INFORMATION ON DATA PROCESSING IN THE CONTEXT OF RECRUITMENT AND VACANCY-FILLING PROCEDURES

Version 1.0, valid from 1 October 2026, ISMS-DS-E-17

This privacy notice is intended for natural and legal persons involved in recruitment and job-filling procedures. Depending on the position and the context of the project, various third parties may be involved in the recruitment process alongside acib and the individuals applying for the relevant position. This may include, in particular, the involvement of a contracted recruitment consultancy or agency to review and shortlist applications; the involvement of external experts or an independent assessment committee to carry out a professional evaluation, particularly for academic positions or EU-funded programmes with a mandatory selection panel; the carrying out of background checks, including sanctions list screenings, for security-related or dual-use positions; and the involvement of funding bodies (e.g. FFG, European Commission), insofar as the position is funded as part of a funded project and documentation of the selection process is required for the funding body. Not all of these parties are involved in every procedure; which ones apply in each individual case depends on the position in question. acib is the sole data controller within the meaning of Article 4(7) of the GDPR for the personal data processed in this context, unless there is joint controllership with a partner institution in a specific case (see Section 5.3).

CLARIFICATION: acib GmbH does not currently conduct recruitment procedures on behalf of third parties; it therefore does not act as a recruitment agency commissioned by other institutions. Should this change in future, this privacy policy will be updated accordingly.

SCOPE: This information applies exclusively to the duration of the respective recruitment process, from the submission of documents until a rejection is issued, the application is withdrawn, or the candidate is added to a talent pool. Upon conclusion of an employment contract or a contract for services, the separate data protection information for employees of acib GmbH applies from that point onwards. Separate data protection information applies to other areas (procurement, commissioning, sponsorship, general events, academic collaborations, funding bodies) and can be found at https://www.acib.at/privacy. The summaries on the acib website are intended for day-to-day use; for legal matters, this detailed version is authoritative.

RELATIONSHIP TO CONTRACTUAL PROVISIONS: This information supplements any agreements with commissioned recruitment consultancies or agencies, cooperation agreements with partner institutions for jointly filled positions, the terms of use for applicant management software employed, and other agreements concluded on a case-by-case basis (e.g. confidentiality agreements for security-sensitive positions). In the event of any conflict between this

privacy policy and more specific contractual agreements or binding special statutory provisions (in particular the Equal Treatment Act (GlBG) and export control regulations), the more specific provisions shall take precedence. Subsequent versions of this document shall replace earlier versions from the respective effective date stated therein.

1 DATA CONTROLLER AND CONTACT

The data controller responsible for data processing in connection with application and recruitment procedures is

acib GmbH	Krenngasse 37/2, A-8010 Graz, Austria
Email	office@acib.at
Website	https://www.acib.at
Commercial Register Court	Regional Court for Civil Matters, Graz
Company register number	FN 224687y
VAT number	ATU54545504
Contact person for data protection matters	privacy@acib.at

2 CATEGORIES OF DATA SUBJECTS

In connection with recruitment procedures, we process personal data relating to the following groups of individuals:

GROUP OF INDIVIDUALS	DESCRIPTION
Applicants for advertised vacancies	Individuals who have applied for a specific job vacancy advertised by acib GmbH.
Unsolicited applicants	People who have applied to acib without reference to a specific vacancy.
Interns and thesis candidates	Individuals who have applied for an internship or a Bachelor's, Master's or doctoral thesis at acib, including underage summer interns.
Legal guardians	Legal guardians of underage applicants, particularly in connection with the granting of necessary consents.
References	Individuals named by applicants who provide information about previous employment as part of the suitability assessment.
Contact persons at recruitment consultancies and agencies	Contact persons responsible for acib at external recruitment consultancies commissioned by acib, insofar as they are involved in the screening or pre-selection of applications.
External assessors and members of assessment committees	Individuals who contribute to the professional assessment of applications, particularly within the framework of EU-funded programmes requiring a mandatory independent selection panel.

