Company policy - external partners

Content

Company policy - external partners

1. Foreword (Company and Business Purpose)

We, Allgeier Engineering GmbH, are a service provider for quality management, system integration, verification & validation, software development and project management. In the product development process and in series support, we look after various areas in the automotive and railway environment. Due to the activities and the proximity to the development areas in these industries, we require an effective management system, which must also be adhered to by the relevant partners. The company guideline provides information on the most important aspects of our management system.

2. Scope/area of application

This company policy applies in all areas and applies to all external persons (e.g. service providers, suppliers, customers and persons involved in project work) who regularly work in our company or have access to our company systems. It is binding for all and must be observed throughout. Any deviation from the guideline is only permitted with the prior documented approval of the Compliance Officer, Data Protection Officer, Quality Officer or Information Security Officer. A violation of the regulations in the corporate guideline can lead to consequences. If the policy is violated intentionally or negligently and the contractor suffers damage as a result, the party responsible shall be liable to the client in accordance with the principles applicable in the law and in case law. In the case of violations of data protection law, it should be noted that the originator becomes liable if he processes personal data contrary to or without the instruction of the client in a manner that violates the data protection requirements of the EU General Data Protection Regulation (DS-GVO) and the Federal Data Protection Act (BDSG). Unlawful processing of personal data may also result in claims for damages by a data subject. The decision on the steps to be taken is made and followed up in the management meeting. The decision is derived from the consideration of each individual case, taking into account the damage that has occurred for the company.

3. Legal compliance

When handling information and data in our company, external persons must comply with the applicable legal provisions on data protection (DS-GVO and BDSG) and information security (e.g. ISO 27001/27002) as well as the company regulations. If external persons are unsure whether and to what extent legal provisions or company regulations must be complied with, they must contact their internal contact person for clarification. If necessary, the contact person must coordinate any ambiguities with one of the management representatives (CO, DPO, ISB, QMB).

4. Deviation from specifications

Any deviation from the requirements of this policy requires prior documented approval by one of the management system officers. In the event of compliance incidents, the Compliance Officer must be involved. In the case of quality issues, the Quality Management Officer shall be involved, and in the case of information security issues, the Information Security Officer shall be involved. The Data Protection Officer must be involved in the decision-making process if the deviation is relevant to data protection.

5. Compliance

The Allgeier Group stands for acting with integrity and ethics as well as for unconditional compliance with the law. This is not only a fundamental matter of course as a listed company, but also crucial in the cooperation with our partners and customers. This guideline represents our commitment to Corporate Social Responsibility (CSR) and the sustainable use of resources. We divide the requirements into four areas.

5.1 Economic responsibility

- Binding requirements for Tier 1 suppliers to pass on standards along the supply chain: For example, we expect our main suppliers to pass on these standards to their own suppliers.
- Decarbonisation: For example, we are actively working to reduce our CO2 emissions and encourage our suppliers to take similar steps.

5.2 Social responsibility

- We expect our suppliers and their supply chain to respect and protect human rights. We reject any form of discrimination or unequal treatment based on race, ethnicity, gender, religion, belief, disability, age or sexual identity. We are committed to gender equality and the elimination of discrimination and violence against women in all aspects of our business. We do not tolerate harassment, bullying or modern slavery (servitude, forced labour or human trafficking). We respect the rights of minorities and indigenous peoples and value the diversity and cultural differences of our employees, customers and stakeholders. We also comply with the law on child labour and young workers, as well as wages and benefits set by law. We also recognise the right to freedom of association and collective bargaining.
- Use of private or public security forces: We make sure that these forces respect human rights and are trained accordingly.
- Animal welfare: For example, we make sure that all animal products come from species-appropriate husbandry.
- Land, forest and water rights and forced evictions: We work to ensure that local communities in the areas where we operate are able to uphold their rights to land and natural resources.

5.3 Environmental responsibility

Environmental expectations require suppliers and their supply chain to act responsibly and consider environmental impacts. This may include:

- Reuse and recycling: We are committed to the reuse and recycling of materials, such as the return of packaging materials for reuse.
- Biodiversity, land use and deforestation: We are committed to protecting biodiversity and avoid business practices that could contribute to deforestation.
- Soil quality: We support practices that protect the soil and maintain its quality for future generations. When chemicals are used, there must be clear guidelines and rules on how to deal with them.
- Noise emissions: We value quiet operations and encourage suppliers to minimise noise levels.

