INFORMATION ON DATA PROTECTION OF SCHEIDT & BACHMANN GMBH

pursuant to Art. 13, 14 and 21 of the General Data Protection Regulation (GDPR)

We, the Scheidt & Bachmann GmbH (hereinafter "we", "us" or "Scheidt & Bachmann"), take the protection of your personal data very seriously and would like to inform you here about data protection at Scheidt & Bachmann.

Our data protection information is regularly updated in accordance with legal and technical requirements. Please note the current version of our data protection information.

CONTENT

I. GENERAL INFORMATION

1. DATA CONTROLLER

Data controller in the sense of Art. 4 No. 7 GDPR is:

Scheidt & Bachmann GmbH
Breite Straße 132, 41238 Mönchengladbach, Deutschland
Phone: +49 2166 266-0; e mail: info@scheidt-bachmann.de

2. CONTACT DETAILS OF THE DATA PROTECTION OFFICER

You can reach our data protection officer at the following contact details:

Scheidt & Bachmann GmbH
Datenschutzbeauftragten
Breite Straße 132, 41238 Mönchengladbach, Deutschland
Phone: +49 2166 266-839; e-mail: datenschutzbeauftragter@scheidt-bachmann.de

3. GENERAL INFORMATION ON DATA TRANSMISSION

We only transfer your personal data to third parties if

- you have given us consent to transfer the information to third parties,

- this is necessary in accordance with Art. 6 para. 1 p. 1 lit. b GDPR for the processing of contractual relationships with you,
- we are obliged to disclose, report and pass on data due to legal requirements,
- external service providers process the data on our behalf as order processors in accordance with Art. 28 GDPR or function transferees (e. g. external data centres, IT service providers, archiving, data destruction, legal advice, auditing, credit institutions, logistics companies, courier services).

In addition, we pass on your personal data to Scheidt & Bachmann group companies, which also process personal data partly under their own responsibility (so-called responsible parties, cf. Art. 4 No. 7 GDPR), to the extent necessary.

Within Scheidt & Bachmann, only those organisational units receive your data that require it to fulfil our contractual and legal obligations or in the context of processing and implementing our legitimate interest.

Beyond that, we do not pass on your personal data to third parties.

We do not intend to transfer your personal data to countries outside the European Union (EU) or the European Economic Area (EEA), but this may be done by external service providers if necessary. If external service providers come into contact with your personal data, we take legal, technical and organisational measures to ensure that they comply with the provisions of data protection laws and - if they act as processors - only process your data on our behalf and in accordance with our instructions.

4. YOUR DATA SUBJECT RIGHTS

Every data subject has the right to information under Art. 15 GDPR, the right to rectification under Art. 16 GDPR, the right to erasure under Art. 17 GDPR, the right to restriction of processing under Art. 18 GDPR and the right to data portability under Art. 20 GDPR. In order to exercise the aforementioned rights, you can contact the offices mentioned under clauses II and III.

If you have given us your consent to data processing, you can revoke this consent at any time without formalities. If possible, the revocation should be addressed to the offices mentioned under clauses II and III.

Furthermore, there is a right of appeal to a data protection supervisory authority (Art. 77 GDPR). The competent supervisory authority for Scheidt & Bachmann is:

North Rhine-Westphalia State Commissioner for Data Protection and Freedom of Information (LDI NRW)

However, we recommend that you first contact our data protection officer with a complaint.

5. YOUR RIGHT TO OBJECT ACCORDING TO ART. 21 GDPR

You have the right to file an objection at any time, on grounds relating to your particular situation, against the processing of personal data relating to you which is carried out on the

basis of Art. 6 para. 1 lit. f GDPR (processing of data on the basis of a weighing-up of interests) or Art. 6 para 1 lit. e GDPR; this also applies to any profiling based on this provision within the meaning of Art. 4 para. 4 GDPR.

If you file an objection, we will no longer process your personal data unless we can demonstrate compelling legitimate grounds for the processing which override your interests, rights and freedoms, or the processing serves to assert, exercise or defend legal claims.

In individual cases, we process your personal data for the purpose of direct advertising. You have the right to object at any time to the processing of personal data concerning you for the purpose of such advertising; this also applies to profiling insofar as it is associated with such direct advertising.

If you file an objection to processing for direct marketing purposes, we will no longer process your personal data for these purposes.

The objection can be made form-free and should, if possible, be addressed to the offices mentioned in the data protection statement under clauses II and III.

II. INFORMATION FOR BUSINESS PARTNERS

This data protection information applies to the collection, processing and use of your personal data when we have contact with you as a contact person of interested companies, customers, suppliers, service providers, clients, contractors and cooperation partners (hereinafter "business partners").

1. SCOPE OF THE PROCESSING

General data from the business relationship

We collect, process and use the following personal data in particular within the scope of the (developing) business relationship:

- Master data, in particular name and, if requested, function in the company;
- Contact details, in particular current business address, telephone numbers and email addresses and, if requested, post office box;
- If applicable, other data of your employer related to the fulfilment of the respective business relationship, such as dealer number, address data, contract data and/or payment and booking data

We collect, process and use personal data that is

- you have voluntarily surrendered to us,
- you or your employer have provided to us as part of the business relationship,
- arise from correspondence (postal and electronic) between you and your employer and us,
- arising from other postal, electronic or telephone communication.

Data from other sources

Furthermore, we also process - insofar as it is necessary for the fulfilment of the contract or pre-contractual measures with your employer or you or your employer have consented - such personal data that we have permissibly received from Scheidt & Bachmann group companies and other third parties.

We only process personal data from publicly accessible sources (e.g. authorities, internet) if this is legally permissible, for example because it is necessary for the provision of our services or you or your client/employer have consented**.**

E-mail

Should you wish to contact us by e-mail, we would like to point out that the content of unencrypted e-mails can be viewed by third parties. We therefore recommend sending confidential information by post. Please note that personal data transmitted by e-mail will be stored and processed for the purpose of following up your enquiry.