GROUP OF INDIVIDUALS	DESCRIPTION
Representatives of partner institutions for jointly filled positions	Individuals from cooperating universities or research institutions who are involved in the selection and assessment of applicants for jointly run projects or jointly supervised positions (e.g. PhD positions with dual supervision, EU MSCA networks), where applicable within the framework of joint responsibility in accordance with Article 26 of the GDPR.
Former employers and educational institutions	Organisations that verify certificates, periods of employment or evidence of training as part of background checks.
Public authorities in the context of background checks	Bodies that issue criminal record extracts or certificates of good conduct, as well as security authorities in the context of export control checks for security-sensitive positions.
Representatives of funding bodies	Case managers or specialist advisers at funding bodies (e.g. FFG, European Commission), provided that the position in question is funded as part of a funded project and that evidence of the selection process must be provided to the funding body.
Audit bodies (courts of auditors)	The Court of Auditors (RH) and the European Court of Auditors (ECA), provided that the post is funded as part of a funded project and that evidence of the selection process is required in the context of audits.
Occupational health service	For posts involving access to laboratories or higher levels of biological safety, where an occupational health assessment is required.
Members of the works council	Individuals who, in accordance with the rights of participation under Section 99 of the Works Constitution Act (ArbVG), are provided with information regarding the planned appointment of the selected candidate.

3 CATEGORIES OF DATA PROCESSED

We process the following categories of data which you provide to us directly, which are provided to us by third parties (e.g. referees, recruitment agencies, partner institutions) or which are generated as part of the selection or recruitment process:

Personal and contact details	
Personal information	First name and surname, date of birth, nationality, academic title
Contact details	Postal address, email address, telephone number
Application documents	
Application documents	Cover letter, CV, letter of motivation, photograph (optional)
Evidence of qualifications	School reports, diplomas, certificates, language skills, lists of publications
Terms and conditions	Salary expectations, availability, preferred start date, preference for fixed-term or full-time/part-time role
Process and interview data	
Communication details	Emails, interview transcripts, interviewers' notes

Aptitude data	Results of subject-specific tests, work samples, assessment centre evaluations, where applicable
Reference data	Information provided by referees, obtained only with your prior consent
Reports and evaluations	Statements from external experts or evaluation committees, particularly in the case of EU-funded programmes
Background check data	Results of academic and employment verifications, criminal record extracts or certificates of good conduct, where required for the position
Special categories of data and security data	
Voluntary information	Severe disability or health restrictions, where voluntarily disclosed for the purposes of assessing suitability or in connection with disability-related support schemes
Security screening data	Sanctions list and export control screening for security-related or dual-use-related positions
Occupational health data	Results of a fitness-for-work assessment carried out by the occupational health service, where required for roles involving access to laboratories
Funding and supporting documentation	
Evidence submitted to funding bodies	Documentation of the selection process (e.g. call for applications, evaluation reports), where the post is funded as part of a funded project and evidence must be provided

4 PURPOSES OF PROCESSING

We process data for the following purposes:

Purpose	Description
Application management	Reviewing, assessing and comparing applications received in relation to the advertised or a comparable position.
Communication	Arranging, conducting and following up on job interviews, as well as providing feedback on the status of the process.
Engaging recruitment consultancies	Sourcing and pre-selection of applications by external recruitment consultancies or agencies, where commissioned on a case-by-case basis.
Coordination with partner institutions	Coordination of the selection process for jointly run projects or jointly filled positions, e.g. PhD positions with dual supervision or EU MSCA networks.
Involvement of external assessors	Conducting independent expert assessments, particularly within the framework of EU-funded programmes requiring a selection panel.
Aptitude assessment	Conducting subject-specific tests or work samples, where required for the post.

Purpose	Description
Obtaining references	Contacting the referees you have named, exclusively with your prior consent.
Contract preparation	Preparation of an employment contract or contract for services in the event of a successful application, including the necessary administrative steps.
Retention for future roles (talent pool)	Storing your application documents beyond the current recruitment process for future, suitable positions, subject only to your separate consent.
Equal treatment	Documentation of the selection process to fulfil the obligations to provide evidence under the Equal Treatment Act (GlBG).
Security screening	Sanctions list and export control screening for positions with access to dual-use-relevant research areas in accordance with the Foreign Trade Act (AußWG) and EU Regulation 2021/821.
Information security	Protection of data processed during the application procedure in accordance with the NISG 2026 and Article 32 of the GDPR.
Documentation for funding bodies	Documentation of the selection process, insofar as the post is funded as part of a funded project and documentation is required for the funding body.