5.4 Governance

- Business ethics: Business ethics expectations require suppliers and their supply chain to be transparent, responsible and ethical in their activities. This includes no corruption or extortion and bribery.Any benefit must be granted transparently, recorded in the business records and audited for tax purposes if necessary.
- Data protection: The protection of privacy and data protection must be guaranteed.
- Antitrust law: Fair competition and compliance with antitrust law as well as the avoidance or minimisation of conflicts of interest.
- Whistleblowing: Whistleblowing should be enabled and protection against retaliation must be ensured.

5.5 Compliance incidents - what happens when it happens?

This can always happen - we inadvertently act in a non-compliant manner. As written above, we always want to live a positive error culture.

Compliance incidents can be:

- a possible violation of legal, in particular criminal or fine law provisions or company regulations
- Impending and ongoing requests for information or investigation proceedings by German authorities
- deliberately committed property damage or financial loss of more than EUR 50 at our expense
- deliberately untruthful reporting of compliance incidents (false suspicion, "blackening")

Compliance incidents or violations are investigated factually and legally and, depending on their relevance, classified as a serious or normal incident. Depending on the classification, certain measures are then taken. Serious violations (e.g. such incidents that already have an effect outside our company) must also be reported to ALLGEIER SE via the Compliance Officer, among others. If there are any suspicions regarding a possible compliance violation, you can confidentially contact the Compliance Officer or your direct AEN contact person.

This does not apply to the following exceptions:

- There is an imminent danger to the public.
- There is a threat of internal retaliation.
- There is no internal reaction to the notice without justification.

We take compliance incidents seriously, clarify them and then take appropriate measures.

Possible compliance incidents must be reported, if necessary to the contact persons named for this purpose (AEN contact person and compliance officer). Anonymity will be maintained in any form at your request. However, we are not bound by your other instructions or wishes. Whistleblowers who report compliance incidents in good faith are protected from reprisals: A whistleblower may not be dismissed, demoted, intimidated or otherwise disadvantaged. Those who support whistleblowers, such as intermediaries, colleagues or relatives, are also protected. However, disciplinary action may be taken on the basis of the whistleblower's own involvement in the incident itself or on the basis of an arbitrary or deliberately untrue denunciation by the whistleblower.

6. Information security and data protection

6.1 Types of information

In order to be able to protect company information, the different types of information in our companies must be classified. The information classification thus forms our basis for handling information. To ensure the secure and careful handling of information, roles for information processing and 3 information classes are defined for the classification of information with regard to their protection requirements.

For all information that is not clearly classified, it must initially always be assumed that this information is to be classified as internal. Before further use, the classification must be determined with the supervisor and or with the information security officer.

6.2 Responsibilities of classification

In order to be able to implement information security, regulations on responsibilities are defined:

Roll	Who has the role?	Tasks
Creator	every employee	- Generates data - Adheres to the company guidelines
Information officer	Supervisor	- Clarifies classification issues with creators - monitors classification process on the part of the creators
User	every employee	- Used data - Adheres to the company guidelines - Provides feedback on grading heights
Classification officer	Information Security Officer	- clarifies classification issues with information officers and users - Monitors the classification process on the part of the technical officers - Coordinates with risk management, data protection and quality management officers

6.3 Information classification and example documents

This table provides an overview of the minimum protection requirements for information. We distinguish between 3 classes of information (public, internal and confidential) and 3 types of use (paper, electronic and oral). The rules of conduct for oral use are shown in Chapter 7 "Proper conduct in public and private settings". In addition, for the types paper and electronic, there are examples of information assigned to the respective category.