2. PURPOSE AND LEGAL BASIS OF THE PROCESSING

We process your personal data insofar as this is necessary to protect the legitimate interests of Scheidt & Bachmann (Art. 6 para. 1 lit. f GDPR), in particular:

- to enter into or perform orders, contracts and other business relationships (including to process purchase orders, deliveries or payments) or to prepare or respond to requests for proposals and to determine the terms of the contractual relationship, with our business partners for whom you may be acting as an agent or employee;
- subsequent direct advertising (by e-mail or post pursuant to § 7 para. 3 Act against Unfair Competion (UWG), with offers of similar products, services or events in connection with the existing business relationship, unless you object or have objected to this use;
- for internal administrative purposes (e.g. for accounting);
- to conduct anti-terrorism and sanctions list screenings, if applicable;
- to conduct court and official proceedings and/or for the purpose of asserting/exercising as well as defending against legal claim(s) at home and abroad;
- in order to send you our customer information to the extent relevant to your business activities, such as newsletters with information on products and references to current topics and events of the Scheidt & Bachmann Group;
- to make documents, such as contract documents or product information, available to you for download as an authorised person in our data room;
- for other communication purposes;
- to ensure the IT security and IT operations of our company;
- Advertising, market and opinion research, insofar as you have not objected to the use of your personal data;
- Review and optimisation of needs assessment procedures;
- Statistical evaluations or market analysis;

- Benchmarking;
- Further development of services and products as well as existing systems and processes;
- Obtaining information such as data exchange with credit agencies;
- on the use of service providers (e.g. external IT service providers) that support our business processes;
- to plan and host events to which you are invited, including coverage of these events on our website or intranet, which may include the publication of images and video footage on the internet or intranet in which you are pictured.

Furthermore, the processing of your personal data might be necessary in the context of the performance of a contract or a pre-contractual measure (Art. 6 para. 1 lit. b GDPR) with you as an individual (natural person).

Furthermore, the processing of your personal data may be required to comply with legal requirements (Art. 6 para. 1 lit. c GDPR), e. g. according to the provisions of the Money Laundering Act (GwG), or in the public interest (Art. 6 para. 1 lit. e GDPR). Likewise, you may also have given us your consent in accordance with Art. 6 para. 1 lit. a GDPR.

3. STORAGE PERIOD

We process your personal data only for as long as is necessary to fulfil the respective processing purpose and to comply with regulatory requirements, usually for the duration of the respective business relationship, or for the duration of any statutory retention period.

In addition, we are subject to various storage and documentation obligations, which result from the German Commercial Code (HGB) or the German Fiscal Code (AO), among other things. These can be up to 10 years.

Finally, the storage period is also assessed according to the statutory limitation periods, which can be up to thirty years, for example, according to §§ 195 et seq. German Civil Code (BGB), with the regular limitation period being three years.

III. SPECIAL INFORMATION FOR THE USE OF MICROSOFT TEAMS

If you access the Microsoft Teams website, the Microsoft Teams provider is responsible for data processing. However, accessing the website is only necessary for using Microsoft Teams in order to download the software for using Microsoft Teams. If you do not want to or cannot use the Microsoft Teams app, you can also use Microsoft Teams via your browser. The service will then also be provided via the Microsoft Teams website.

For more information on data protection at Microsoft, click here:

https://privacy.microsoft.com/de-de/privacystatement

https://www.microsoft.com/de-de/trust-center

1. WHAT DATA IS PROCESSED?

When using Microsoft Teams, various types of data are processed. The scope of the data also depends on the data provided before or during participation in a Teams meeting.

The following personal data are subject to processing:

- User details: e.g. display name, e-mail address if applicable, profile picture (optional), preferred language.
- Meeting metadata: e.g. date, time, meeting ID, phone numbers, location
- Text, audio and video data: It is possible to use the chat function in a Teams meeting. In this respect, the text entries made by the respective user are processed in order to display them in the Teams meeting. In order to enable the display of video and the playback of audio, the data from the microphone of your terminal device as well as from any video camera of the terminal device are processed accordingly for the duration of the meeting. The user can turn off or mute the camera or microphone at any time via the Microsoft Teams applications.

2. PURPOSES AND LEGAL BASES OF DATA PROCESSING

We use Microsoft Teams to conduct online meetings. If online meetings are to be recorded, this will be transparently communicated in advance and consent requested where necessary. The chat content is logged when using Microsoft Teams. Automated decision-making within the meaning of Art. 22 GDPR does not take place.

Insofar as personal data of our employees (or applicants) is processed, § 26 para. 1 Federal Data Protection Act (BDSG) is the legal basis for the data processing. If, in connection with the use of Microsoft Teams, personal data is not required for the establishment, implementation or termination of the employment relationship, but is nevertheless an elementary component in the use of Microsoft Teams, Art. 6 para. 1 lit. f GDPR is the legal basis for data processing. In these cases, our interest lies in the effective implementation of online meetings.

The legal basis for data processing when conducting online meetings is Art. 6 para. 1 lit. f GDPR. Here, too, our interest is in the effective implementation of online meetings.

3. RECIPIENTS OF THE COLLECTED CONTACT DATA

Personal data processed in connection with participation in online meetings will not be disclosed to third parties unless it is intended for disclosure. Please note that the content of online meetings, as well as face-to-face meetings, may be used to communicate information to third parties and are therefore intended for disclosure.

Other recipients: The Microsoft Teams provider necessarily receives knowledge of the above-mentioned data insofar as this is provided for in the context of the order processing agreement with Microsoft.

4. DATA TRANSFER TO A THIRD COUNTRY

Data processing in a third country outside the European Union (EU) does not take place in principle, as we have restricted the storage location to data centres in the European Union. However, we

cannot exclude the possibility that data is routed via internet servers located outside the EU. This may be the case in particular if participants in online meetings are located in a third country. However, the data is encrypted during transport via the internet and thus protected against unauthorised access by third parties.

