Data Protection Policy

Digital Automotive

Version: 1.1.0

Date: 07.01.2025

Confidentiality: low

Availability: high

Integrity: high

Author: Jürgen Sterr / CTO

Contributors:

- Tobias Kellner / ISB

Interested Parties:

- Sales/DevSecOps/CX
- Customers

Version history

Version	Date	Updated by	Approved by	Changes
1.0.0	10.05.2022	Jürgen Sterr	Erik Reiter	Document was created initially.
1.1.0	07.01.2025	Tobias Kellner	Jürgen Sterr	Added further statements and increased accuracy.

1 Content

2 Data Protection Policy

2.1 Goal

This policy applies to IT Manufactory GmbH and is based on globally accepted basic principles for data protection. The protection of data privacy is a basis for trusting business relationships and the reputation of IT Manufactory GmbH as an attractive employer. IT Manufactory GmbH is committed to international compliance with data protection laws as part of its corporate responsibility. The data protection policy ensures the appropriate level of data protection required by the European data protection policy and national laws for cross-border data traffic, even in countries where no appropriate level of data protection exists by law.

2.2 Area of Effect

This data protection policy applies to IT Manufactory GmbH and its employees. The policy covers all processing of personal data. In countries where data of legal entities are protected in the same way as personal data, this policy also applies to data of legal entities in the same way. Anonymized data, e.g., for statistical analysis or research, is not subject to this policy.

2.3 Validity of state law

This policy is based on data protection principles practiced worldwide without replacing existing national law. It supplements the respective national data protection law. The respective national law shall take precedence if it requires deviations from this policy or imposes more extensive requirements. The contents of this policy must also be adhered to if there is no corresponding national law. The notification obligations for data processing that exist due to state law must be observed. IT Manufactory GmbH is responsible for compliance with this data protection guideline as well as with legal obligations. If it is assumed that legal obligations conflict with the obligations arising from this data protection policy, the data protection officer must be informed immediately.

2.4 General principles

2.4.1 Data minimization and data economy

Before personal data is processed, it must be checked whether and to what extent it is necessary to achieve the purpose intended by the processing. If it is possible to achieve the purpose and the effort involved is proportionate to the intended purpose, anonymized or statistical data shall be used. Personal data may not be retained for potential future purposes unless this is required or permitted by state law.

2.4.2 Confidentiality and data secrecy

Personal data is subject to data secrecy. They must be treated confidentially in personal dealings and secured by appropriate organizational and technical measures against unauthorized access, unlawful processing or disclosure, and accidental loss, alteration, or destruction.

2.4.3 Purpose limitation of the processing of personal

Data may only be used for the purposes that were defined before the data was collected. Subsequent changes to the purposes are only possible to a limited extent and require justification.

2.4.4 Fairness and rightfulness

When processing personal data, the personal rights of the data subject must be respected. Personal data must be collected and processed in a lawful and fair manner.

2.4.5 Transparency

The data subject must be informed about the handling of his or her data. In principle, personal data must be collected from the data subject himself/herself. When collecting the data, the data subject must at least be able to recognize the following or be informed accordingly about:

- The identity of the data controller.
- The purpose of the data processing.
- Third parties or categories of third parties to whom the data may be transferred.

2.4.6 Factual accuracy and data actuality

Personal data must be kept accurate, complete, and up to date. Appropriate measures must be taken to ensure that inaccurate, incomplete, or outdated data is deleted, corrected, supplemented, or updated.

2.4.7 Deletion

Personal data that is no longer required after the expiry of legal or business process-related retention periods must be deleted.

2.5 Permissibility of data processing

Personal data is individual information about the personal and factual circumstances of a specific or identifiable person. This includes information such as your correct first and last name, your address, your telephone, fax, mobile phone number, e-mail address or your birthday and any other data. In contrast, information that is not directly associated with your person, such as the number of users of a website, is not personal data. The collection, processing and use of personal data is only permitted if one of the following permissible circumstances exists. Such an authorization is also required if the purpose for the collection, processing and use of the personal data is to be changed from the original purpose.

2.5.1 Customer data

2.5.1.1 Data processing for a contractual relationship

Personal data of the interested party or customer concerned may be processed for the purpose of establishing, implementing, and terminating a contract. This also includes the support of the contractual partner, insofar as this is related to the purpose of the contract. In the run-up to a contract - i.e., in the contract initiation phase - the processing of personal data is permitted for the

preparation of offers, the preparation of purchase applications or for the fulfilment of other wishes of the interested party directed towards the conclusion of a contract. Interested parties may be contacted during the contract initiation phase using the data they have provided. Any restrictions expressed by the interested party must be observed.

2.5.1.2 Data processing for advertising purposes

If the data subject contacts IT Manufactory GmbH with a request for information (e.g., a request for information material about a product), the data processing is permitted for the fulfilment of this request.

