

Information on data processing for interested/contracted parties (merchants) by PAYONE GmbH according to Art. 13 GDPR



PAYONE GmbH (hereinafter: PAYONE) is a full service provider for the processing of cashless payment transactions. We offer our contracting parties (merchants) complete solutions for payments in stationary retail, e-commerce, mobile commerce and in the direct payment sector and consequently create the framework for integrated payment using additional services. Please find below the information required according to Art. 13 General Data Protection Regulation (GDPR) regarding the data processing conducted by PAYONE.

1 NAME AND CONTACT DETAILS OF THE CONTROLLER AND THE DATA PROTECTION OFFICER (DPO)

PAYONE GmbH, Lyoner Str. 15, 60528 Frankfurt/Main, www.payone.com; Managing Directors: Ottmar Bloching, Frank Hartmann, Dr. Matthias Böcker, Roland Schaar, Chairman of the Board: Sven Korschinowski.

Postal address of the DPO: the contact details of the DPO are the same as the above mentioned; please use additionally c/o DPO. Email address of the DPO: privacy@payone.com.

As a payment institution PAYONE is licensed and supervised by the German Federal Financial Supervisory Authority, Graurheindorfer Straße 108, 53117 Bonn, Germany.

2 PURPOSES OF THE PROCESSING

If an interested party approaches us, requests information on PAYONE's services or becomes a contracting party, i.e., enters into a contractual relationship with us, PAYONE shall process personal data (e.g. from contact partners, individual companies). The data processing purposes include:

- Making contact and dispatch of information materials on request;
- Contact initiation and entering into a contractual relationship as well as contract performance (processing of commissioned services);
- Provision of our platforms and service portals, facilitation of use and support;
- Customer care, customer service;
- Newsletter dispatch (subject to separate consent).

The following other purposes of data processing apply as well:

- Fraud prevention, risk management: this includes various measures to prevent and defend against fraud and to hence avoid payment defaults;
- Mandatory verifications according to the law on the tracking of proceeds from serious criminal offences (Money Laundering Act, GwG);
- Detection and prevention of a violation of regulations or applicable conditions of use;
- Credit assessment (check of creditworthiness and financial solvency);
- Accounts receivable management, collection: collection of outstanding receivables via commissioned collection agencies;
- Evaluations for needs-based offers, reporting;
- Protection of the internal IT infrastructure, as well as detection and tracking of cyber-attacks, improvement of services by optimizing user friendliness.

3 LEGAL BASIS OF THE PROCESSING

Where the processing is necessary for the performance of a contract or in order to take steps prior to entering into a contract, the processing is based on Art. 6 (1) (b) GDPR. Provided that a consent is necessary to ensure the processing (e.g., receiving newsletters), the legal basis is Art. 6 (1) (a) GDPR. When required by law, e.g., to conduct mandatory verifications (GwG), the processing is based on Art. 6 (1) (c) GDPR. In all other cases, the processing is based on the legitimate interests of PAYONE or its contractual partners (Art. 6 (1) (f) GDPR). Legitimate interests particularly include the avoidance of payment default (protection against financial and/or economic risk), the monitoring of fulfilling the contractual agreements, as well as cost optimization and improvement of customer service in the mutual interest of the parties

4 CATEGORIES OF PERSONAL DATA PROCESSED BY PAYONE AND ITS SOURCES

PAYONE only stores and processes the personal data that is necessary for providing the specific service. Master and contact data (e.g., name of the interested party, address, telephone number and email address) are required for contacting the data subject. Further information, e.g., on legal representation, authorized parties, beneficial owners, business sector of the company, are required for entering into an agreement. If persons are identified for money laundering purposes, further personal data, such as audio and/or video recordings and identification documents of the person to be identified, are collected. When performing the contract, type and scope of the concrete processed personal data depend on the content and the respective commissioned services. The processed data is generally collected directly from the interested party or contracting partner (merchants). In certain cases and in compliance with the legal requirements, data is collected from external sources (e.g., banking institute managing the account transfers identification data to comply with the GwG, collection of bank information of a general nature or transfer of probability/scoring values from credit agency companies to assess creditworthiness). In order to comply with legal and regulatory requirements (in particular those arising from the German Money Laundering Act (GwG)), identification documents may also be transferred to banks holding fiduciary accounts. If the contract is concluded via a PAYONE cooperation partner (e.g. intermediary, sales partner), the latter may receive data from the contract

and from its execution (e.g. information on contract term, booked products, terminals, etc.) for the purpose of customer service and commission settlement. For further information, please see the respective contract documentation.

5 5 CATEGORIES OF RECIPIENTS OF PERSONAL DATA

Depending on the provided service, PAYONE transfers personal data to the following recipients in order to fulfill its contractual and legal obligations:

- Reliable third parties who carry out or commission the identification under money laundering law;
- Cooperation partners, providing services mediation and/or customer care services;
- Group entities (entities belonging to the DSV- and/or Worldline group);
- Banks, card schemes (including VISA, MasterCard), payment provider (e.g. Alipay);
- Online: web crawling providers, hosting providers, data center operators, tracking service providers;
- E-commerce providers (providers of payment solutions for online shops);
- Value added services providers (e.g., Receipt Hero for digital recipients);
- Clearing agencies, service providers for clearing and settlement;
- Other service providers: including credit agencies for creditworthiness checks and risk assessment, collection agencies, print service providers for invoicing, service providers to hedge the direct debiting process, Service provider for the provision of electronic contract conclusion and video identification;
- Legal authorities (particularly investigative authorities such as the police and the public prosecutor's office) in the event of justified requests.

