



	<p>Personal data is needed from you when you pay by card.</p> <p>This website will provide you with details about the processing of your personal data.</p>		
Question to the customer	<p>Which payment method do you wish to learn more about?</p>		
Options	<p>Payment by direct debit</p> 	<p>Electronic cash ("girocard")</p> 	<p>Other methods of payment by card</p>
<p>General introductory text</p>	<p>When you pay with your card, the merchant collects personal data via their payment terminal. They transmit the data to the network operator.</p> <p>The network operator and the respective payment service providers for the acceptance and settlement of payments (e.g. acquirers) process the data. The processing of personal data takes place in particular to handle payment transactions, prevent card misuse and limit the risk of payment defaults, as well as for legally prescribed purposes such as anti-money laundering and criminal prosecution. For these purposes, your data is also transmitted to other data controllers, such as the bank which issued your card.</p> <p>You will find details on the processing of your personal data below.</p> <p>All references made here to “merchants” refer to the payment recipients. This may be a merchant in the truest sense of the word, but it could also be any other business where you pay with your card, e.g. a restaurant or garage.</p>		
<p>1. Who is responsible for the processing of my data and who can I</p>	<p>Many steps are necessary so that you can safely pay with your card. That is why the merchant you pay by card works with a network operator. The merchant and the network operator are each responsible – as data controllers – for the processing of the data within their own technical area:</p>	<p>Many steps are necessary so that you can safely pay with your card. That is why the merchant you pay by card works with a network operator as well as one or several acquirers. The merchant,</p>	

<p>contact?</p>	<p>a) The merchant for the operation of the payment terminal at the cash desk and possibly for its internal network up to the safe transmission of the data via the Internet or by telephone line to the network operator.</p> <p>You will find the name and contact details of the merchant at the cash desk or at the shop door.</p> <p>b) The network operator for the central operation of the network, the processing carried out in the network, recoding, risk assessment and further transmission. Its contact details are as follows:</p> <p>PAYONE GmbH, Lyoner Straße 9, 60528 Frankfurt am Main, www.payone.com</p> <p>Data Protection Officer: privacy@payone.com</p> <p>Competent data protection authority: The Hesse Data Protection Commissioner, Gustav-Stresemann-Ring 1, 65189 Wiesbaden, https://datenschutz.hessen.de/</p> <p>If the merchant uses a commercial network operator other than PAYONE, the merchant will ensure that its name and contact details are available to you. You can find this information on a notice or by enquiring at the cash desk.</p>	<p>network operator and acquirer are all controllers of the processing of the data, each in their own technical area:</p> <p>a) The merchant for the operation of the payment terminal at the cash desk and possibly for its internal network up to the safe transmission of the data via the Internet or by telephone line to the network operator.</p> <p>You will find the name and contact details of the merchant at the cash desk or at the shop door.</p> <p>b) The network operator for the central operation of the network, the processing carried out in the network, recoding, risk assessment and further transmission. Its contact details are as follows:</p> <p>PAYONE GmbH, Lyoner Straße 9, 60528 Frankfurt am Main, www.payone.com</p> <p>Data Protection Officer: privacy@payone.com</p> <p>Competent data protection authority: The Hesse Data Protection</p>
------------------------	---	--

		<p>Commissioner, Gustav-Stresemann-Ring 1, 65189 Wiesbaden, https://datenschutz.hessen.de/</p> <p>If the merchant uses a commercial network operator other than PAYONE, the merchant will ensure that its name and contact details are available to you. You can find this information on a notice or by enquiring at the cash desk.</p> <p>c) An acquirer is a payment service provider regulated under the Payment Services Supervision Act (ZAG) which performs the acceptance and settlement of payments on behalf of the merchant.</p> <p>Who the acquirer is depends on the card which you used. The merchant will ensure that the acquirer's contact details and those of the data protection authority responsible for the acquirer are available to you. You can find this information on a notice or by enquiring at the cash desk.</p> <p>Where PAYONE is responsible for acquiring, the contact details already</p>
--	--	---

