Mercedes-Benz

NP.50.14.110 - Basic Requirements for Information Security

For Contracts with IT Supported Data Processing by Mercedes

1. The Contractor undertakes to effectively secure all information and data which the Contractor collects or processes for the Customer or information to which it has access, in accordance with the applicable current standard of technology against unauthorized access, alteration, destruction or loss, prohibited transmission and any other prohibited processing or other misuse. The Contractor has an appropriate security concept in place for this purpose.
2. The Contractor shall coordinate its security concept with the Customer. In particular, the information security requirements and specifications defined in the requirements specification or in other written specifications shall be observed and taken into account for the security concept. The responsible Information Security Officer of the Customer shall provide support in this regard. The Customer may demand appropriate, periodic written proof of the implementation of and conformity with the security concept. In cases of doubt, the Contractor shall also enable the Customer to carry out an on-site inspection and will provide all necessary information.
3. The Contractor shall designate a contact person endowed with sufficient authority for Security Management who is available for all topics concerning information security, e.g. for Incident Management (Management of Information security incidents).
4. The Contractor must inform the Customer in text form (as per § 126 b BGB) of any significant changes in the processing of the data. Changes are considered to be significant in particular if they relate to the security concept. The notification must contain a description of the scope of the change and the effect on the security concept. In the event of a foreseeable reduction in the protective effect, the approval of the Customer must be obtained in advance in text form (as per § 126 b BGB).
5. The information and data of the Customer may only be used by the Contractor for the contractually agreed purposes and to the extent required for the performance of the contract. In the case of data processing for different customers, the segregation of such data must be verifiably ensured (separation of customers).
6. Access to data processing equipment („DP equipment“) of the Customer or its Contractor may only be granted with the permission of the Customer within the allowed scope that is necessary for the performance of the contract by the persons who are authorized to this end. The Contractor undertakes to not disclose the access authorizations granted to it for the use of the system to any unauthorized persons. The Contractor may only provide subcontractors or freelance staff with access to the DP systems of the Customer within the scope required for the performance of the contract and with the prior approval of the Customer. The Contractor must notify the Customer without delay if any employees of the Contractor, subcontractor or freelance staff with access privileges or access authorizations for DP systems of the Customer, its agents or subcontractors or subcontractors are no longer engaged with the performance of the contractually agreed service, in order to enable the Customer to cancel the existing access privileges or access authorizations.
7. In the case of data transmission and data storage on mobile devices, the Contractor must protect all information of the Customer which is classified as confidential or secret through appropriate cryptographic measures, in accordance with the current standard of technology. In the case of transmission or storage within a secure environment, this is not required. If so requested by the Customer, the Contractor shall prove that the environments where confidential or secret data is processed are designed in accordance with the applicable current standard of technology.
8. The Contractor must notify the Customer without delay of any knowledge or justified suspicion of data protection violations, security breaches and other manipulations of the processing work flow which relate to Mercedes data and services and must in consultation with the Customer - immediately initiate all necessary steps for the clarification of the matter and limitation of the loss.
9. If the data processing takes place onsite at Mercedes or through a data exchange with Mercedes systems, the Contractor shall take appropriate measures to avoid any impairment of Mercedes infrastructure (and of third parties as a result thereof) as required. The Contractor must observe the relevant applicable information security requirements of the Customer.
10. The Contractor shall inform the Customer without delay of any danger that unauthorized persons could access data of Mercedes as a result of seizure, confiscation or other official intervention, in insolvency or settlement proceedings or through any other events or measures. The Contractor shall inform the third parties that data of Mercedes is involved.
11. The Contractor shall inform its employees, subcontractors or freelance staff with access to or access privileges for DP systems of the Customer about relevant topics of information security in relation to the service performance for the Customer on a regular basis.