6 TRANSFERS OF PERSONAL DATA TO THIRD COUNTRIES (I.E., OUTSIDE THE EU/EEA)

Some of the data recipients are located in third countries, i.e., outside the European Union (EU) or the European Economic Area (EEA), where the level of data protection may be lower than within the EU/EEA. PAYONE only transfers personal data to third countries if this is necessary to fulfil contractual obligations, to safeguard legitimate interests or if otherwise required by law. Depending on the service provided, personal data are transferred to the following third countries, among others:

- China, Japan (registered offices of card schemes, payment providers);
- U.S. (registered offices of card schemes, tracking service providers, clearing agencies, service providers for clearing and settlement, IT service providers).

Purposes of the transfer:

- Processing of payment transactions;
- Risk management;
- Provision of corporate IT services;
- Website analysis and marketing tools on websites, social media;
- Marketing and customer loyalty.

To ensure an adequate level of data protection, the data transfer is ensured by a valid adequacy decision issued by the EU Commission or adequate and appropriate guarantees in the form of EU standard contractual clauses or a legal exception applies which justifies data transfers without the existence of an adequacy decision or suitable guarantees (Art. 49 GDPR).

7 DATA RETENTION

Personal data is stored and processed as long as it is necessary for the performance of the contract and for the fulfilment of PAYONE's contractual and legal obligations. If the data is no longer needed for the fulfilment of contractual or specific legal obligations and the purpose of processing has ceased to apply, personal data will be deleted, unless further processing is necessary, such as:

- Complying with legal obligations (e.g., commercial, tax and other legal obligations, e.g., accounting-relevant data has to be stored for 10 years);
- Preservation of evidence within the framework of the statutory limitation period.

8 8 CONTRACTUAL AND/OR STATUTORY OBLIGATION TO PROVIDE PERSONAL DATA

In order to enter into a contractual relationship with PAYONE, you are obliged to provide us with the personal data that is necessary for the performance of the contractual relationship or that we are required to collect by law (e.g., for the purpose of identification in accordance with Sections 4 and 7 GwG). If you do not provide us with this data, PAYONE cannot enter into a contract with you.

9 CREATION OF PROFILES/ PROFILING/ SCORING

PAYONE itself does not create profiles nor performs profiling/scoring for the purpose of evaluating creditworthiness and risk assessments. However, the following service providers (credit agencies) might perform such operations:

- Creditreform Consulting Networks GmbH (CrefoDirect), Hellersbergstraße 11, 41460 Neuss;

**Information on data processing for interested/contracted parties (merchants)
by PAYONE GmbH according to Art. 13 GDPR**



- Bureau van Dijk (BvD), Hanauer Landstraße 175-179, 60314 Frankfurt am Main;
- SCHUFA Holding AG, Kormoranweg 5, 65201 Wiesbaden;
- Creditsafe Deutschland GmbH, Schreiberhauer Straße 30, 10317 Berlin.

If relevant, PAYONE transfers – for purposes of entering into a contractual relationship and/or in specific limited cases – data to the credit agency company to receive an assessment of the creditworthiness. The credit agency company only provides information on the interested party/contracting party when PAYONE credibly demonstrates that in this specific case there is a legitimate interest. When providing this information, the credit agency company can additionally transfer a probability or scoring value calculated from their database to assess the credit risk to PAYONE. The interested/contracting party is entitled to receive information on the information on its person that is accessible by the credit agency company. PAYONE is obliged to provide information to which exact credit agency company the information has been submitted.

10 DATA SUBJECTS RIGHTS

Each data subject, subject to the relevant legal conditions, has the right of access (Art. 15 GDPR), the right to rectification (Art. 16 GDPR), the right to erasure (Art. 17 GDPR), the right to restriction of processing (Art. 18 GDPR), the right to object (Art. 21 GDPR) and the right to data portability (Art. 20 GDPR). In Germany, when asserting the right of access and the right of erasure, Section 34 and 35 of the (new) German Federal Data Protection Act (BDSG) apply, too. If you have provided your consent, the consent may be revoked at any time with future effect. The data subject also has a right to lodge a complaint with a competent data protection supervisory authority (Art. 77 GDPR in conjunction with Section 19 BDSG – the latter for Germany). This right can be exercised, for example, with the supervisory authority responsible for PAYONE: Der Hessische Datenschutzbeauftragte, Gustav-Stresemann-Ring 1, 65189 Wiesbaden, Germany, <https://datenschutz.hessen.de/>.

INFORMATION ON THE RIGHT TO OBJECT

You may object to the processing of your data under the conditions of Art. 21 GDPR at any time, provided that the data processing is based on our legitimate interests or those of a third party (see also Art. 6 (1) (f) GDPR). In this case, we will no longer process your personal data unless we demonstrate compelling legitimate grounds for the processing which override your interests, rights and freedoms, or for the establishment, exercise or defense of legal claims.