5. STORAGE PERIOD

Personal data is generally deleted if there is no need for further storage. A requirement may exist if the data is still needed, for example, to fulfil contractual services. In the case of statutory retention obligations, deletion is only considered after the expiry of the respective retention obligation.

IV. ADDITIONAL INFORMATION FOR VISITORS TO THE COMPANY PREMISES

1. VISITOR MANAGEMENT

Scope and purpose of processing: When you visit our premises, e. g. as a supplier, service provider or customer, the following personal data may be collected:

- Identification data such as surname, first name, company, vehicle registration number, special authorisations (for truck drivers) or QR codes for the use of reserved visitor parking spaces in order to be able to identify you as an authorised visitor, for documentation, e.g. of meetings, events and agreements, for complaint management and dispute resolution, assertion or defence of legal claims or for the performance of internal and external audits and external inspections by licensing and supervisory authorities.
- Addresses and contact details such as postal address, e-mail address, telephone number and, if applicable, organisational data such as company, department, function, in order to be able to contact you if, for example, questions need to be clarified, information needs to be exchanged, appointments need to be made or access to the internet needs to be set up for you.
- Time recording, e. g. on company premises or for the provision of services, in order to be able to invoice services.
- IP address and voucher code if you, as a visitor, have been granted temporary access to the Internet via LAN (local aera network) or WLAN (wireless local aera network) via a captive portal, for authorisation and identity management for e-services, including technical support and troubleshooting.
- Name and address, as export control law requires that visitors to the S&B Group companies located at the Mönchengladbach site (natural persons and legal entities) be subjected to a sanctions list screening at the latest before entering the company premises. The basis for this is the legal obligation on the part of the data controller and its subsidiaries to ensure compliance with the requirements of foreign trade laws and regulations, including Art. 2 para. 1 lit. B of Regulation (EC) No. 2580/2001, Art. 2 para. 2 of Regulation (EC) No. 881/2002 and Art. 3 para. 2 of Regulation (EU) No. 753/2011. Within the scope of this screening, the person and/or the company (firm) are checked against the current sanctions lists of the

Federal Republic of Germany, the European Union and the USA. In the event of a verified hit, the person and/or the company is to be prohibited from entering the company premises. The results of the check are stored in the system for 365 days. Furthermore, a sanctions list check is carried out before each new visit.

We collect, process and use personal data that is

- you have voluntarily surrendered to us,
- you or your employer/client have provided to us as part of the business relationship,
- arise from correspondence (postal and electronic) between you and your employer/client and us,
- arising from other postal, electronic or telephone communication.

The legal basis for this processing of your personal data is Article 6 para. 1 lit. f GDPR. We have a legitimate interest in exercising our domiciliary rights, to ensure security at the site, to comply with legal requirements and to contact you quickly and easily. In addition, the processing of your personal data could be necessary in the context of the fulfilment of a contract or a pre-contractual measure (Art. 6 para. 1 lit. b GDPR), for the fulfilment of legal requirements (Art. 6 para. 1 lit. c GDPR) or in the public interest (Art. 6 para. 1 lit. e GDPR). Likewise, you may also have given us your consent in accordance with Article 6 (1) a GDPR.

Storage period: We only process your personal data for as long as is necessary to fulfil the respective processing purpose and to meet regulatory requirements, usually for the duration of the respective business relationship, or for the duration of any statutory retention period.

In addition, we are subject to various storage and documentation obligations, which result from the German Commercial Code (HGB) or the German Fiscal Code (AO), among other things. These can be up to 10 years.

Finally, the storage period is also assessed according to the statutory limitation periods, which can be up to thirty years, for example, according to §§ 195 et seq. German Civil Code (BGB), with the regular limitation period being three years.

2. Video surveillance

Scope and purpose of the processing: A video surveillance system is operated to monitor the company premises. The purpose of the video surveillance of the employee / company car parks, the entrances and exits to the company premises, the forecourt of the shipping department, the entrances for persons, the plant roads as well as the construction sites located on the company premises is to safeguard the domiciliary right, to protect the company premises and its facilities, the people and the things located thereon, but also to document the changes on the company premises for the company history. This right is basically covered by the domiciliary right. Furthermore, the purpose of video surveillance is to increase the sense of security of the people who are in these places, to deter people who are willing to commit vandalism, to prevent crime and to preserve evidence for the effective prosecution and enforcement of criminal and civil claims of both the person in charge and the employees and third parties.

Legal basis: Video surveillance is carried out on the basis of our legitimate interest within the meaning of Art. 6 para. 1 lit. f GDPR as well as §§ 4, 26 para. 4 Federal Data Protection Act (BDSG): Exercise of domiciliary rights; protection of property, people, things and facilities located on the company premises; protection against criminal offences; assertion of claims for damages under civil law by the responsible party and its employees as well as third parties; documentation of changes on the company premises for the company history; on the basis of a collective agreement in the case of processing of personal data of employees.

However, it can be assumed that the interest of the controller or a third party in video surveillance does not unduly interfere with the rights and freedoms of natural persons, especially since they are made aware of the video surveillance. Video surveillance is necessary and suitable to fulfil the intended purpose and is also the mildest means in this respect. Video surveillance is suitable for deterring possible troublemakers/offenders. The video surveillance is easily recognisable for everyone; in addition, signs indicate the video surveillance. Video surveillance provides usable images that support the implementation of house rights or criminal prosecution. No equally suitable, milder means can be identified. If this function were to be carried out by security guards, this would require staff around the clock. Even the use of dummy cameras is only likely to provide a comparable deterrent in the short term, as it cannot be ruled out that this will become known. The observation boundary ends at the boundary of the property.

Storage period: The data is deleted 5 working days after it has been created, insofar as it is not used.

3. License plate recognition

Scope and purpose of the processing: The entrances and exits to the company premises are equipped with barriers and TCP/IP-connected cameras for license plate recognition. The image capture is triggered by driving over an induction loop embedded in the roadway, whereby the license plate number is captured in an image file and read out together with the entry and exit time.

