

Privacy Policy secupay AG

Table of contents

1.	Privacy Policy secupay AG.....	2
2.	Data controller responsible for processing.....	2
3.	Contact details of the data protection officer	2
4.	Collecting your data.....	2
5.	Purposes and legal bases	3
5.1.	Technical provision of secupay AG websites and secupay services	3
5.2.	Provision of our services.....	3
5.3.	Content Delivery Networks	4
5.4.	Google Web Fonts (local hosting).....	4
5.5.	Real Cookie Banner.....	4
5.6.	Web services.....	4
5.6.1.	Google Analytics and Google Signals.....	5
5.6.2.	Google Tag Manager.....	5
5.6.3.	Google Ads	6
5.6.4.	Google reCAPTCHA	6
5.6.5.	Google Maps	6
5.6.6.	Tracking pixel from Netzeffekt	6
5.7.	secupay AG in social media.....	7
5.7.1.	Facebook	7
5.7.2.	X (Twitter).....	7
5.7.3.	LinkedIn.....	8
5.7.4.	XING	8
5.7.5.	YouTube.....	8
5.8.	Inquiries by email, contact form and phone.....	9
5.9.	Your application with us	9
5.10.	Use of our services and business communication	10
5.11.	Exercising your rights as a data subject.....	10
6.	Disclosure of personal data	11
7.	Is there automated decision-making in individual cases (including profiling)?.....	12
8.	Fraud Prevention with Device Fingerprinting	12
9.	Time limits for storage.....	12
10.	Your rights as a data subject	13
11.	Protection of personal data	15

1. Privacy Policy secupay AG

secupay AG (further referred to as "**secupay AG**" or "**we**") takes the protection of your personal data very seriously. We treat your personal data confidentially and in accordance with the statutory data protection regulations and, in particular, the General Data Protection Regulation ("**GDPR**") and German Federal Data Protection Act ("**BDSG**") as well as this Privacy Policy.

When you visit this website, various personal data is collected. Personal data is data with which you can be personally identified. This Privacy Policy explains what data we collect and what we use it for. It also explains how this is done and for what purpose.

2. Data controller responsible for processing

secupay AG

Goethestrasse 6

01896 Pulsnitz

Phone: +49 (0) 35955 7550-0

Email: info@secupay.com

Represented by the Executive Board Hans-Peter Weber, Katja Hartmann

As the controller, we determine the purposes and means for processing personal data described herein, alone or jointly with others.

3. Contact details of the data protection officer

If you have any questions and/or concerns regarding data protection, you can reach our data protection officer at the following contact details:

Frau Dominika Juszczuk

IBS data protection services and consulting GmbH

Zirkusweg 1

20359 Hamburg

Germany

Email: privacy@secupay.com

4. Collecting your data

First, your data is collected by you providing it to us. This may be, for example, data that you enter in a contact form.

Other data is collected automatically or after your consent when you visit the website via our IT systems. This is mainly technical data (e.g. Internet browser, operating system or time of page view). This data is collected automatically as soon as you enter this website.

5. Purposes and legal bases

5.1. Technical provision of secupay AG websites and secupay services

The processing occurs, for the purpose of providing our websites on the basis of an overriding legitimate interest in accordance with **Art. 6(1)(f) GDPR**. Our legitimate interests are the provision of technically necessary and expressly requested telemedia services, ensuring the security and trouble-free operation of our IT systems, and the assertion, exercise and defence of legal claims.

When you visit our websites, we collect pseudonymized connection data required to display the requested web pages (e.g. IP address, referrer URL, target page, timestamp) and store this data in connection logs (**server log files**) on the web server.

In addition, we store pseudonymized information in your browser in certain cases (**cookies or local storage**) insofar as this is necessary to display our websites or to enable necessary functions on our websites (**technically necessary services or cookies**) such as cookies that are necessary to carry out the electronic communication process or to provide certain functions that you have requested (e.g. for the shopping cart function). The storage of information in your terminal device or the access to information stored there is absolutely necessary in these cases according to **§ 25(2)(2) German Data Protection and Privacy in Telecommunications and Telemedia Act (Gesetz über den Datenschutz und den Schutz der Privatsphäre in der Telekommunikation und bei Telemedien "TTDSG")** in order to provide you with the expressly requested telemedia service.

If you use a contact form provided by us, we collect the data you enter, at the least, the information marked as mandatory. The transmission to the web server is encrypted via https (SSL) and then sent to us by email. In any communication by email, in addition to entered data (message content), connection data (e.g. IP address, mail client, timestamp) and metadata (e.g. size of transmitted data) as well as attachments containing personal data, if applicable, are processed. Emails are always checked for unwanted content (e.g. viruses, spam) through technical means in our IT systems.

You must provide this data without this constituting any legal or contractual obligation. A visit to our websites is not possible or only possible with restrictions without the provision of this information.

5.2. Provision of our services

We process personal data that we receive from you in the course of a business initiation or business relationship in order to carry out our services, the execution of your orders, as well as all activities necessary for the operation and administration of a financial transfer service provider (Art. 6(1)(b) GDPR).