5 LEGAL BASIS FOR PROCESSING

5.1 OVERVIEW OF LEGAL BASES

The processing of personal data is carried out on the following legal bases:

- Article 6(1)(b) of the GDPR (pre-contractual measures): Conducting the selection process at your request with a view to potentially entering into an employment contract or a contract for services, including coordination with partner institutions in the case of jointly filled positions.
- Article 6(1)(a) of the GDPR (consent): For inclusion in a talent pool, the collection of references and the voluntary provision of special categories of personal data.
- Article 6(1)(c) of the GDPR (Legal obligation): To fulfil documentation and evidence requirements under the Equal Treatment Act, export control regulations, reporting obligations to funding bodies, and the works council's rights of participation pursuant to Section 99 of the Works Constitution Act (ArbVG).
- Article 6(1)(f) of the GDPR (legitimate interests): To safeguard the integrity of the selection process, ensure efficient recruitment with the involvement of external recruitment consultancies, and guarantee IT security when processing application documents.
- Article 9(2)(a) of the GDPR (Consent to special categories of data): Where you voluntarily provide information regarding a severe disability or health impairment that is not related to statutory employment obligations.

- Article 9(2)(b) of the GDPR in conjunction with the Act on the Employment of People with Disabilities (BEinstG): Insofar as the processing is necessary to fulfil obligations and exercise rights arising from employment law, for example in connection with the obligation to employ people with disabilities or preferential treatment for people with disabilities.

5.2 MAPPING OF PROCESSING PURPOSES TO LEGAL BASES

The table below assigns the specific legal basis under the GDPR, as well as the relevant special provisions under national and EU law, to each purpose mentioned in Chapter 4. In the case of processing based on Article 6(1)(f) of the GDPR, the overriding legitimate interest in each case is also specified.

SPECIFIC PROCESSING ACTIVITY	LEGAL BASIS UNDER THE GDPR	SPECIAL PROVISION / SUPPLEMENT	LEGITIMATE INTEREST (IN THE CASE OF POINT (F))
Application management, review and assessment of documents	Art. 6(1)(b)	---	---
Communication and arranging appointments	Art. 6(1)(b)	---	---
Engaging recruitment agencies	Art. 6(1)(b) and (f)	---	Efficient recruitment
Coordination with partner organisations in joint recruitment	Art. 6(1)(b) and (f)	Cooperation agreement	Implementation of joint recruitment
Involvement of external assessors and evaluation committees	Art. 6(1)(b) and (c)	Horizon Europe/MSCA programme rules	---
Aptitude tests, assessments, work samples	Art. 6(1)(b)	---	---
Obtaining references	Art. 6(1)(a)	---	---
Initiating a contract upon acceptance	Art. 6(1)(b)	---	---
Inclusion in the talent pool	Art. 6(1)(a)	---	---
Documentation on equal treatment	Art. 6(1)(c)	Equal Treatment Act	---
Security and export control screening	Art. 6(1)(c) and (f)	AußWG, Regulation (EU) 2021/821	Protection against export control breaches, integrity of the research centre
Information security / TOMs pursuant to Article 32 of the GDPR	Art. 6(1)(c) and (f)	NISG 2026	Protection of application data
Maintenance of records for funding bodies	Art. 6(1)(c)	FTFG, COMET Programme Document	---
Informing the works council prior to recruitment	Art. 6(1)(c)	Section 99 of the Works Constitution Act (ArbVG)	---

5.3 RESPONSIBILITY AND DATA PROCESSING IN THE RECRUITMENT PROCESS

acib GmbH is the sole data controller within the meaning of Article 4(7) of the GDPR for the processing of your personal data in the recruitment process. Where acib uses applicant tracking software or external recruitment consultancies, these parties process your data exclusively as data processors in accordance with Article 28 of the GDPR, following the instructions of acib GmbH. There is no joint controllership within the meaning of Article 26 of the GDPR with these service providers.

However, in the case of projects run jointly with partner institutions or jointly filled positions, for example within the framework of EU MSCA networks or PhD positions with dual supervision, joint controllership within the meaning of Article 26 of the GDPR may exist between acib and the respective partner institution, provided that the purposes and means of the selection process are determined jointly. In this case, an agreement in accordance with Article 26(1) of the GDPR specifies, in particular, which of the organisations involved fulfils their information obligations under Articles 13 and 14 of the GDPR and how data subjects' rights are to be coordinated. The key provisions of this agreement will be made available to you on request.

The AVV Register of acib GmbH provides information on the specific provider of the applicant management software used and on the conclusion of a data processing agreement; product-related details are not covered by this privacy policy.

5.4 SECURITY AND EXPORT CONTROL SCREENING

For positions involving access to dual-use-relevant research findings in industrial biotechnology, acib GmbH carries out a screening against relevant sanctions lists prior to concluding an employment or contract for services agreement.