Vehicle number plate recognition could constitute video surveillance within the meaning of § 4 Federal Data Protection Act (BDSG) due to the permanent observation of a detection area and the recurring short-term image capture.

The legal basis for video surveillance is our legitimate interest within the meaning of Art. 6 Para. 1 lit. f GDPR as well as §§ 4, 26 Para. 4 Federal Data Protection Act (BDSG) for the following purpose: exercise of domiciliary rights, access control, protection of property, people, things and installations located on the company premises; protection against criminal offences; assertion of claims for damages under civil law by the responsible party and its employees as well as third parties; on the basis of a collective agreement in the case of processing personal data of employees.

Video surveillance is a suitable means of safeguarding the responsible person's domiciliary rights by giving the responsible person the possibility to decide who may enter the company premises and/or use the parking space located thereon. In addition, vehicle number plate recognition can be used for preventive purposes, such as deterring violations of the law within the traffic area, or for repressive purposes, such as preserving evidence for the enforcement of civil claims by the responsible party. A milder means of achieving the objective is not recognisable.

Storage period: The data is deleted 14 working days after collection if it has not been used.

Individual cases: In individual cases and only for a short period (max. 8 weeks), additional video cameras may be installed on the company premises for vehicle licence plate recognition. The data collected there will be processed by our subsidiary, Scheidt & Bachmann Parking Solutions GmbH, for testing purposes within the scope of product development and then deleted. The processing of vehicle video data for product development is our legitimate interest within the meaning of Art. 6 para. 1 lit. f GDPR and does not affect the interests or fundamental rights and freedoms of the data subject requiring the protection of personal data, as the video data is deleted immediately if it is processed for testing purposes without delay.

4. Construction site surveillance

Scope and purpose of processing: A video surveillance system is operated to monitor the construction sites on the company premises. The purpose of video surveillance of the construction sites is to safeguard domiciliary rights, protect the construction site and its facilities, the people and property located there, but also to document changes on the company premises for the company's history. This right is fundamentally covered by the domiciliary right. In addition, the purpose of video surveillance is to increase the sense of security of people who are on the construction site, to deter people who are prone to vandalism, to prevent crime and to preserve evidence for the effective prosecution and enforcement of criminal and civil law claims by the person responsible as well as employees and third parties.

Legal basis: Video surveillance is carried out on the basis of our legitimate interest within the meaning of Art. 6 para. 1 lit. f GDPR and §§ 4, 26 para. 4 BDSG: exercise of domiciliary rights; protection of property, people, objects and facilities located on the company premises; protection against criminal offenses; assertion of civil law claims for damages by the controller and its employees and third parties; documentation of changes on the company premises for the company's history; on the basis of a collective agreement in the event of the processing of personal data.

However, it can be assumed that the interest of the controller, the employees or a third party in video surveillance does not excessively interfere with the rights and freedoms of natural persons, especially since they are made aware of the video surveillance. Video surveillance is necessary and suitable to fulfill the intended purpose and also represents the mildest means in this regard. Video surveillance is suitable for deterring potential troublemakers/offenders. The video surveillance is easily recognizable for everyone; in addition, signs indicate the video surveillance. Video surveillance provides usable images that support the implementation of the house rules or criminal prosecution. An equally suitable, milder means is not recognizable. If this function were to be carried out by security staff, employees would be required around the clock. The use of dummy cameras is also only likely to provide a comparable deterrent in the short term, as it cannot be ruled out that this will become known. The observation limit ends at the boundary of the property.

Storage period: The data is stored for the duration of the construction site and then deleted if it is not used.

V. ADDITIONAL INFORMATION FOR PHOTOGRAPHY AND FILMING EVENTS

1. SCOPE OF THE PROCESSING

In the context of events, we may take photographs and/or film recordings and collect and process the following in this context

- Photo and film data and sound recordings of you
- If applicable, your name and, if requested, function in the company
- Contact details, if applicable.

If you do not wish to be photographed/filmed, please mention this directly to the photographer/cameraman so that your wish can be taken into account.

2. PURPOSE AND LEGAL BASIS OF THE PROCESSING

The legal basis for the data processing is Art. 6 para. 1 lit. f DSGVO. The photos/films will be taken for the purpose of documenting the event and will be used/saved/copied/distributed/exhibited/published on the internet via the company homepage of the responsible party and/or on the intranet, in social media channels as well as in print media, in particular in the newsletter, for the purpose of documenting the event, for public relations and the presentation of the activities of the responsible party in order to increase the level of awareness of the responsible party as well as, if applicable, also for the long-term documentation of the company history of the responsible party.

It can be assumed that the interest of the responsible person in the production and use of the photos/films does not unduly interfere with the rights and freedoms of the natural persons, especially since they are informed about the production and use of the photos/films in advance and/or at the event, and care is taken both in the production of photos/films and in the publication of the same that no legitimate interests of persons depicted are violated. If the rights and freedoms of a person depicted are violated for reasons particularly worthy of consideration, we will take appropriate measures to refrain from further processing. A deletion in print media that have already been issued cannot take place. Deletion on the website, in social media channels or on the intranet will be carried out within the scope of technical possibilities.

3. STORAGE PERIOD

Data not used following the event will be deleted immediately. Otherwise, the data will be stored and deleted at the end of the 4th calendar year after production if it has not been used.

4. ADDITIONAL INFORMATION ON DATA TRANSMISSION

Departments of the data controller that necessarily need to receive the data in the course of carrying out the activity (e. g. marketing, IT, other administrative units), Scheidt & Bachmann group companies, contractors and processors involved in the processing (preparation as well as publication).

If applicable, tax advisors, authorities (tax office, other authorities) as well as legal representatives (in the enforcement of rights or defence against claims or in the context of official proceedings).