			<p>provided shall apply:</p> <p>PAYONE GmbH, Lyoner Straße 9, 60528 Frankfurt am Main, www.payone.com</p> <p>Data Protection Officer: privacy@payone.com</p> <p>Competent data protection authority: The Hesse Data Protection Commissioner, Gustav-Stresemann- Ring 1, 65189 Wiesbaden, https://datenschutz.hessen.de/</p>
<p>2. What data is used for the payment?</p>	<ul style="list-style-type: none"> • Card data (data which is stored on your card): IBAN or account number and bank sort code, card expiry date and card suffix. • Other payment data: Amount, date, time, identification of the payment terminal (location, company and branch where you are paying), your signature. • In the case of a chargeback: Information about the non-execution of a direct debit by the bank which issued your card or the revocation of a direct debit by yourself, information about the amount due, such as your 	<ul style="list-style-type: none"> • Card data (data which is stored on your card): IBAN or account number and bank sort code, card expiry date and card suffix. • Other payment data: Amount, date, time, identification of the payment terminal (location, company and branch where you are paying), verification data of your card-issuing bank ("EMV data"). • PIN: Your PIN entry is checked by the card-issuing bank after being cryptographically secured. The network operator adopts cryptographic safeguards and 	<ul style="list-style-type: none"> • Card data (data which is stored on your card): Card number, type of card (e.g. VISA, Mastercard, American Express) and expiry date. • Other payment data: Amount, date, time, identification of the payment terminal (location, company and branch where you are paying), verification data of your card-issuing institution ("EMV data"), in some cases your signature. • PIN: Your PIN entry is checked by the card-issuing institution after being cryptographically secured. The network operator adopts

	<p>name, address, bank charges, reminder fees, reason for the chargeback, customer number with your contractual partner (not the nature of your purchases).</p>	<p>transmissions, but does not store the PIN and has no access to the encrypted PIN.</p>	<p>cryptographic safeguards and transmissions, but does not store the PIN and has no access to the encrypted PIN.</p> <ul style="list-style-type: none"> • Chargeback - if you are disputing a transaction performed with your card: In this case, the sales receipt and any other information about you with which the merchant wishes to prove the debt you owe (e.g. name and address) can be forwarded to the card-issuing institution.
<p>3. From what sources is your data derived?</p>	<ul style="list-style-type: none"> • The payment terminal reads the card data from your card. • The other payment data is provided by the payment terminal and in some cases directly by the merchant. • You provide your signature yourself. • To the extent necessary to prevent card misuse and to limit the risk of payment defaults, data is collected from the police KUNO system and from the network operator's in-house databases. • As far as is necessary to handle a 	<ul style="list-style-type: none"> • The payment terminal reads the card data from your card. • The other payment data is provided by the payment terminal and in some cases directly by the merchant. • You enter your PIN yourself. 	<ul style="list-style-type: none"> • The payment terminal reads the card data from your card. • The other payment data is provided by the payment terminal and in some cases directly by the merchant. • You enter your PIN yourself; you provide your signature yourself.

	<p>chargeback, in compliance with the statutory provisions, data is also processed which is taken from publicly accessible sources (e.g. debtor lists) or transmitted by third parties (e.g. the bank which issued your card or a credit agency).</p>		
<p>4. For what purpose is your data processed and on what legal basis?</p>	<ul style="list-style-type: none"> • Merchant: <ul style="list-style-type: none"> ○ Verification and execution of your payment to the merchant, Art. 6 (1) b) GDPR. ○ Archiving of records in compliance with legal obligations, in particular Sections 257 (1) no. 4 Commercial Code (HGB), Section 147 (1) no. 4 Fiscal Code (AO); Art. 6 (1) c) GDPR. ○ Sale of the amount receivable to the network operator by way of factoring, Art. 6 (1) f) GDPR. ○ Communicating an address to the network operator after a chargeback, Art. 6 (1) b) and f) GDPR. 	<ul style="list-style-type: none"> • Merchant: <ul style="list-style-type: none"> ○ Verification and execution of your payment to the merchant, Art. 6 (1) b) GDPR. ○ Archiving of records in compliance with legal obligations, in particular Sections 257 (1) no. 4 Commercial Code (HGB), Section 147 (1) no. 4 Fiscal Code (AO); Art. 6 (1) c) GDPR. • Network operator: <ul style="list-style-type: none"> ○ Verification and execution of your payment to the merchant, Art. 6 (1) b) GDPR. ○ Safe transmission of your data, particularly in accordance with the legal requirements for SEPA payments, Sections 25a Banking 	<ul style="list-style-type: none"> • Merchant: <ul style="list-style-type: none"> ○ Verification and execution of your payment to the merchant, Art. 6 (1) b) GDPR. ○ Archiving of records in compliance with legal obligations, in particular Sections 257 (1) no. 4 Commercial Code (HGB), Section 147 (1) no. 4 Fiscal Code (AO); Art. 6 (1) c) GDPR. • Network operator: <ul style="list-style-type: none"> ○ Verification and execution of your payment to the merchant, Art. 6 (1) b) GDPR. ○ Safe transmission of your data, particularly in accordance with the legal requirements, Sections 25a Banking Act (KWG), 27