LEGAL BASIS: Article 6(1)(c) of the GDPR in conjunction with the Foreign Trade Act (AußWG) and EU Regulation 2021/821 (Dual-Use Regulation); additionally, Article 6(1)(f) of the GDPR to protect the integrity of the research centre.

CATEGORIES OF DATA PROCESSED: first name and surname, date of birth, nationality, hit or no-hit status, date of the check.

NO AUTOMATED INDIVIDUAL DECISION-MAKING: A match is always verified manually by qualified staff; no automated decision within the meaning of Article 22 of the GDPR takes place.

DATA SUBJECTS' RIGHTS: You have the right to be informed about any check carried out and to have your data rectified in the event of a name mix-up. Please address any requests to privacy@acib.at.

6 RECIPIENTS AND CATEGORIES OF RECIPIENTS

Within acib GmbH, only the Human Resources department and the specialist department responsible for the advertised position (hiring manager) have access to your application documents. In addition, we disclose your personal data in the following cases:

RECIPIENT CATEGORY	DESCRIPTION
Applicant tracking system provider	As a data processor in accordance with Article 28 of the GDPR for the technical handling of the application process.
External recruitment consultancies and recruitment agencies	Where acib has commissioned an external recruitment consultancy to carry out sourcing or pre-selection.
External assessors and evaluation committees	For the independent expert assessment of applications, particularly within the framework of EU-funded programmes requiring a selection panel.
Partner institutions for jointly filled positions	Universities or research institutions with which acib jointly fills a post, e.g. PhD positions with dual supervision or EU MSCA networks.
Funding bodies	National and international funding bodies (e.g. FFG, European Commission), provided that the post is funded as part of a funded project and documentation of the selection process is required.
Authorities in the context of background checks	Bodies that issue criminal record extracts or certificates of good conduct, as well as security authorities in the context of export control checks for security-sensitive positions.
Audit bodies (courts of auditors)	The Court of Auditors (RH) and the European Court of Auditors (ECA), provided that the post is funded as part of a funded project and documentation of the selection process is required in the context of audits.
Works council	Information regarding the planned appointment in accordance with Section 99 of the Works Constitution Act (ArbVG), limited to the data necessary for the exercise of participation rights, usually the name and intended position of the selected candidate; application documents of unsuccessful candidates shall not be disclosed.
Occupational Health Service	For posts involving access to laboratories or higher levels of biological safety, where an occupational health assessment is required.
Public authorities	Tax office, courts and other public authorities, where there is a legal obligation to do so or where this is necessary to assert, exercise or defend legal claims.

7 FREEDOM OF INFORMATION (IFG)

As acib GmbH is subject to scrutiny by the Court of Auditors (RH), we are obliged to provide information in accordance with the Freedom of Information Act (IFG). Personal application data is generally exempt from this obligation due to the high level of protection it requires;

nevertheless, we carry out a rigorous balancing of interests in each individual case to safeguard your personal data to the fullest extent permitted by law.

8 SOURCE OF THE DATA

Where we do not collect data directly from you, it originates in particular from the following sources:

SOURCE	DESCRIPTION
Direct collection	Data that you provide to us directly, for example via an application form, by email or via a job portal.
Job boards and career portals	Data from application platforms you use.
Recruitment consultancies and agencies	Data provided to us by a commissioned recruitment consultancy as part of the sourcing or pre-selection process.
References	Information provided by the referees you have named, exclusively with your prior consent.
Former employers and training institutions	Verification data relating to certificates, periods of employment or evidence of training as part of background checks.
Partner institutions	Nominations, shortlists or assessment documents in the context of jointly filled positions, e.g. in EU MSCA networks or PhD positions with dual supervision.
Publicly accessible professional networks	Information from your publicly viewable profile, provided you have made it available for employers to contact you.

