



These “Instructions regarding credit and debit card data security” are technical and organizational regulations and instructions, which are considered to be binding components of the contractual relationship to Telekurs Multipay. They are therefore to be read and adhered to by the merchant (see section 14.1 of the “General Business Conditions for Cashless Payments” and section 12.4 of the “Special Business Conditions for the Acceptance of Credit Cards in the Absence of the credit card” and in the “Special Business Conditions for the Acceptance of Debit Cards in the Absence of the Debit Card”). Failure to adhere to these regulations represents a contract infraction by the merchant and could result in legal repercussions as established in the General and Special Business Conditions. Specifically, such infractions entitle Telekurs Multipay to immediately terminate the contract relationship and to assert claims for damages resulting from levied by the card organizations and claims for compensation from the card issuer.

To protect merchants, card holders and the entire payment system from losses caused by the misuse of card data, MasterCard and VISA have established security specifications for the processing, transmission and storing of card data. For acceptance of credit or debit cards, the merchant must at least fulfill the following security specifications if he/she does not transmit, process or save any card data. If the merchant does in fact do so, then the “Instructions for merchants concerning compliance with the PCI security regulations”.

<p>Security rules for merchants</p>	<p>All merchants who do not transmit, process or save card data are obligated to at least adhere to the security rules listed in this data sheet.</p> <p>Merchants who transmit, process or save card data on their systems, are additionally obligated to meet the security specifications of the Payment Card Industry Data Security Standards (PIC DSS) (please refer to the leaflet entitled “Instructions for merchants concerning compliance with the PCI security regulations”).)</p>
<p>Service provider, assigned third parties</p>	<p>Telekurs Multipay is to be informed about third parties assigned by the merchant (DSE – Date Storage Entities, such as IT supplies, Payment Service Providers – PSP) that transmit, process or store card data. The merchant is responsible for ensuring that such third parties adhere the security specifications of the Payment Card Industry Data Security Standards (PIC DSS) (please refer to the leaflet entitled “Instructions for merchants concerning compliance with the PCI security regulations”).)</p>
<p>Saving and storing of card data</p>	<p>Only the commercially-relevant portion of the card data may be saved, if any data is to be saved at all: cardholder’s name, card number and the expiry date. Data carriers with such data (e. g. authorization logs, transaction lists, confirmations, car rental contracts, carbon copies, faxes, coupons) are to be stored in a secure environment with limited access.</p> <p>The following data may under no circumstance be stored, <b>not even in an encrypted form:</b></p> <ul style="list-style-type: none"> <li>• The complete contents of any track on the card’s magnetic strip</li> <li>• The card’s verification value (CVC2/CVV2, a three-digit value contained in the signature field on the back of the card)</li> <li>• PIN code</li> <li>• Passwords for cardholder authentication for “MasterCard SecureCode” and “Verified by VISA”.</li> </ul>



Destruction of card data	Sales slips containing card data are to be destroyed after expiration of the retention period as stipulated in the Special Business Conditions (24 months).
Obligation to report security incidents	If unauthorized persons have accessed card data, the merchant must report this to Telekurs Multipay immediately and cooperate with Telekurs Multipay in its investigations. Only through immediate notification can the existing procedures to prevent unauthorized use of the card data be activated. In this way the merchant limits the risk of loss for all participants and any potential loss compensation claims upon him.