The data is made available on the internet to the worldwide public, on the intranet worldwide to the employees of the Scheidt & Bachmann group companies, and published in social media channels. The data will be published in print media: Employee newsletters distributed to employees of Scheidt & Bachmann group companies in a limited edition of 4,000 copies. Trade press/newsletters are distributed to the worldwide public.

The data will not be passed on to recipients who pursue their own purposes with this data. In the case of social media channels, however, it may be that the respective social media service receives the right to exploit the published data.

No other transfer to recipients in a third country (outside the EU) or to an international organisation is envisaged.

Through the use on the website, there is the possibility of worldwide access to the images/films or the retrieval of the posted data and images also from countries in which no or no sufficient data protection standard exists. The responsible party can therefore neither influence the access to these data via the internet nor the use of these data and in this respect also cannot assume any guarantee for the observance of data protection.

Using suitable search engines, personal data can be found on the internet and the persons depicted in images can also be identified under certain circumstances. This also makes it possible to create personality profiles by combining this data and information with other data available on the internet and to open up additional possibilities of use, e. g. for advertising purposes. Due to the possibilities of worldwide retrieval and storage of data by other bodies or persons, further use by other bodies or persons or retrieval via archive functions of search engines cannot be ruled out in the event of revocation of consent and despite removal of your data and images from our website. Unidentification in print media that have already been issued cannot take place.

VI. ADDITIONAL INFORMATION FOR SOCIAL MEDIA

1. SCOPE

We would like to inform you about the processing of your personal data and about your rights as a data subject in the area of our social media pages. This applies to all our appearances on the following social media platforms:

LinkedIn
"Scheidt & Bachmann" - https://www.linkedin.com/company/scheidt-&-bachmann/

XING
"Scheidt & Bachmann GmbH" - https://www.xing.com/pages/scheidt-bachmanngmbh

Instagram
"Scheidt & Bachmann Career" - https://www.instagram.com/scheidtundbachmann_karriere/

Facebook
"Scheidt & Bachmann" - https://www.facebook.com/scheidtundbachmann
"Careers at Scheidt & Bachmann" - https://www.facebook.com/profile.php?id=61551198496181

2. PROVIDER OF SOCIAL MEDIA PLATFORMS

In addition to us, the respective operator of the social media platform (hereinafter "provider") is also responsible for data processing on our social media pages. In detail, these are

- for the **LinkedIn platform,** LinkedIn Ireland Unlimited Company, Wilton Plaza, Wilton Place, Dublin 2, Ireland (hereinafter also referred to as "LinkedIn"),
- for the **XING platform**, XING SE, Dammtorstraße 30, 20354 Hamburg, Germany (hereinafter also referred to as "Xing") and
- Meta Platforms Ireland Ltd, 4 Grand Canal Square, Grand Canal Harbour Dublin 2, Ireland (hereinafter also referred to as "Meta Platforms" or "Facebook") for the **Facebook** and **Instagram platform.**

We have entered into a joint responsibility agreement with Meta Platforms Ireland, Xing SE and LinkedIn Ireland in accordance with Article 26 of the GDPR, in which we have defined how the respective tasks and responsibilities are organised when processing personal data and who fulfils which data protection obligations.. In particular, we have determined how an appropriate level of security and your rights as a data subject can be ensured, how we can jointly fulfil the information obligations under data protection law and how we can monitor potential data protection incidents. This also includes ensuring that we can fulfil our reporting and notification obligations. For more information on the "Page Insights" function and the main content of our agreement with the operators of the social media platform, please refer to section IV.1.

You can contact the respective data protection officer of those jointly responsible with us as follows:

- You can contact **LinkedIn**'s data protection officer using the form below: https://www.linkedin.com/help/linkedin/ask/TSO-DPO
- You can contact **XING**'s data protection officer via a form: https://www.xing.com/support/contact/security/data_protection
- You can contact the data protection officer of **Facebook** and **Instagram** via a form: https://www.facebook.com/help/contact/540977946302970

The operators of the social media platforms are available to you as a central point of contact. However, you can also assert your rights in relation to processing under joint responsibility against us. If you contact us, we will coordinate with the respective provider in order to answer your enquiry and guarantee your rights as a data subject.

3. GENERAL INFORMATION FOR SOCIAL MEDIA PAGES

We would like to point out that you use our social media pages and their functions as well as social media platforms as a whole on your own responsibility. This applies in particular to the use of interactive functions (e.g. liking, commenting, sharing, rating).

Your use of the **LinkedIn platform** is primarily governed by the user agreement (https://www.linkedin.com/legal/user-agreement) and LinkedIn's privacy policy (https://www.linkedin.com/legal/privacy-policy).

Your use of the **XING platform** and data processing by Xing are primarily governed by the General Terms and Conditions (https://www.xing.com/terms) and XING's Privacy Policy (https://privacy.xing.com/de/datenschutzerklaerung).

Your use of the **Instagram platform** and data processing by **Facebook is primarily** governed by Facebook's Terms of Use (https://de-de.facebook.com/legal/terms/) and Data Policy (https://de-de.facebook.com/about/privacy) and Instagram's Terms of Use (https://help.instagram.com/581066165581870) and Privacy Policy (https://help.instagram.com/519522125107875).

We expressly draw your attention to the fact that the respective providers may also store the data of their registered users (hereinafter "users") and other interested visitors to the social media platforms (hereinafter "visitors"), e.g. personal information, IP address, cookies, etc., outside the European Union (EU) or the European Economic Area (EEA) and use them for their own business purposes.

We generally have no influence on the collection of data and its further use by the providers. To what extent, where and for how long the data is stored, to what extent the providers comply with existing deletion obligations, which analyses and links are made with the data and to whom the data is passed on is neither recognisable nor influenceable for us. We therefore ask you to carefully check which personal data you disclose as a user on social media platforms.

If you would like to find out more about our company without using social media platforms, you can alternatively access much of the information provided on our social media pages on our website https://www.scheidt-bachmann.de/de/.