9 INTERNATIONAL DATA TRANSFERS AND TRANSFERS TO THIRD COUNTRIES

Where, as part of the application process, data is transferred to recipients outside the EU or the EEA – for example, to internationally used applicant management software or to partner institutions in the case of jointly filled positions – this is carried out exclusively in strict compliance with the legal provisions set out in Article 44 et seq. of the GDPR. In doing so, we rely on the following mechanisms:

MECHANISM	DESCRIPTION
Adequacy decisions by the European Commission	Preferred transfers to third countries for which the European Commission has determined an adequate level of data protection (e.g. Switzerland, the United Kingdom, Japan, Canada, South Korea).
Data transfers to the USA	In the case of US-based providers of applicant tracking systems, we rely primarily on the EU-US Data Privacy Framework (DPF), provided the recipient is certified accordingly.
EU Standard Contractual Clauses (SCCs) and supplementary measures	Where no adequacy decision is in place, we agree with the data recipients to use the Standard Contractual Clauses issued by the European Commission in accordance with

MECHANISM	DESCRIPTION
	Implementing Decision (EU) 2021/914, together with supplementary technical measures where necessary.
Transfer to partner institutions outside the EU/EEA	In the case of jointly filled positions with partner institutions in third countries (e.g. within the framework of international EU programmes), we base the transfer on the mechanisms mentioned above or on the grounds for derogation under Article 49 of the GDPR, insofar as this is strictly necessary for the conduct of the selection procedure in the interests of the data subject.
Countries subject to sanctions and embargoes	Transfers to countries subject to international sanctions or embargoes take place only in strict compliance with export control regulations; no transfer shall take place that contravenes applicable EU or UN sanctions regulations.

10 RETENTION PERIOD, DATA PROTECTION

We store your personal data only for as long as is necessary to fulfil the relevant purposes or as required by statutory retention obligations.

DATA CATEGORY	RETENTION PERIOD	REASON
Application documents in the event of Rejection	Up to 7 months after the conclusion of the process, after which they are deleted	Defence against claims under the Equal Treatment Act (GlBG)
Talent pool	Up to 2 years from the date of your consent	Thereafter, consent will be sought again or the data will be deleted
Background check data (references, verifications)	Up to 7 months after the conclusion of the process, after which they are deleted	As for application documents
Security screening records	7 years	General civil law retention practice
Supporting documentation for funding bodies	Up to 10 years after the end of the project	Reporting and audit obligations towards funding bodies, RH/ECA
IT log files (access and security logs)	Usually 6 months	No longer required for performance measurement thereafter; longer storage only in the event of security-related incidents
Data in the event of a successful application	Transferred to the personnel file	In accordance with the separate data protection notice for employees

11 DATA SECURITY AND TECHNICAL AND ORGANISATIONAL MEASURES

As a key organisation, acib GmbH is subject to the provisions of the NISG 2026 as well as the GDPR. To protect your application data, acib has implemented appropriate technical and organisational measures in accordance with Article 32 of the GDPR. This includes, in particular:

- Encryption of data during transmission (TLS 1.2+) and at rest (AES-256)
- A role- and rights-based access concept based on the 'need-to-know' principle, restricted to the HR department and the relevant specialist department
- Logging of security-related events and centralised SIEM monitoring
- Regular internal and external penetration tests, as well as an ISMS based on ISO/IEC 27001
- Training and awareness-raising measures for all staff involved in recruitment processes
- Careful selection and contractual obligations of data processors in accordance with Article 28 of the GDPR

Further information can be found in our Transparency and Trust Centre at https://www.a-cib.at/ttc.

12 YOUR RIGHTS AS A DATA SUBJECT

12.1 INDIVIDUAL RIGHTS

Under the GDPR, you have the following rights:

RIGHT	DESCRIPTION
Right of access (Art. 15 GDPR)	Information as to whether and which of your personal data we process, as well as a copy of this data.
Right to rectification (Art. 16 GDPR)	Rectification of inaccurate personal data or completion of incomplete personal data.
Right to erasure (Art. 17 GDPR)	Erasure of your personal data, provided there is a legal basis for doing so and no retention obligations prevent this.
Right to restriction of processing (Art. 18 GDPR)	Restriction of processing under certain conditions.
Right to data portability (Art. 20 GDPR)	Receipt of your data in a structured, commonly used and machine-readable format, provided that the processing is based on consent or a contract and is carried out by automated means.
Right to object (Art. 21 GDPR)	Objection to processing based on Article 6(1)(f) of the GDPR.
Withdrawal of consent (Article 7(3) of the GDPR)	Withdrawal at any time of consent previously given, for example for inclusion in the talent pool or for obtaining references, without affecting the lawfulness of the processing carried out up to that point.
Right to lodge a complaint with the supervisory authority (Article 77 of the GDPR)	Lodging a complaint with the relevant data protection supervisory authority.