2.5.1.3 Consent to data processing

Data processing may take place based on the consent of the data subject. Before consent is given, the data subject must be informed in accordance with 2.4.5 of this policy. For reasons of evidence, the declaration of consent must always be obtained in writing or electronically. Under certain circumstances, e.g., in the case of telephone consultation, consent may also be given verbally. Its granting must be documented.

2.5.1.4 Data processing based on legal permission

The processing of personal data is also permitted if governmental legal provisions require, presuppose, or permit the data processing. The type and scope of data processing must be necessary for the legally permissible data processing and are based on these legal regulations.

2.5.1.5 Data processing based on legitimate interest

Personal data may also be processed if this is necessary to achieve a legitimate interest of IT Manufactory GmbH. Legitimate interests are usually legal (e.g., enforcement of outstanding claims) or economic (e.g., avoidance of contractual disruptions). Personal data may not be processed based on a legitimate interest if, in an individual case, there is an indication that interests of the data subject that are worthy of protection outweigh the interest in the processing. The interests worthy of protection must be examined for each processing operation.

2.5.1.6 Processing of particularly sensitive data

Personal data requiring special protection may only be processed if this is required by law or the data subject has expressly consented. The processing of such data is also permitted if it is necessary to assert, exercise or defend legal claims against the data subject. If the processing of particularly sensitive data is planned, the data protection officer must be informed in advance.

2.5.1.7 User data and the Internet

If personal data is collected, processed, and used on websites, the data subjects must be informed of this in data protection notices. The data protection notices must be integrated in such a way that they are easily recognizable, directly accessible, and permanently available to the data subjects.

2.5.2 Employee data

2.5.2.1 Data processing for employment

Personal data may only be processed for the employment relationship if it is required for the establishment, implementation, and termination of the employment contract. Personal data of applicants may be processed during the initiation of an employment relationship. After rejection, the applicant's data must be deleted, considering time limits under the law of evidence, unless the applicant has consented to further storage for a subsequent selection process. Consent is also required for the data to be used for further application processes. In an existing employment relationship, data processing must always be related to the purpose of the employment contract, unless one of the following permissible circumstances for data processing applies. If it is necessary to collect further information about the applicant from a third party during the initiation of the employment relationship or in the existing employment relationship, the respective national legal requirements must be taken into account. In case of doubt, the consent of the data subject must be obtained. For processing of personal data that is related to the employment relationship but does not originally serve to fulfil the employment contract, there must be a legal justification in each case. This may be legal requirements, the consent of the employee or the legitimate interests of the company.

2.5.2.2 Data processing based on legal permission

The processing of personal employee data is also permitted if state legal provisions require, presuppose, or permit the data processing. The type and scope of data processing must be necessary for the legally permissible data processing and are based on these legal provisions. If there is legal room for manoeuvre, the employee's interests worthy of protection must be taken into account.

2.5.2.3 Consent to data processing

Employee data may be processed on the basis of the consent of the data subjects. Declarations of consent must be given voluntarily. Involuntary consent is invalid. For reasons of evidence, the declaration of consent must always be obtained in writing or electronically. In exceptional cases, consent may also be given verbally. In any case, the granting of consent must be properly documented. In the case of informed voluntary provision of data by the data subject, consent may be assumed if national law does not require explicit consent. Before consent is given, the data subject must be informed in accordance with 2.4.5 of this policy.

2.5.2.4 Data processing based on legitimate interest

Personal employee data may also be processed if this is necessary to realize a legitimate interest of IT Manufactory GmbH. Legitimate interests are usually based in law (e.g., the assertion, exercise, or defence of legal claims). Personal data may not be processed on the basis of a legitimate interest if there is an indication in the individual case that interests of the employee that are worthy of protection outweigh the interest in the processing. The existence of interest worthy of protection must be examined for each processing operation. Control measures requiring the processing of employee data may only be carried out if there is a legal obligation to do so or if there is a justified reason to do so. Even if there is a justified reason, the proportionality of the control measure must be examined. The legitimate interests of the company in the implementation of the control measure (e.g., compliance with legal provisions and internal company rules) must be weighed against a possible interest of the employee affected by the measure that is worthy of protection in the

exclusion of the measure and may only be implemented if they are appropriate. The legitimate interest of the company and the possible interests of the employee worthy of protection must be determined and documented before any measure is taken. In addition, any further requirements existing under state law (e.g., information rights of the affected persons) must be taken into account.

