection authority responsible for us is the

Austrian Data Protection Authority (Österreichische Datenschutzbehörde)
Barichgasse 40–42
1030 Vienna, Austria
Tel: 01/52 152-0
Email: dsb@dsb.gv.at

Data Protection Information last updated: 09/2026