Type of use / information classification	public	internal	confidential / <u>strictly confidential</u>
Physical	No special protective measures	Marking with confidential, Clean Desktops, External forwarding in envelopes, Destruction with document shredder security level P-04.	Marking with confidential, Clean Desktops, External forwarding in envelopes, Destruction with document shredder security level P-05
Digital	No special protective measures	Information is accessible to users, depending on the release. For external recipients, a secure transmission (AEN mail server or a shared cloud service) must be used.	information, must additionally be stored internally in encrypted form. For cloud services, ISO27001 must be available. For external transmission, "end-to-end" encryption must be ensured. (e.g. 7-Zip or Panama) Confidential or secret client data is always considered strictly confidential and should, if possible, only be stored on the client system.
Oral	No special protective measures	see chapter 7. correct behaviour in public and in private surroundings	see chapter 7. correct behaviour in public and in private surroundings
Examples	Marketing documents & reference list, job descriptions	Quotations & sales presentations, meeting minutes (no customer data), purchase orders, project P&L info, manuals, guides, policies, staff phone directory, organisational charts, project sign-offs, invoices, role descriptions, contracts (non-personal).	Passwords, personnel and applicant records, problem reports, management evaluations and decisions, financial statements, customer and project data, pre-series devices (prototypes)

6.4 Proper handling of sensitive information when travelling

The mobile devices provided by the company (e.g. laptops, mobile phones, smartphones, tablets, USB sticks, ...) contain the company's own data. Their loss or theft can have damaging effects for the company. Therefore, the following security instructions must be observed:

- As a rule, only take the documents that you actually need with you on business trips.
- When travelling to third countries (e.g. China, USA, Russia), it cannot be ruled out that authorities will access data from end devices upon entry. Therefore, when travelling to such

countries, notebooks provided by the IT administration must always be used without local data availability. Access to the data (e-mails, files) is possible via VPN. Upon return, the notebook must be handed in immediately to the IT administration for checking without access to the company network.

- In the case of smartphones/tablets, the e-mail account must be deleted from the end device before the start of the journey.
- Store only the data you need locally in encrypted form when you are on the road.
- In case of loss or theft of mobile devices, notify your supervisor and the IT department.
- Do not carry mobile devices without password protection.
- Don't give up mobile devices with your suitcase when travelling.
- Never leave documents and mobile devices unattended (e.g. in the car). Temperature fluctuations can also damage not only the hard disk, but also other storage media and the LCD display.
- Pre-series parts/prototypes that are not yet in series production must be protected opaque during transport.

6.5 Proper behaviour in public and private settings

Many business secrets are revealed through thoughtlessness, especially in conversations with colleagues or through telephone conversations in public or private settings (e.g. aeroplane, beer garden, restaurant). Therefore, the following safety instructions must be observed:

- Always be aware of what you are communicating about and where. Ensure confidentiality in all conversations.
- Only disclose information in telephone conversations to personally known business partners.
- If in doubt, check the identity of the caller by calling back.

- On the road, make sure that no one can see what you are working on (e.g. laptop, documents, etc.).
- Do not disclose confidential company information in private conversations.
- Do not have confidential conversations in public (e.g. on planes, in hotels, restaurants).
- Do not transmit confidential information about third parties.
- Never leave mobile devices unattended.
- Do not disclose confidential information over the phone.
- Do not give the company hardware to family members and third parties.
- Make sure that third parties do not use the company hardware.

Even in the case of activities by employees in a private environment, the employer remains responsible for data processing (Art. 4 No. 7 DS-GVO). In order to exercise the control rights of the employer in the handling of personal data, the employee shall grant the management, the data protection officer and the supervisory authority responsible for data protection unrestricted access to the workplace during the normal working hours of the company after prior notification by telephone. The employee shall ensure that any other co-owner of the living space has been informed of this agreement and agrees to the right of access.

6.6 Correct behaviour on the Internet and when using e-mail

Many trade secrets are also revealed through thoughtlessness and the improper use of electronic means of communication. Therefore, the following security instructions must be observed:

- Do not disclose information about client projects on social networks (XING, Facebook or similar).
- Note that when communicating on social networks, a connection with the company can also be established. Therefore, care should be taken to use appropriate language.
- Personal profiles must not contain additions such as "currently working for client XXXX" or similar.
- Only visit trustworthy websites.
- Do not click on links contained in SPAM mails or "chain letters".
- Do not use your company-provided email address in blogs, newsgroups or guest books on the Internet.
- Do not reply to emails requesting personal passwords or PINs.
- If you doubt the sender of the e-mail - do not reply.
- Send only links to documents wherever possible
- Send confidential information via a secure exchange drive or encrypted
- Business e-mail boxes may only be used for business communication and may not be forwarded to external e-mail boxes.
- Even if the employee is absent, it must be possible for the company to access the business e-mails in the mailbox. It is not technically possible to distinguish between business and private correspondence in the business e-mail box. You have the option to delete all private e-mails from the business e-mail box. The employer can also access the e-mail box if you have not deleted all private e-mails.

