

Data protection information in accordance with Art. 13, 14 of the General Data Protection Regulation (GDPR) regarding card payments

When you pay by card, personal data is required from you. Here you can find details about the processing of your personal data.

Which payment method would you like to be informed about?			
	Payment by direct debit 	electronic cash ("girocard") 	Credit card
	When you pay with your card, the merchant collects personal data with his payment terminal. He transmits the data to the network operator. The network operator and the respective payment service providers for the acceptance and settlement of payment transactions (e.g. acquirer) further process the data. This is done in particular for payment processing, to prevent card misuse, to limit the risk of payment defaults and for legally prescribed purposes, such as anti-money laundering and criminal prosecution. For these purposes, your data will also be transmitted to other responsible parties, such as your card-issuing bank. Details on the processing of your personal data can be found below. When "merchant" is referred to here, it always means the payee. This can be a merchant in the true sense, but also anyone else where you pay with your card, e.g. a restaurant or a workshop.		
1. Who is responsible for the processing of my data and whom can I contact?	Many steps are necessary so that you can pay securely with your card. The merchant where you pay by card therefore cooperates with a network operator. Merchant and network operator are (separated as follows) independent Controllers for processing in their technical sphere of influence on the data: a) Merchant for the operation of the payment terminal at the checkout and, if applicable, for its internal network up to the secured transmission via Internet or telephone line to the network operator.		Many steps are necessary for you to pay securely with your card. The merchant where you pay by card therefore works with a network operator and with one or more acquirers. The merchant, the network operator and the acquirer are each independent Controllers for the processing of

	You can find the name and contact details of the retailer at the checkout or also on the store door. b) Network operator for central network operation, processing, recoding, risk assessment and further transmission there: Nexi Germany GmbH, Helfmann-Park 7, 65760 Eschborn, Tel. 069 7922 0 Data Protection Officer: DPO-DACH@nexigroup .com Responsible data protection supervisory authority: The Hessian Commissioner for Data Protection and Freedom of Information, Gustav-Stresemann-Ring 1,65189 Wiesbaden	the data within their technical sphere of influence: a) Merchant for the operation of the payment terminal at the checkout and, if applicable, for its internal network up to the secured transmission via Internet or telephone line to the network operator. You can find the name and contact details of the retailer at the checkout or also on the store door. b) Network operator for central network operation, processing, recoding, risk assessment and further transmission there: Nexi Germany GmbH, Helfmann-Park 7, 65760 Eschborn, Tel. 069 7922 0 Data protection officer: DPO-DACH@nexigroup.com Responsible data protection supervisory authority: The Hessian Commissioner for Data Protection and Freedom of Information, Gustav-Stresemann-Ring 1,65189 Wiesbaden c) Acquirer is a payment service provider regulated under the German Payment Services Supervision Act (Zahlungsdienstaufsichtsgesetz, ZAG) that
--	---	--

			performs the acceptance and settlement of payment transactions on behalf of the merchant. Who the acquirer is depends on what kind of card you have used. The merchant will provide you with the contact details of the acquirer and the data protection supervisory authority responsible for the acquirer. You will receive this information via a notice or upon request at the checkout.
2. What data is used for payment?	• Card data (data stored on your card): IBAN or account number and short bank code, card expiry date and card sequence number. • Other payment data: Amount, date, time, payment terminal identifier (place, company and branch where you pay), your signature. • In the event of a returned direct debit: Information about the non-payment of a direct debit by your card-issuing bank or the revocation of a direct debit by you, information about the outstanding debt, e.g. your name, address, bank charges, reminder fees, reason for the return debit note, customer number with your	• Card data (data stored on your card): IBAN or account number and short bank code, card expiry date and card sequence number. • Other payment data: Amount, date, time, payment terminal identifier (location, company and branch where you pay), verification data from your card-issuing bank ("EMV data"). • PIN: Your PIN entry is cryptographically secured and verified by the card-issuing bank. The network operator takes care of cryptographic backups and transmissions, but does not store a PIN and has no access to the encrypted PIN.	• Card data (data stored on your card): Card number, card type (e.g. VISA, Mastercard, American Express) and expiration date. • Other payment data: Amount, date, time, payment terminal identifier (location, company and branch where you pay), verification data of your card-issuing institution ("EMV data"), your signature if applicable. • PIN: Your PIN entry is cryptographically secured and verified by the card-issuing institution. The network operator takes over cryptographic backups and