	<ul style="list-style-type: none"> • Network operator: <ul style="list-style-type: none"> ○ Verification and execution of your payment to the merchant, Art. 6 (1) b) GDPR. ○ Prevention of card misuse (Section 10 (1) no. 5 Money Laundering Act (GWG)); Art. 6 (1) (c) GDPR. ○ Limitation of the risk of non-payment, Art. 6 (1) f) GDPR. ○ Safe transmission of your data, particularly in accordance with the legal requirements for SEPA payments, Sections 25a Banking Act (KWG), 27 Payment Services Supervision Act (ZAG); Art. 6 (1) c) and f) GDPR. ○ Avoidance of future non-payment through the transmission of chargeback data, should your payment result in a chargeback, Art. 6 (1) f) GDPR. ○ Archiving of records in compliance with legal obligations, in particular Sections 257 (1) no. 4 Commercial Code 	<p>Act (KWG), 27 Payment Services Supervision Act (ZAG); and the regulations of the Association of German Banks; Art. 6 (1) c) and f) GDPR.</p> <ul style="list-style-type: none"> ○ Archiving of records in compliance with legal obligations, in particular Sections 257 (1) no. 4 Commercial Code (HGB), Section 147 (1) no. 4 Fiscal Code (AO); Art. 6 (1) c) GDPR. ○ Settlement of the fees which the merchant owes your card-issuing bank, Art. 6 (1) f) GDPR. ○ Reporting (exclusively masked or pseudonymised as well as with aggregated data), Art. 6 (1) f) DSGVO. 	<p>Payment Services Supervision Act (ZAG), and the regulations of the credit card organisations; Art. 6 (1) c) and f) GDPR.</p> <ul style="list-style-type: none"> • Acquirer: <ul style="list-style-type: none"> ○ Verification and execution of your payment to the merchant, Art. 6 (1) b) GDPR. ○ Prevention of card misuse (Section 10 (1) no. 5 Money Laundering Act (GWG)); Art. 6 (1) (c) GDPR. ○ Limitation of the risk of non-payment, Art. 6 (1) f) GDPR. ○ Safe transmission of your data, particularly in accordance with the legal requirements, Sections 25a Banking Act (KWG), 27 Payment Services Supervision Act (ZAG); and the regulations of the credit card organisations; Art. 6 (1) c) and f) GDPR. ○ Settlement of the fees which the merchant owes your card-issuing institution, Art. 6 (1) f) GDPR. ○ Archiving of records, in particular
--	--	---	---

	<p>(HGB), Section 147 (1) no. 4 Fiscal Code (AO); Art. 6 (1) c) GDPR.</p> <ul style="list-style-type: none"> ○ Debt recovery after a chargeback, Art. 6 (1) b) and f) GDPR. ○ Reporting (exclusively masked or pseudonymised as well as with aggregated data), Art. 6 (1) f) DSGVO. 		<p>in accordance with Sections 257 (1) no. 4 Commercial Code (HGB), Section 147 (1) no. 4 Fiscal Code (AO); Art. 6 (1) c) GDPR.</p> <ul style="list-style-type: none"> ○ Debt recovery after a chargeback, Art. 6 (1) b) and f) GDPR. ○ Reporting (exclusively masked or pseudonymised as well as with aggregated data), Art. 6 (1) f) DSGVO.
5. Who receives the data?	<p>Apart from the merchant and the network operator, other parties require your data in order to carry out the payment or to comply with legal obligations. Your data will only be passed on to this extent, and to the following entities:</p> <ul style="list-style-type: none"> • your card-issuing bank and the merchant's payment service provider • the entities acting as intermediaries on behalf of the German credit industry, which assume the clearing and settlement of payments • judicial authorities in the cases 	<p>Apart from the merchant and the network operator, other parties require your data in order to carry out the payment or to comply with legal obligations. Your data will only be passed on to this extent, and to the following entities:</p> <ul style="list-style-type: none"> • your card-issuing bank and the merchant's payment service provider • the entities acting as intermediaries on behalf of the German credit industry, which assume the clearing and settlement of payments • judicial authorities in the cases 	<p>Apart from the merchant and the network operator, other parties require your data in order to carry out the payment or to comply with legal obligations. Your data will only be passed on to this extent, and to the following entities:</p> <ul style="list-style-type: none"> • the payment card system • your card-issuing institution and the acquirer's bank • the entities acting as intermediaries on behalf of the credit card organisations, which assume the