4. SCOPE, PURPOSE AND LEGAL BASIS OF THE PROCESSING

The subject of data protection is the protection of personal data. This is all information that relates to an identified or identifiable natural person (so-called data subject). This includes information such as the data you provide; your respective profile, date and time of interaction, type of end device, type and content of interaction (e.g. likes, direct messages, comments), profile name, profile picture, contact information, education, professional background, "Like" information, but also other information about you that arises in the context of using our social media pages (e.g. connection and usage data).

Below you will find an overview of the purposes and legal bases of data processing. We operate our social media pages to inform users and visitors about our company and to exchange information with them.

Unless otherwise described below, your data is processed on the basis of our legitimate interests (Article 6 para. 1 lit. f GDPR) in the economic operation, optimisation and usage analysis of our social media pages and in order to communicate with you as a user/visitor, to inform you about current topics and to carry out advertising activities on the social media platforms.

If you contact us via a social media site for the purpose of concluding a contract with us, Art. 6 para. 1 sentence 1 lit. b) GDPR is the legal basis for processing.

It is sometimes possible to use our social media pages without registering with the social media platforms. Even if you use the social media pages without registering, personal data may be processed.

Below you will find an overview of the type, scope, purposes and, if applicable, specific legal bases of automated data processing in the context of the use of our social media pages.

Utilisation analysis

In connection with the operation of our social media pages, we use the "Insights" or "Analytics" function of the social media platforms, by means of which the provider provides us with statistical data on the use of our social media pages, which are anonymous to us, i.e. the personal data of individual users or visitors cannot be viewed by us. We do not know in detail which data the provider uses to analyse usage in connection with our social media pages.

In connection with the operation of our Instagram pages and **Facebook pages,** we use the "Page Insights" function of Facebook (the provider of the services), which Facebook uses to provide us with statistical data on the use of our Instagram page, which is anonymous to us, i.e. the personal data of individual users or visitors cannot be viewed by us. You can find out what data Facebook uses to analyse usage in connection with our **Instagram page** ("Page Insights data") and what information Facebook provides on data processing in connection with the Page Insights function here: https://de-de.facebook.com/legal/terms/information_about_page_insights_data.

With regard to Page Insights data, we are jointly responsible with **Facebook** for data processing and have concluded an agreement between joint controllers ("Page Insights Addendum" - https://de-de.facebook.com/legal/terms/page_controller_addendum), which sets out our respective obligations under the GDPR. We have agreed therein that

- we are jointly responsible with Meta Platforms for the processing of Page Insights data;
- Meta Platforms assumes primary responsibility and is primarily responsible for providing you with information about the joint processing and enabling you to exercise your rights under the GDPR (see below section VIII);
- of Meta Platforms alone can make and, if necessary, implement decisions regarding the processing of Page Insights data and the fulfilment of its data protection obligations;
- Meta Platforms is solely responsible for the processing of other personal data in connection with Page Insights that is not covered by the Page Insights Addendum; we cannot request disclosure in this regard;
- the Irish Data Protection Commission (https://www.dataprotection.ie) is the authority responsible for the supervision of processing under joint responsibility.

In particular, we receive aggregated data from **LinkedIn in the** following areas: Reach (impressions, page views, unique users, access to subpages), target group (demographic information), interaction (impressions, reactions, click rate, likes, shares, comments, (link) clicks, engagement rate), target group (demographic/geographic information)

With regard to Page Insights data, we are jointly responsible with LinkedIn for data processing and have concluded an agreement between joint controllers ("Page Insights Addendum" - https://legal.linkedin.com/pages-joint-controller-addendum), which sets out our respective obligations under the GDPR. We have agreed therein that

- we are jointly responsible with LinkedIn for the processing of Page Insights data;
- **LinkedIn** assumes primary responsibility and is primarily responsible for providing you with information about the joint processing and enabling you to exercise your rights under the GDPR (see section 8 below);
- the Irish Data Protection Commission (https://www.dataprotection.ie) is the authority in charge of the supervision of processing under shared responsibility.

In particular, we receive aggregated data from **Xing** in the following areas: Reach (impressions), interactions ((link) clicks, likes, shares, comments), target group (demographic/geographical data, previously visited websites).

Direct contact

If you contact us directly via our social media pages (e.g. via personal message, messenger or a pre-filled form), the data you provide (e.g. name, email address, other details) will only be processed for the purpose of recording and, if necessary, responding to your enquiry. We do not transfer this data to our internal systems.

As far as the initiation of a contractual relationship is concerned, the processing of data transmitted in the context of direct contact via the social media platform is based on Article 6 (1) (b) GDPR. Insofar as you are asked by us for consent to data processing, e.g. with the help of a checkbox in connection with forms provided by us, the legal basis for data processing in this respect may be Article 6 para. 1 lit. a) GDPR.

As we are not aware of the confidentiality of the information you provide when contacting us directly and its use by the provider itself, please refrain from transmitting sensitive data or other confidential information, such as application documents or bank or credit card details. We recommend that you use a more secure means of transmission, such as letter post or our career portal at https://www.scheidt-bachmann.de/de/karriere.

If you contact us directly as part of a job application, in particular via our **Xing** or **LinkedIn** page, and send us information about yourself, we regularly delete such requests immediately from the respective social media platform.

Other user interactions

In accordance with the way a social media platform works, it is possible for us to gain knowledge of the users who like, subscribe to, rate, comment on or share our social media pages and our posts, provided that you have made your interaction on the social media platform public and have not expressly labelled it as "private" using the settings of the social media platform. We analyse this information in aggregated form in order to provide our users and visitors with more relevant content that may be of greater interest to them. The information obtained in this way does not allow any conclusions to be drawn about a natural person.

In your respective social media profile, you as a user have the option, for example, to actively hide your "posts", "tweets", "rated videos", "subscriptions", "followers", "pins" or other profile information or to no longer follow or subscribe to our social media pages. You will then no longer appear in the list of followers or subscribers to this social media page.