6.7 Safety zones

A safety zone concept is in place for all locations. There are different safety zones within the respective locations:

Area	Behaviour	Examples
Zone 3 - High security area	Access only in company of persons authorised for security zone 3	- Server rooms, IT administration offices, distribution rooms
Zone 2 - Internal area	Access only in company of persons authorised for security zone 2	- Personnel offices, project offices, finance and legal department offices
Zone 1 - Controlled indoor area	Access is only granted to authorised persons (employees, invited visitors)	- all other rooms of the company
Zone 0 - Outdoor area	No restrictions	- Public areas in a building

6.8 Proper conduct on our business premises

When entering our business premises, the following safety instructions must be observed:

- External persons must register at reception.
- The site-related safety instructions must be observed (e.g. photography ban, protective equipment, etc.).

- Third-party devices may only be connected to the company network after approval.

6.9 Secure storage of information and equipment

The secure storage of information is the basis for the effectiveness of information security. Therefore, the following security instructions must be observed:

- If possible, lock up confidential documents in roll containers, cupboards or safes.
- Lock your computer before leaving the workplace (click "Windows key + L" keys), or always end the session on your computer by "shutting down" and not by "hibernation" or "standby".
- Do not leave documents (especially notes on flip charts or whiteboards etc.) in meeting rooms.
- Never leave confidential work documents unattended on your desk.
- Never leave mobile devices unattended. If possible, notebooks should be secured with a Kensington lock or locked away.
- Pre-series parts/prototypes that are not yet in series production may only be stored in Zone 2 or 3 areas.

6.10 Proper handling of operating resources (assets) and private devices (BYOD)

Confidential company information is often stored on electronic storage and communication media (e.g. notebooks, USB sticks, CDs, DVDs, etc.). In order to protect this information, it is imperative to handle these media securely. Therefore, the following security instructions must be observed:

- Only store confidential data encrypted on mobile storage media.
- When travelling by air, stow your mobile devices in your hand luggage.
- Keep laptops, mobile phones, keys etc. safe, even outside working hours.
- Never leave documents and devices you carry with you visible and unattended (e.g. in the car, train stations, airports, restaurants).
- Never leave mobile devices unattended on your desk.
- Images of confidential information may only be created using an assigned company device.
- Data on mobile devices are not subject to backup (e.g. local laptop hard drive, USB sticks, USB hard drives).
- The use of private hardware or hardware owned/not owned by our company is only permitted after approval by the IT department.
- The use of private devices with photo/video/sound recording functions is prohibited in Zone 2 and Zone 3 areas.
- There are extended requirements for testing and measuring equipment that needs to be calibrated. Please clarify these with your contact person.

6.11 Deletion and destruction of storage media and information

You are responsible for proper destruction as a user of electronic and non-electronic storage and communication media. Company and non-company information does not belong in the waste paper basket, but must be disposed of specifically. For this purpose, use e.g. the document shredders provided near the multifunction printers for disposal and also observe the following safety instructions:

- Delete or destroy confidential information that is no longer needed.
- Dispose of confidential information in paper form only in the "document shredder/shredder" provided for this purpose.

- Cut CDs and floppy disks into the smallest possible pieces if no containers or shredders are available.
- Delete all data (including trash) on your terminals before returning them.

In general, all storage media and information whose content is not public must be deleted according to the following guidelines.

Data carrier type	**Procedure**
Hard disks from notebooks, desktops and servers as well as external hard disks, NAS disks and backup tapes.	Hand in to the IT department for secure deletion/disposal.
Small devices with built-in storage media (smartphones, tablets, cameras, etc..) or memory cards, USB sticks, etc..	Reset to factory settings then hand in to the IT department for reuse or safe disposal.
CDs, DVDs and other optical storage media	Scratching, deleting and handing in to the IT department
Paper and microfilm	Shredding with shredders of security level 4 of DIN 66399
Other data carriers, whether electronic or physical in nature	Reset, destroy or safely erase electronic data carriers; do not destroy electronic data carriers.