	<p>provided for by law</p> <ul style="list-style-type: none"> financial intelligence units in the cases provided for by law in the event of a chargeback, in order to find out the address by means of the account number and the bank code (IBAN) of the card used: the card-issuing bank, a credit agency such as SCHUFA Holding AG, or alternatively, the merchant, insofar as the address is known to them Please see section 10 for further details 	<p>provided for by law</p> <ul style="list-style-type: none"> financial intelligence units in the cases provided for by law 	<p>clearing and settlement of payments</p> <ul style="list-style-type: none"> judicial authorities in the cases provided for by law financial intelligence units in the cases provided for by law
<p>6. Is data transferred to a third country or an international organisation?</p>	<p>No, no such transmission takes place.</p>	<p>No, no such transmission takes place.</p>	<p>The acquirer forwards your data to the payment card system outside of the European Economic Area in accordance with the respectively agreed rules (e.g. binding corporate rules, standard contractual clauses) or for the purpose of fulfilling the contract with the foreign payer in order to authorise and carry out your payment.</p> <p>With regard to the processing of your data by the payment card system, please consult its data privacy</p>

			<p>provisions:</p> <ul style="list-style-type: none"> a) MasterCard Europe SPRL, Chaussée de Tervuren 198A, 1410 Waterloo, Belgium, for the payment brands “MasterCard” and “Maestro”, https://www.mastercard.de/de-de/datenschutz.html b) Visa Europe Services LLC, registered in Delaware USA, acting through its branch office in London, 1 Sheldon Square, London W2 6TT, UK, for the payment brands “Visa”, “Visa Electron” and “V PAY” https://www.visa.co.uk/privacy/ c) American Express Payment Services Ltd., Branch Office Frankfurt am Main, Theodor- Heuss-Allee 112, 60486 Frankfurt am Main, for the payment brand “American Express”; www.americanexpress.de/datenschutz d) Diners Club International Ltd., 2500 Lake Cook Road, Riverwoods, IL 60016, USA, for the payment brands “Diners”, “Diners Club” and “Discover”;
--	--	--	--

			https://www.dinersclub.com/privacy-policy e) JCB International Co., Ltd., 5-1-22, Minami Aoyama, Minato-Ku, Tokyo, Japan, for the payment brand “ JCB ”; http://www.jcbeurope.eu/privacy/ f) Union Pay International Co., Ltd., German Branch, An der Welle 4, 60322 Frankfurt, for the payment brands “ CUP ” and “ Union Pay ” http://www.unionpayintl.com/en/aboutUs/companyProfile/contactUs/Europe/Europe2/?currentPath=%2FglobalCard%2Fen%2Fglobal7%2F10050072
7. For what length of time is my data stored?	PAYONE stores and processes your data for as long as is necessary for the performance of the contract and fulfilment of our contractual and statutory obligations. Where storage of the data for the performance of contractual or special statutory obligations is no longer necessary and the purpose of storage no longer applies, the data will be erased, except where its continued processing is necessary for the following reasons: <ul style="list-style-type: none"> • Satisfaction of storage 	PAYONE stores and processes your data for as long as is necessary for the performance of the contract and fulfilment of our contractual and statutory obligations. Where storage of the data for the performance of contractual or special statutory obligations is no longer necessary and the purpose of storage no longer applies, the data will be erased, except where its continued processing is necessary for the following reasons: <ul style="list-style-type: none"> • Satisfaction of storage 	PAYONE stores and processes your data for as long as is necessary for the performance of the contract and fulfilment of our contractual and statutory obligations. Where storage of the data for the performance of contractual or special statutory obligations is no longer necessary and the purpose of storage no longer applies, the data will be erased, except where its continued processing is necessary for the following reasons: <ul style="list-style-type: none"> • Satisfaction of storage