Interest-based advertising

We are able to use demographic and geographical analyses of our target groups provided to us by the provider in order to place targeted interest-based advertisements on our social media pages or to highlight our posts, but without obtaining direct knowledge of the identity of the user or visitor to whom the advertisements are displayed. In this case, the display of advertisements or highlighting of posts on our social media pages is based on an analysis of previous usage behaviour by the provider, whereby we only have anonymised or pseudonymised information that regularly does not allow us to identify you personally and is not merged with any personal data stored by us at any time.

As a user of the **LinkedIn** platform, you can control the extent to which your user behaviour may be recorded and used by LinkedIn in the LinkedIn ad settings (https://www.linkedin.com/psettings/advertising). Further information on managing ad settings on the LinkedIn platform can be found here: https://www.linkedin.com/help/linkedin/answer/65446/anzeigeneinstellungen-verwalten?lang=de

As a user of the **Xing** platform, you can control the extent to which your user behaviour may be recorded and used by Xing in the settings for "Measurement and optimisation of advertising" (https://privacy.xing.com/de/datenschutzerklaerung/informationen-die-wir-auf-grund-ihrer-nutzung-von-xing-automatisch-erhalten/messung-und-optimierung-von-werbung).

If you as a user have linked your **Instagram** account to your **Facebook** account, you can control the extent to which your user behaviour may be recorded and used by Facebook (on Facebook and Instagram pages) in the Facebook advertising preferences settings (https://de-de.facebook.com/ads/preferences).

5. RECIPIENT OF PERSONAL DATA

Within our company, only those persons have access to your personal data who need it for the purposes stated in each case. We only pass on your personal data to external recipients if we are legally authorised to do so or if we have your consent. The recipient of the data is initially the respective provider of the social media platform, where it may be passed on to third parties for their own purposes and under the responsibility of the provider of the social media platform. The recipient of publications is also the public, i.e. potentially anyone.

6. DATA PROCESSING IN THIRD COUNTRIES

If we transfer data to bodies whose registered office or place of data processing is not located in a member state of the European Union, another signatory state to the Agreement on the European Economic Area or a state for which an adequate level of data protection has been established by a decision of the European Commission, we will ensure before the transfer that the data transfer is either covered by a legal authorisation, that there are guarantees for an adequate level of data

protection with regard to the data transfer (e.g. through the EU standard contractual clauses) or that you have given your consent to the data transfer. e.g. through the EU standard contractual clauses) or that you have given your consent to the data transfer.

If the data transfer is based on Article 46, 47 or 49 (1) subparagraph 2 GDPR, you can obtain from us a copy of the guarantees for the existence of an adequate level of data protection in relation to the data transfer or an indication of the availability of a copy of the guarantees. Please use the information in section VIII.

7. STORAGE PERIOD, DELETION

If we are legally authorised to do so, we will only store your personal data for as long as necessary to achieve the purposes pursued or as long as you have not withdrawn your consent. In the event of an objection to processing, we will erase your personal data unless further processing is still permitted under the statutory provisions. We will also erase your personal data if we are obliged to do so for other legal reasons. Applying these general principles, we usually delete your personal data immediately

- after the legal basis no longer applies and provided that no other legal basis (e.g. retention periods under commercial and tax law) applies. If the latter applies, we delete the data after the other legal basis no longer applies;
- if your personal data is no longer required for the purposes pursued by us and no other legal basis (e.g. retention periods under commercial and tax law) applies. If the latter applies, we will delete the data once the other legal basis no longer applies.

We review the necessity of the personal data stored by us on the social m

edia platforms at least once a year and carry out corresponding deletion routines, as part of which we initiate the removal of messenger messages, for example. However, due to the lack of technical control over the social media platforms, we cannot ensure that the social media providers will actually delete the data.

In principle, we have no influence on how the providers of the social media platforms store or delete your data on their platforms. For details on this, please refer to the

- LinkedIn privacy policy (https://www.linkedin.com/legal/privacy-policy),
- Privacy policy of Xing (https://privacy.xing.com/de/datenschutzerklaerung),
- Facebook privacy policy (https://de-de.facebook.com/about/privacy),
- Instagram privacy policy (https://help.instagram.com/519522125107875).

VII. INTERNAL REPORTING UNIT UNDER THE WHISTLEBLOWER PROTECTION ACT

The internal reporting unit is part of a whistleblower system that fulfils the requirements of the EU Whistleblower Protection Directive (Directive (EU) 2019/1937; Whistleblower Directive), the Act for Better Protection of Whistleblowers (Whistleblower Protection Act - HinSchG) and other laws.

Scheidt & Bachmann GmbH (Breite Straße 132, 41238 Mönchengladbach, Germany) has set up an internal reporting unit for all companies affiliated with Scheidt & Bachmann GmbH pursuant to Sections 15 et seq. Aktiengesetz (German Stock Corporation Act) (hereinafter referred to individually or collectively as "Scheidt & Bachmann"). The internal reporting office is operated for all Scheidt & Bachmann Group companies that are obliged to operate an internal reporting office under the Whistleblower Protection Act in conjunction with the EU Whistleblower Protection Directive or that voluntarily operate an internal reporting unit in accordance with the Whistleblower Protection Act.

The internal reporting unit receives your report and forwards it to the Scheidt & Bachmann company concerned for further processing. Your personal data will only be processed if your report is not anonymous.

1. CATEGORIES OF PERSONAL DATA THAT ARE PROCESSED

Personal data is any information relating to an identified or identifiable natural person. This includes, for example, your name or address. Non-personal data is all information that does not allow any conclusions to be drawn about the identity of a person (anonymous data).

If you do not submit your report anonymously to the internal reporting unit, it will only collect the personal data that you provide. This is usually your name and, if applicable, your contact details and other personal data resulting from your report. Other personal data may be processed if it is collected in connection with the processing of your report. We process this data in accordance with the provisions of the applicable data protection laws, such as the EU General Data Protection Regulation (GDPR) and the German Federal Data Protection Act (BDSG).