2.5.2.5 Processing of particularly sensitive data

Personal data requiring special protection may only be processed under certain conditions. Data worthy of special protection are data on racial and ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or the health or sex life of the data subject. On the basis of state law, further data categories may be classified as particularly worthy of protection, or the content of the data categories may be filled out differently. Similarly, data relating to criminal offenses may often be processed only under special conditions established by state law. Processing must be expressly permitted or required by state law. Additionally, processing may be permitted if it is necessary for the controller to comply with its rights and obligations in the area of employment law. The employee may also voluntarily and expressly consent to the processing. If the processing of data requiring special protection is planned, the data protection officer must be informed in advance.

2.5.2.6 Telecommunication and Internet

Telephone systems, e-mail addresses, intranets and the internet are primarily provided by the company as part of its business tasks. They are work equipment and a company resource. They may be used within the framework of the applicable legal provisions and the company's internal guidelines. In the case of permitted use for private purposes, the secrecy of telecommunications and the applicable national telecommunications law must be observed, insofar as these apply. There is no general monitoring of telephone and e-mail communications or of intranet and internet use. In order to defend against attacks on the IT infrastructure or on individual users, protective measures may be implemented at the points of entry into the IT Manufactory GmbH network that block technically harmful content or analyse the patterns of attacks. For security reasons, the use of the telephone systems, e-mail addresses, the intranet and internet, and internal social networks may be logged for a limited period of time. Personal evaluations of this data may only be carried out in the event of a concrete, justified suspicion of a violation of laws or guidelines of IT Manufactory GmbH. These controls may only be carried out by investigating departments in compliance with the principle of proportionality. The respective national laws must be observed as well as the existing regulations of IT Manufactory GmbH in this regard.

2.6 Transmission of personal data

A transfer of personal data to recipients outside of IT Manufactory GmbH or to recipients within IT Manufactory GmbH is subject to the reliability requirements for the processing of personal data under Section 2.5. The recipient of the data must be obligated to use it only for the specified purposes. In the event of a data transfer to a recipient outside of IT Manufactory GmbH in a third country, the recipient must ensure a level of data protection equivalent to this policy. This does not apply if the transfer is based on a legal obligation. Such a legal obligation may result from the law of the country in which the company transferring the data has its registered office, or the law of the country in which the company has its registered office recognizes the objective of the data transfer pursued by the legal obligation of a third country. In the case of data transfer from third parties to companies of IT Manufacturing GmbH, it must be ensured that the data is only used for the intended purposes. If personal data is transferred from a group company with its registered office in the European Economic Area to a group company with its registered office outside the European

Economic Area (third country), the data-importing company is obliged to cooperate with the supervisory authority responsible for the data-exporting company in all inquiries and to comply with the findings of the supervisory authority about the transferred data. The same applies to data transfers by group companies from other countries.

2.7 Commissioned data processing

Commissioned data processing occurs when a contractor is commissioned with the processing of personal data without being assigned responsibility for the associated business process. In these cases, an agreement on commissioned data processing must be concluded both with external contractors and IT Manufactory GmbH. In this case, the commissioning company retains full responsibility for the correct execution of the data processing. The contractor may process personal data only within the scope of the client's instructions. When placing the order, the following requirements must be complied with. The commissioning department must ensure their implementation.

- The contractor shall be selected on the basis of its suitability to ensure the necessary technical and organizational protective measures.
- The order must be placed in text form. The instructions for data processing and the responsibilities of the customer and the contractor must be documented.
- The contract standards provided by the data protection officer must be observed.
- The client must satisfy itself of the contractor's compliance with its obligations before data processing begins. A contractor can demonstrate compliance with data security requirements in particular by submitting suitable certification. Depending on the risk of the data processing, the inspection must be repeated regularly during the term of the contract.
- In the case of cross-border commissioned data processing, the respective national requirements for the transfer of personal data abroad must be met.

2.8 Rights of the data subject

Every data subject can exercise the following rights. Their assertion must be processed immediately by the responsible area and must not lead to any disadvantages for the data subject.

- The data subject may request information about which personal data of what origin is stored about him/her and for what purpose. If the employment relationship provides for further rights of access to the employer's documents (e.g., personnel file) according to the respective employment law, these shall remain unaffected.
- If personal data is transferred to third parties, information must also be provided about the identity of the recipient or the categories of recipients.
- If personal data is incorrect or incomplete, the data subject may request that it be corrected or supplemented.
- The data subject is entitled to demand the deletion of his/her data if the legal basis for processing the data is missing or has ceased to exist. The same applies if the purpose of the data processing has ceased to exist due to the passage of time or for other reasons. Existing retention obligations and interests worthy of protection that conflict with deletion must be observed.
- The data subject has a fundamental right to object to the processing of his/her data, which must be taken into account if his/her interest worthy of protection due to a special personal

situation outweighs the interest in the processing. This does not apply if a legal provision obliges the processing to be carried out.