12.2 EXERCISING YOUR DATA SUBJECT RIGHTS

You may exercise the rights set out in section 12.1 at any time, without any formal requirements and free of charge. We have established a dedicated process to ensure your requests are handled efficiently and transparently. The following contact channels are available to you for this purpose:

- **PRIMARY CHANNEL (RECOMMENDED):** by email to privacy@acib.at – this email address is used exclusively for data protection matters.
- **SECURITY INCIDENTS AND TECHNICAL DATA PROTECTION QUERIES:** security@acib.at (exclusively for reports of data breaches, IT security incidents or technical protective measures).

To ensure your enquiry can be clearly identified, please provide the following information:

- First name and surname, as well as your role and company affiliation, if applicable
- The specific right being exercised (e.g. right of access, rectification, erasure)
- Subject matter and timeframe or project reference, where known

Where there are reasonable doubts as to your identity, we are entitled, in accordance with Article 12(6) of the GDPR, to request additional information to confirm your identity. We limit this request to what is strictly necessary to prevent misuse and to protect your data from unauthorised access.

PROCESSING TIMEFRAMES IN ACCORDANCE WITH ARTICLE 12(3) OF THE GDPR: We will provide you with information regarding the measures taken in response to your request without undue delay, and in any event within one month of receiving the request. This period may be extended by a further two months, taking into account the complexity and number of requests. We will inform you of any such extension and the reasons for it within one month of receiving your request. If you submit your request electronically, we will, where possible, respond electronically as well, unless you specify otherwise.

If we do not act on your request, we will inform you without delay, and at the latest within one month of receiving the request, of the reasons for this and of the possibility of lodging a complaint with the supervisory authority or seeking a judicial remedy (Article 12(4) of the GDPR).

COSTS: Your request will be processed free of charge. In the case of manifestly unfounded requests or – particularly in the event of frequent repetition – excessive requests, we may, in accordance with Article 12(5) of the GDPR, either charge a reasonable fee or refuse to process the request; the burden of proof regarding the manifestly unfounded or excessive nature of the request lies with acib.

INTERNAL PROCESS: Upon receipt of your request, you will receive an acknowledgement of receipt within five working days, together with a reference code. The data protection team will then review the admissibility of the request using the dual-control principle, identify the relevant systems and processing activities, and coordinate the response with the relevant specialist departments (IT, project management, legal, HR).

WITHDRAWAL OF CONSENT: If you have given your consent (e.g. to be included in the talent pool or for us to obtain references), you may withdraw it at any time with future effect via the contact channels listed above. The lawfulness of the processing carried out prior to the withdrawal remains unaffected (Article 7(3) of the GDPR).

12.3 COMPETENT SUPERVISORY AUTHORITY IN AUSTRIA:

AUSTRIAN DATA PROTECTION AUTHORITY, Barichgasse 40–42, 1030 Vienna, Austria
Telephone: +43 1 521 52-0
Email: dsb@dsb.gv.at
Website: https://www.dsb.gv.at

LODGING A COMPLAINT: Complaints can be lodged online using the form on the Data Protection Authority's website, by email or by post. The procedure is free of charge for you.

13 OBLIGATION TO PROVIDE DATA

Providing your application documents is voluntary, but essential for the selection process to take place. Without the basic details (contact details, CV), we cannot process your application. Additional details (e.g. photo, salary expectations) are voluntary and will not negatively affect the decision on your application if you choose not to provide them.

14 ANALYSIS OF BUSINESS DATA AND USE OF AI TOOLS

acib GmbH does not use automated decision-making, including profiling, as defined in Article 22 of the GDPR, which produces legal effects concerning you or similarly significantly affects you. Decisions with legal implications are always made by humans (**human-in-the-loop**).

However, we reserve the right to analyse data for internal business purposes (e.g. process optimisation, market analyses or scientific evaluations). In doing so, modern artificial intelligence tools (e.g. Large Language Models / LLMs) may also be used for support, structuring or evaluation. Such evaluations have no legal effect and serve solely as supplementary information for business processes.

Your personal data is expressly not used for training AI models (training data).

15 COPYRIGHT NOTICE

This privacy policy was created with the assistance of artificial intelligence systems (including Perplexity) and edited by acib GmbH. It constitutes a copyright-protected work of acib GmbH. The copyright in the structure, wording and compilation of the content rests exclusively with

acib GmbH. Any form of reproduction, distribution, adaptation or public communication, even in part, requires the prior written consent of acib GmbH. Unauthorised use, in particular the reproduction of the texts for one's own commercial purposes, is prohibited and may be subject to legal action.