2. PURPOSE AND LEGAL BASIS OF THE PROCESSING

The processing of personal data by the internal reporting unit serves the early detection and clarification of compliance violations, violations of legal regulations and violations in connection with our business operations by employees, customers, suppliers and other third parties. If you disclose your identity to the internal reporting unit and consent to your name being passed on to one of the Scheidt & Bachmann companies concerned, the legal basis for the processing of your personal data as a whistleblower is your consent (Art. 6 para. 1 sentence 1 lit. a GDPR).

The legal basis for the processing of the personal data of the persons affected by the report is our legitimate interest in the detection and prevention of legal violations and misconduct (Art. 6 para. 1 sentence 1 lit. f GDPR). We have a legitimate interest in detecting and preventing breaches of the law and misconduct if we are legally obliged to do so in certain areas. In addition, such violations can not only cause considerable economic damage, but also lead to a considerable loss of reputation.

If the data subject is an employee of Scheidt & Bachmann, the legal basis for the processing in the course of processing or further investigation of the reported facts is Section 26 para. 1 sentence 1 BDSG (processing for the purposes of the employment relationship) or Section 26 para. 1 sentence 2 BDSG (processing for the detection of criminal offences) and, if applicable, our legitimate interest described above (Art. 6 para. 1 sentence 1 lit. f GDPR).

3. SCOPE AND LOCATION OF DATA PROCESSING

General information

You can send your report to the internal reporting unit

- by telephone

  from Germany on +49 800 3800 999 and

  from other countries on +49 69 99998839,

- by e-mail to whistleblower@scheidt-bachmann.de,
- by post to Scheidt & Bachmann GmbH, Corporate Compliance, Whistleblower Protection Reporting Unit, Breite Straße 1321, 41238 Mönchengladbach, Germany,
- by internal mail to Corporate Compliance, Reporting Unit Whistleblower Protection, or
- by using the web-based whistleblower system "Legal Tegrity".

Whistleblowing system “Legal Tegrity"

You can access the "Legal Tegrity" whistleblower system via a hyperlink on the website www.scheidt-bachmann.de and submit your report there. When you submit your report, you can set up a non-personalised mailbox so that you can communicate with us during the processing of your report. Setting up the mailbox is voluntary and not required for submitting a notification. Access to this mailbox is password-protected in the form of a PIN number, which will be sent to you after you have submitted your report.

The "Legal Tegrity" whistleblowing system does not collect any data that could lead to identification in any way.

4. CONFIDENTIALITY AND DISCLOSURE OF DATA

Scheidt & Bachmann handles all incoming reports responsibly and carefully. This applies in particular to the personal data that you submit about yourself, but also to the personal data of the person affected by your report. All reports or complaints are processed by selected and specially trained employees of the Corporate Compliance department and, if necessary, by employees of the Scheidt & Bachmann company concerned.

All persons involved in the process are subject to confidentiality, are impartial and independent in the fulfilment of their duties and are not bound by instructions.

Legal Tegrity GmbH, which operates the whistleblowing system, is appointed with the processing of any personal data as a processor.

Scheidt & Bachmann relies on law firms or auditing companies to process your report, to take the necessary clarification measures and to assert, exercise and defend legal claims. In exceptional cases, personal data of the whistleblower and the person concerned must be transmitted to authorities, courts or third parties if the disclosure of information is mandatory for Scheidt & Bachmann. In addition, under certain circumstances, Scheidt & Bachmann must also disclose the reported information to the person affected by the report.

If the whistleblower has disclosed his/her identity and/or contact details, the internal reporting unit will inform the whistleblower if the reported information must be disclosed and the reasons for this. Notification will only be omitted if this would jeopardise the official investigation.

5. NO DATA TRANSFER TO THIRD COUNTRIES

The data transmitted to the internal reporting unit will be processed by us and the processor exclusively in the Federal Republic of Germany. Data will not be transferred to countries outside the European Union (EU) or the European Economic Area (EEA) unless your report concerns a Scheidt & Bachmann company in a third country.

Scheidt & Bachmann companies are located in the following third countries: United Kingdom of Great Britain and Northern Ireland, Russia, Switzerland, Tunisia, Israel, Ukraine, USA and Canada. If there is no adequacy decision by the EU Commission for the country in question in accordance with Art. 45 GDPR, we ensure that your rights and freedoms are adequately protected and guaranteed in accordance with the requirements of the GDPR by means of appropriate contracts.

6. STORAGE OF THE DATA

The data transmitted by you will be deleted at the latest 3 years after completion of the procedure. The storage period may be extended in order to fulfil the requirements of the HinSchG or other legal provisions, if and insofar as this is necessary and proportionate.

In addition, special statutory provisions may require a longer retention period, such as the preservation of evidence within the framework of statutory limitation periods. According to Sections 195 et seq. of the German Civil Code (BGB), the standard limitation period is three years, but limitation periods of up to 30 years may also be applicable.

If the data is no longer required for the fulfilment of contractual or legal obligations and rights, it is regularly deleted, unless its - temporary - further processing is necessary for the fulfilment of the above-mentioned purposes due to an overriding legitimate interest.

7. OBLIGATION TO PROVIDE DATA

The use of Scheidt & Bachmann's internal reporting unit is voluntary on the part of the person providing the information. There is no obligation to provide data.

VIII. FINAL REMARKS

Security: We use technical and organisational security measures in order to adequately protect your personal data processed by us against accidental or intentional manipulation, loss, destruction or against access by unauthorised persons.

Validity and actuality of the privacy policy: This privacy policy is dated August 2025 and is valid as long as no updated version replaces it.

Due to the implementation of new technologies, it may become necessary to change this privacy policy. We reserve the right to change the privacy policy at any time with effect for the future. We recommend that you re-read the current data protection declaration from time to time.