	<p>requirements under commercial law or fiscal law or for other mandatory reasons (e.g. accounting data must be kept for 10 years)</p> <ul style="list-style-type: none"> • Preservation of evidence within the framework of statutory limitation periods 	<p>requirements under commercial law or fiscal law or for other mandatory reasons (e.g. accounting data must be kept for 10 years)</p> <ul style="list-style-type: none"> • Preservation of evidence within the framework of statutory limitation periods 	<p>requirements under commercial law or fiscal law or for other mandatory reasons (e.g. accounting data must be kept for 10 years)</p> <ul style="list-style-type: none"> • Preservation of evidence within the framework of statutory limitation periods
<p>8. What data protection rights do I have?</p>	<p>Every data subject may assert the following data protection rights with the respective data controller (see Section 1 above):</p> <ul style="list-style-type: none"> ○ the right to access pursuant to Article 15 GDPR ○ the right to rectification pursuant to Article 16 GDPR ○ the right to erasure pursuant to Article 17 GDPR ○ the right to restriction of processing pursuant to Article 18 GDPR ○ the right to object pursuant to Article 21 GDPR ○ the right to data portability pursuant to Article 20 GDPR <p>The restrictions set forth in Sections 34 and 35 of the Federal Data Protection Act (BDSG) apply in respect of the right to access and the right to erasure.</p> <p>Additionally, every data subject has the right to lodge a complaint with a supervisory authority for data protection (Art. 77 GDPR in conjunction with Section 19 BDSG). You can find PAYONE's competent supervisory authority for data protection in the context of payment processing in Section 1. Alternatively, you can contact your own local supervisory authority for data protection.</p>		
<p>9. Must I make my</p>	<p>You are neither legally nor contractually obliged to supply your data. If you do not wish to supply your data, you can choose</p>		

data available?	another payment method, such as paying in cash.	
10. Is my data used for automated decision-making?	<p>To prevent card misuse and to limit the risk of payment defaults, maximum amounts are fixed for payments within certain periods of time. The decision also takes into consideration whether a direct debit from your card-issuing bank was previously not honoured due to insufficient funds or revoked by you (chargeback). This information is not included in the decision if the chargeback is made in the context of a revocation declaring the assertion of rights based on the underlying transaction (e.g. due to a material defect in a purchase). This information serves to prevent future payment defaults. Upon complete settlement of outstanding debts, this data is deleted.</p> <p>This information enables the network operator to make recommendations to merchants using its system as to whether or not to accept a direct debit payment. For this purpose, the network operator may</p> <ul style="list-style-type: none"> ○ use chargeback information of all the merchants linked to the network; 	<p>When you wish to use your card for payment, the card payment must first be authorised. This authorisation is given automatically on the basis of your data. The following criteria in particular can play a role: Amount of payment, place of payment, previous payment history, merchant, purpose of payment. Without authorisation, payment by card is not possible. This has no effect on other payment methods (other cards or cash, for example).</p>

	<ul style="list-style-type: none"> ○ for a short time – only a few days – evaluate payment information across multiple merchants in order to prevent card misuse; ○ apart from that, only evaluate payment information received from one and the same merchant. ○ Your data is not used for solvency checks. Your payment data is only used to decide whether or not to recommend payment by direct debit to the respective merchant. 	
11. Right to object in individual cases	<p>You have the right to object at any time, for reasons arising from your particular situation, to the processing of data which takes place pursuant to Article 6 (1) f) GDPR, i.e. to the processing of data based on a balancing of interests.</p> <p>Please direct your objection to: privacy@payone.com</p> <p>If you file a justified objection, your data will no longer be processed pursuant to Article 6 (1) f) GDPR, with two exceptions:</p> <ul style="list-style-type: none"> ○ Your data will continue to be processed if the data controller can prove the existence of compelling reasons for the processing which are worthy of protection and which outweigh your interests, rights and freedoms, in particular, for example, in the case of legal retention obligations and for carrying out a payment which has already been started at the payment terminal but not yet completed. ○ Your data will continue to be processed if this serves to assert, exercise or defend legal claims. 	
12. Information up	30 July 2021	

to date as at	
---------------	--