	contracting party (not the content of your purchases).		transmissions, but does not store a PIN and has no access to the encrypted PIN. • Reversal (Chargeback) - If you dispute a transaction that was made with your card: In this case, the purchase receipt and, if applicable, other information about you that the merchant will use to prove its claim (e.g., name and address) may be disclosed to the card-issuing institution.
3. What are the sources of your data?	• The card data is read from your card by the payment terminal. • The payment terminal and, if necessary, the merchant directly provide the other payment data. • You provide your signature yourself. • To the extent necessary to prevent card misuse and limit the risk of non-payment, data from the KUNO system of the police and from internal databases of the network operator are used. • To the extent necessary for processing the claim arising from a returned direct debit, data taken from publicly accessible sources (e.g. debtor directories) or transmitted by third parties (e.g. your card-issuing bank or a credit reference	• The card data is read from your card by the payment terminal. • The payment terminal and, if necessary, the merchant directly provide the other payment data. • You enter your PIN yourself.	• The card data is read from your card by the payment terminal. • The payment terminal and, if necessary, the merchant directly provide the other payment data. • You enter your PIN yourself, and you provide your signature yourself.

	agency) will also be processed in compliance with the statutory provisions.		
4. For what purpose is your data processed and on what legal basis ?	• Dealers: ○ Verification and execution of your payment to the merchant, Art. 6 (1) (b) GDPR. ○ Document archiving in accordance with statutory provisions, in particular in accordance with §§ 257 (1) No. 4 HGB, § 147 (1) No. 4 AO; Art. 6 (1) (c) GDPR. ○ Sale of the receivable to the network operator by way of factoring, Art. 6 (1) (f) GDPR. • Network operator: ○ Verification and execution of your payment to the merchant, Art. 6 (1) (b) GDPR. ○ Prevention of card misuse (Sec. 10 (1) No. 5 GWG); Art. 6 (1) (c) GDPR ○ Limitation of the risk of non-payment, Art. 6 (1) (f) GDPR. ○ Secure transfer of your data, in particular in accordance with the legal	• Dealers: ○ Verification and execution of your payment to the merchant, Art. 6 (1) (b) GDPR. ○ Document archiving in accordance with statutory provisions, in particular in accordance with §§ 257 (1) No. 4 HGB, § 147 (1) No. 4 AO; Art. 6 (1) (c) GDPR. • Network operator: ○ Verification and execution of your payment to the merchant, Art. 6 (1) (b) GDPR. ○ Secure transmission of your data, in particular in accordance with the legal provisions for SEPA payments, §§ 25a KWG, 27 ZAG; and the provisions of the German Banking Association, Art. 6 (1) (c) and (f) GDPR. ○ Document archiving in accordance with statutory provisions, in particular in accordance with §§ 257 (1) No. 4	• Dealers: ○ Verification and execution of your payment to the merchant, Art. 6 (1) (b) GDPR. ○ Document archiving in accordance with statutory provisions, in particular in accordance with §§ 257 (1) No. 4 HGB, § 147 (1) No. 4 AO; Art. 6 (1) (c) GDPR. • Network operator: ○ Verification and execution of your payment to the merchant, Art. 6 (1) (b) GDPR. ○ Secure transmission of your data, in particular in accordance with the legal provisions, §§ 25a KWG, 27 ZAG, and the provisions of the credit card organization, Art. 6 (1) (c) and (f) GDPR.

	requirements for SEPA payments, §§ 25a KWG, 27 ZAG; Art. 6 (1) (c) and (f) GDPR. ○ Avoidance of future payment defaults by transmitting return debit note data if your payment results in a return debit note, Art. 6 (1) (f) GDPR. ○ Document archiving in accordance with statutory provisions, in particular in accordance with §§ 257 (1) No. 4 HGB, § 147 (1) No. 4 AO; Art. 6 (1) (c) GDPR. ○ Debt recovery after a return debit note, Art. 6 (1) (b) GDPR.	HGB, § 147 (1) No. 4 AO; Art. 6 (1) (c) GDPR. ○ Settlement of fees owed by the merchant to your card-issuing bank, Art. 6 (1) (f) GDPR.	• Acquirer: ○ Verification and execution of your payment to the merchant, Art. 6 (1) (b) GDPR. ○ Prevention of card misuse (Sec. 10 (1) No. 5 GWG); Art. 6 (1) (c) GDPR ○ Limitation of the risk of non-payment, Art. 6 (1) (f) GDPR. ○ Secure transmission of your data, in particular in accordance with the legal provisions, §§ 25a KWG, 27 ZAG, and the provisions of the credit card organization, Art. 6 (1) (c) and (f) GDPR. ○ Settlement of fees owed by the merchant to your card-issuing institution, Art. 6 (1)(f) GDPR. ○ Document archiving, in particular according to §§ 257 para. 1 no. 4 HGB, § 147 para. 1 no. 4 AO; Art. 6 (1) (c) GDPR. ○ Debt recovery after a return debit note, Art. 6 (1) (f) GDPR.
5. Who gets the data?	In addition to the merchant and the network operator, other entities require your data in order to make the payment or to comply with	In addition to the merchant and the network operator, other entities require your data in order to make the payment or to comply with	In addition to the merchant and the network operator, other entities need your data to make the payment or to comply with legal