6.12 Passwords and Multifactor Authentication

To ensure sufficient access protection, it is imperative that authorised persons with access to the IT systems use secure passwords. Each person authorised to access our systems receives a unique user name assigned to him or her, with which the user is uniquely identified at the respective system. The following password regulations must therefore be observed by every authorised user:

- Start passwords that the authorised users receive as part of the initial registration must be replaced immediately with their own (individual) passwords.
- Passwords must not be written down or left at the workplace.
- Passwords must not be passed on to third parties (including colleagues in the department).
- Logging in with the login data of another user is prohibited.
- When entering passwords, make sure that third parties do not take note of passwords.
- Passwords must have at least 10 characters.
- Passwords must contain at least 3 of the 4 options: an uppercase letter, a lowercase letter, a number and or a special character.
- Trivial passwords must not be used (e.g. qwertz, 12345678, abcdefg).
- The date of birth of the user or his/her relatives may not be used as a password.
- Passwords must be changed independently by the user on a regular basis, but at least every 90 days, or passwords must be changed immediately at the request of the Information Security Officer, if explicitly instructed to do so by the Information Security Officer.
- Passwords must be changed immediately if there is any suspicion that they have been compromised or if the Information Security Officer instructs this change.
- The user name must not be part of the password.
- Passwords must not be stored in the data processing system (e.g. in an Internet browser) without appropriate protection mechanisms.
- Passwords used within the company (network) must not be used for applications on the Internet or in a private environment.
- Passwords may only be stored using a password safe approved by the IT administration.
- In addition to the password, multifactor authentication should always be used where possible.

6.13 Principles for handling personal data

When handling personal data, the following principles must be observed:

- If the principles cannot be or have not been complied with, the data protection coordinator or the data protection officer must be contacted immediately.
- All activities in which personal data are processed must be reported to ims@allgeier-engineering.com.
- All data processing procedures must be made transparent and documented. Every change must be recorded.
- The processing of personal data always requires a legal basis or the verifiable consent of a data subject.
- The data subjects must be informed about the data processing.
- All data processing procedures must be made transparent.
- Personal data may only be used for the purpose for which it was actually collected.
- Only the personal data that are actually required for the performance of the respective task may be processed.
- Personal data must always be collected directly from the data subject.
- Personal data may only be stored for as long as is necessary for the processing activity.
- The possibility of anonymising or pseudonymising personal data must be taken into account.
- Personal data must always be stored or kept protected from access.
- Personal data must be protected against accidental or unintentional loss.
- Requests for information, requests for correction, deletion or transfer of personal data are sent to ims@allgeier-engineering.com and answered by them.

6.14 Behaviour in case of incidents

If you, as an external partner, become aware that the protection or security of information could be compromised in any way, you must immediately contact your internal contact person. This applies in particular if the threat relates to personal data. If you notice that the quality of work could be endangered in any way, contact your supervisor immediately. The behaviour in case of incidents is described in the problem management process.

7. Contact

You can reach us as follows:

Compliance Officer (CO)

Marcus Reimann

Wilhelm-Wagenfeld-Strasse 28 - 80807 Munich

Mail: marcus.reimann@allgeier-engineering.com

IMS Officer (DS,ISB,QMB)

Allgeier Engineering GmbH

Wilhelm-Wagenfeld-Strasse 28 - 80807 Munich

Tel: +49 89 1241487 43

Mail: IMS@allgeier-engineering.com

Data Protection Officer

Ralf Zlamal IITR Regional Partner Baden-Württemberg

Schubertstraße 2

73660 Urbach

Tel. 08918917360

Email: zlamal@iitr.de

Allgeier Ombudsmen (External)

Compliance - Allgeier German

Einsteinstraße 172 - 81677 Munich

Form: Welcome to the Whistleblowing System of the Allgeier SE Group of Companies - Ombudsman & Whistleblowing System (ihre-ombudsstelle.de)