2.9 Confidentiality of processing

Personal data is subject to data secrecy. Employees are prohibited from unauthorized collection, processing, or use. Any processing carried out by an employee without being entrusted and authorized to do so in the course of performing his or her duties is unauthorized. The need-to-know principle applies. Employees may only have access to personal data if and to the extent that this is required for their respective tasks. This requires the careful division and separation of roles and responsibilities, as well as their implementation and maintenance within the framework of authorization concepts. Employees are not permitted to use personal data for their own private or commercial purposes, to pass it on to unauthorized persons, or to make it accessible to them in any other way. Supervisors must inform their employees of the obligation to maintain data secrecy at the beginning of the employment relationship. This obligation shall continue to apply after termination of the employment relationship.

2.10 Processing safety

Personal data must be protected at all times against unauthorized access, unlawful processing or disclosure, and against loss, corruption or destruction. This applies regardless of whether the data is processed electronically or in paper form. Before introducing new data processing procedures, in particular new IT systems, technical and organizational measures for the protection of personal data must be defined and implemented. These measures must be based on the state of the art of technology, the risks arising from the processing and the need for protection of the data. The technical and organizational measures for the protection of personal data are part of the Group-wide information security management and must be continuously adapted to technical developments and organizational changes.

2.11 Data protection monitoring

Compliance with the data protection guidelines and the applicable data protection laws is regularly checked by means of inspections. The data protection officer or commissioned external auditors are responsible for carrying out these checks. The results of the data protection checks must be reported to the data protection officer. The management shall be informed of significant results within the framework of the respective reporting obligations. Upon request, the results of data protection audits shall be made available to the competent data protection supervisory authority. The competent data protection supervisory authority may also carry out its own checks on compliance with the provisions of this Directive within the scope of its powers under national law.

2.12 Data protection incidents

Each employee shall immediately report to his or her respective supervisor or to the data protection officer in cases of any violation of this data protection Policy or other regulations on the protection of personal data. The responsible manager is obliged to inform the responsible data protection officer immediately of any data protection incidents.

In cases of:

- unlawful transmission of personal data to third parties,

- unlawful access by third parties to personal data or
- loss of personal data,

are the notifications to be made without delay so that existing notification obligations of data protection incidents under state law can be fulfilled.

2.13 Responsibilities and sanctions

The management boards are responsible for data processing in their area of responsibility. As such, they are obliged to ensure that the statutory data protection requirements and those contained in the data protection policy are taken into account (e.g., national reporting obligations). It is a management task of executives to ensure proper data processing in compliance with data protection through organizational, personnel and technical measures. The implementation of these requirements is the responsibility of the employees in charge. In the event of data protection checks by the authorities, the data protection officer must be informed immediately.

2.14 The processing directory

IT Manufactory GmbH must maintain documentation of all processing operations in which personal data is collected, processed, or stored. In close connection with the information security management system, the responsibilities are clearly regulated to compile the required information of the respective department concerned and to send it to the data protection officer. The data protection officer will compile the information and document it in a processing directory in accordance with the requirements of Article 30 of the GDPR. Upon request, the company shall make the documentation available to the responsible supervisory authority. In agreement with the management, the data protection officer is responsible for this and cooperates with the supervisory authority.

2.15 Data protection officer

In accordance with Article 37 of the GDPR, IT Manufactory GmbH has appointed an external full-time data protection officer and integrated him into the corporate culture. The data protection officer, as an external body independent of instructions, works to ensure compliance with national and international data protection regulations.

2.15.1 Duties

- Advice on data protection issues
- Monitoring and compliance with data protection regulations (GDPR, BDSG as well as other legal provisions) as well as the company's own data protection regulations and training of employees.
- Communication with the data protection supervisory authority.
- Contact for data subjects and employees on all processes related to the processing of their data and the exercise of their rights.
- Support of the data controller in establishing processes and documentation for the fulfilment of data protection obligations, support in the obligation to report and notify data protection violations, and fulfilment of the rights of data subjects (right to information, correction, restriction of data processing, and deletion of data).

- Support in the creation of a register of processing activities. The data protection officer is appointed by the management of IT Manufactory GmbH. Any data subject may contact the data protection officer with suggestions, inquiries, requests for information or complaints regarding data protection or data security issues. Inquiries and complaints will be treated confidentially upon request. If the data protection officer is unable to resolve a complaint or remedy a breach of data protection guidelines, he or she must involve the management.

2.15.2 Data protection officer

Detlef Paßberger
Ries 120
DE-94034 Passau

E-Mail: kontakt@p-teck.de
Mobil: +49 (0) 851 / 37 93 01 28

IT Manufactory GmbH
Brunngasse 4, 94032 Passau / Germany
Phone: +49 (0) 800 14 14 14 7
Email: info@digital-automotive-supplier.com
Web: https://digital-automotive-supplier.com