	legal requirements. Exclusively to this extent, your data will be disclosed to the following entities: • Your card-issuing bank and the merchant's payment service provider • the intermediary bodies set up by the German banking industry to handle the clearing and settlement of payments • Law enforcement authorities in the cases provided by law • Money laundering reporting offices in the cases provided for by law • In the event of a return debit note, to determine the address on the basis of the account number and bank sort code (IBAN) of the card used: the card-issuing bank or alternatively a credit reference agency such as SCHUFA Holding AG. • First Data GmbH, Marienbader Platz 1, 61348 Bad Homburg, Germany	legal requirements. Exclusively to this extent, your data will be disclosed to the following entities: • Your card-issuing bank and the merchant's payment service provider • the intermediary bodies set up by the German banking industry to handle the clearing and settlement of payments • Law enforcement authorities in the cases provided by law • Money laundering reporting offices in the cases provided for by law • First Data GmbH, Marienbader Platz 1, 61348 Bad Homburg, Germany	requirements. Exclusively to this extent, your data will be disclosed to the following entities: • the payment card system • Your card-issuing institution and the acquirer's bank • the intermediary bodies set up by the credit card organizations to handle the clearing and settlement of payments • If applicable, the required card details are transmitted to successors of the original payment service provider in the case of recurring payments. • Law enforcement authorities in the cases provided by law • Money laundering reporting offices in the cases provided for by law • Nexi Croatia d.o.o. , Radnička cesta 50, 10000 Zagreb, Republic of Croatia • Nets Denmark A/S, Klausdalsbrovej 601, DK-2750 Ballerup, Denmark • First Data GmbH, Marienbader Platz 1, 61348 Bad Homburg, Germany
--	--	--	--

6. Is data transferred to a third country or to an international organization?	No, such transmission does not take place.	No, such transmission does not take place.	The acquirer forwards your data to the payment card system (credit card organization) outside the European Economic Area to authorize and execute your payment. Regarding the processing of your data by the payment card system, please refer to its privacy policy: a) MasterCard Europe SPRL, Chaussée de Tervuren 198A, 1410 Waterloo, Belgium, for the "MasterCard" and "Maestro" payment brands, https://www.mastercard.de/de-de/datenschutz.html b) Visa Europe Services LLC, registered in Delaware USA, acting through its London branch, 1 Sheldon Square, London W2 6TT, United Kingdom, for the payment brands "Visa", "Visa Electron" and "V PAY". https://www.visa.co.uk/privacy/ c) American Express Payment Services Ltd., Frankfurt am Main Branch, Theodor-Heuss-Allee 112, 60486 Frankfurt am Main, for the "American Express" payment brand; www.americanexpress.de/datenschutz
--	---	---	--

			d) Diners Club International Ltd, 2500 Lake Cook Road, Riverwoods, IL 60016, USA, for the "Diners", "Diners Club" and "Discover" payment brands; https://www.dinersclub.com/privacy-policy e) JCB International Co, Ltd, 5-1-22, Minami Aoyama, Minato-Ku, Tokyo, Japan, for the payment mark "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%2Fglobal_7%2F10050072 g) Alipay (Europe) Limited S.A; 11-13, Boulevard de la Foire, L – 1528, Luxembourg, for "Alipay" payment brand. https://global.alipay.com/docs/ac/Platform/x1rhufzj
7. How long will my data be stored?	If the data are no longer required for the fulfillment of contractual or legal obligations, they are regularly deleted, unless their (temporary) further processing is necessary for the following purposes:	If the data are no longer required for the fulfillment of contractual or legal obligations, they are regularly deleted, unless their (temporary) further processing is necessary for the following purposes:	If the data are no longer required for the fulfillment of contractual or legal obligations, they are regularly deleted, unless their (temporary) further processing is necessary for the following purposes:

	• Fulfillment of retention obligations under commercial and tax law in accordance with the German Commercial Code (HGB), the German Fiscal Code (AO) and the German Money Laundering Act (GwG). The records are kept for six years in accordance with Section 257 (1) of the German Commercial Code (commercial letters, accounting documents) and for ten years in accordance with Section 147 (1) of the German Fiscal Code (accounting documents, commercial and business letters, documents relevant for taxation). • Return debit data and receivables data are deleted when the receivable has been demonstrably settled.	• Fulfillment of retention obligations under commercial and tax law in accordance with the German Commercial Code (HGB), the German Fiscal Code (AO) and the German Money Laundering Act (GwG). The records are kept for six years in accordance with Section 257 (1) of the German Commercial Code (commercial letters, accounting documents) and for ten years in accordance with Section 147 (1) of the German Fiscal Code (accounting documents, commercial and business letters, documents relevant for taxation). • Return debit data and receivables data are deleted when the receivable has been demonstrably settled.	• Fulfillment of retention obligations under commercial and tax law in accordance with the German Commercial Code (HGB), the German Fiscal Code (AO) and the German Money Laundering Act (GwG). The records are kept for six years in accordance with Section 257 (1) of the German Commercial Code (commercial letters, accounting documents) and for ten years in accordance with Section 147 (1) of the German Fiscal Code (accounting documents, commercial and business letters, documents relevant for taxation). • Return debit data and receivables data are deleted when the receivable has been demonstrably settled.
8. What data protection rights do I have?	Every data subject may assert the following data protection rights with the respective data controller (see point 1. above): ○ the right to information according to Article 15 GDPR ○ the right to rectification according to Article 16 GDPR ○ the right to erasure according to Article 17 GDPR ○ the right to restriction of processing pursuant to Article 18 GDPR ○ the right to object from Article 21 GDPR		

	○ the right to data portability from Article 20 GDPR With regard to the right to information and the right of deletion, the restrictions pursuant to Sections 34 and 35 BDSG apply. Every data subject also has the right to lodge a complaint with a data protection supervisory authority (Article 77 GDPR in conjunction with Section 19 BDSG). In section 1. you will find the competent data protection supervisory authorities for the respective responsible parties in the context of payment processing. Alternatively, you can contact your local data protection supervisory authority.	
9. Do I have to provide my data?	You are under no legal or contractual obligation to provide your data. If you do not want to provide your data, you can use another payment method, e.g. pay cash.	
10. Will my data be used for automated decision making?	To prevent card misuse and limit the risk of payment defaults, maximum amounts are set for payments within certain time periods. The decision-making process also takes into account if a direct debit was previously not honored by your card-issuing bank due to insufficient funds or was revoked by you (returned direct debit). This information is not included in the decision-making process if the return debit note was issued in connection with a revocation of your declared rights arising from the underlying transaction (e.g. due to a material defect in a purchase). The use of this information serves to prevent future payment defaults. With the full settlement of outstanding claims, this data will be deleted. With the help of this information, the network operator can provide recommendations to merchants connected to its system for their decision on whether to accept a direct debit	If you want to use your card for payment, the card payment must first be authorized. Authorization takes place automatically using your data. The following considerations in particular may play a role: Payment amount, place of payment, previous payment history, merchant, payment purpose. Card payment is not possible without authorization. This has no influence on other payment methods (e.g. other cards or cash).

	payment. For this purpose, the network operator may ○ Use chargeback information from all merchants affiliated with it; ○ for a short time - a few days - to prevent card misuse, evaluate payment information even across merchants; ○ furthermore, only evaluate payment information that it has received from the same merchant. ○ Your data will not be used for the purpose of a credit check. Your payment data will only be used to decide whether a direct debit payment is recommended to the respective merchant.	
11. Right of objection in individual cases	You have the right to object at any time, on grounds relating to your particular situation, to the processing of data carried out on the basis of Article 6 (1)(f) GDPR, i.e. the processing of data on the basis of a balance of interests. If you legitimately object, your data will no longer be processed on the basis of Article 6 (1)(f) GDPR, with two exceptions: ○ Your data will continue to be processed insofar as the controller can demonstrate compelling reasons for processing that are worthy of protection and that outweigh your interests, rights and freedoms, in particular, for example, in the case of statutory retention obligations and to execute a payment that has already been started at the payment terminal but has not yet been completed. ○ Your data will be further processed if this serves the assertion, exercise or defense of legal claims.	