Insofar as it is necessary for the provision of our services, we process data received from other companies or other third parties (e. g. infoscore GmbH) in a permissible manner. In addition, we process personal data that we have obtained and are permitted to process from publicly accessible sources (e. g. debtor directories, land registers, commercial and association registers, the press and other media).

Relevant personal data may in particular be relevant:

- Personal data (name, date of birth, place of birth, nationality and similar data)
- Contact details (address, e-mail address, telephone number and similar data)
- Legitimation data (identification, reporting and comparable data)
- Current accounts and credit card data
- Information about your financial situation (creditworthiness data including scoring, i. e. data for assessing credit risk)
- Data on the use of telemedia offered by us (e. g. time of access to our websites, apps or newsletters, clicked pages of us or entries and comparable data)

5.3. Content Delivery Networks

To provide our website and certain services and features, we use what are known as Content Delivery Networks ("CDN"), which are connected to our website and provide content such as files, images and scripts. It is technically necessary for the external CDN servers to process your IP address and browser-based information to establish a connection between the servers and provide the content.

Insofar as CDN connections are part of a function for the provision of the website or the use of technically necessary web technologies, the purposes and legal bases are identical to the respective technically necessary web technology.

If CDN connections are part of a technically non-essential web service based on your prior consent, the purposes and legal basis are identical to the respective non-essential web technology.

We do not store any information about the connection between our website and the CDN servers. More information about unpkg and Cloudflare's Privacy Policy can be found at unpkg.com as well as cloudflare.com/privacypolicy/.

5.4. Google Web Fonts (local hosting)

This site uses what are known as web fonts for the uniform display of fonts, which are provided by Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland, a subsidiary of Google LLC, 1600 Amphitheatre Parkway Mountain View, CA 94043, USA. The Google Fonts are installed locally.

No connection to Google servers takes place. You can find more information about Google Web Fonts at <https://developers.google.com/fonts/faq> and in Google's Privacy Policy: <https://policies.google.com/privacy?hl=en>.

5.5. Real Cookie Banner

The processing occurs, for the purpose of obtaining, managing and proving your consent to the use of non-essential cookies and web services on the basis of an overriding legitimate interest pursuant to **Art. 6(1)(f) GDPR**. Our legitimate interests are the verifiability of compliance with legal requirements according to **Art. 5(2) GDPR** and the assertion, exercise and defence of legal claims.

When you visit our websites, you can give or subsequently change consent to the web services via an additional interface (Consent Manager). In doing so, we process pseudonymous information (e.g. IP address, timestamp) via the Real Cookie Banner and store your consent in your browser (cookie/local storage) to ensure that only services you have consented to are used. Provider of this technology is [devowl.io](https://www.devowl.io) GmbH, Tannet 12, 94539 Grafing.

The storage of information in your end device or the access to information stored there is strictly necessary in these cases according to **§ 25(2)(2) TTDSG** in order to provide you with the expressly requested telemedia service.

You can see an overview of managed cookies and website services **at the top of this page "Cookies settings"**.

You must provide this data without this constituting any legal or contractual obligation. A visit to our websites is not possible or only possible with restrictions without the provision of this information.

5.6. Web services

The processing is carried out for the purpose of statistically evaluating the interaction of website visitors, for integrating content from other websites as well as for advertising purposes and marketing activities on the basis of your consent in accordance with **Art. 6(1)(a) GDPR**. Pursuant to **Article 7 (3) GDPR**, you

have the right to withdraw any consent you have given for the processing of your personal data at any time with effect for the future. The lawfulness of processing based on your consent pursuant to **Art. 6(1)(a) GDPR** or **Art. 9(2)(a)GDPR** remains unaffected until withdrawal.

If you give us your consent to individual or all web services via the Real Cookie banner, we collect pseudonymous information (e.g. IP address, timestamp) and store it in your browser (cookie/local storage). Subsequently, the third-party providers we use gain access to this data in order to provide the requested web services.

The storage of information in your terminal device or the access to information stored there takes place in these cases in accordance with **§ 25(1) TTDSG** on the basis of your consent.

You are under no legal or contractual obligation to provide this data. A visit to our websites is generally possible without providing this information.

We use the following web services in the Real Cookie Banner, depending on the category:

5.6.1. Google Analytics and Google Signals

This website uses functions of the web analysis service Google Analytics. The provider is Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland, a subsidiary of Google LLC, 1600 Amphitheatre Parkway Mountain View, CA 94043, USA.

Google Analytics allows the website operator to analyze the behaviour of website visitors. In this context, the website operator receives various usage data, such as page impressions, duration of visit, operating systems used and origin of the user. This data is summarized in a user ID and assigned to the respective end device of the website visitor.

Furthermore, Google Analytics allows us to record your mouse and scroll movements and clicks, among other things. Furthermore, Google Analytics uses various modelling approaches to augment the data sets it collects and employs machine learning technologies in its data analysis.

Google Analytics uses technologies that enable the recognition of the user for the purpose of analyzing user behaviour (e.g. cookies or device fingerprinting). The information collected by Google about the use of this website is usually transferred to a Google server in the USA and stored there.

We have enabled Google Signals in Google Analytics. When you visit our website, Google Analytics collects, among other things, your location, search history and YouTube history, as well as demographic data (visitor data). This data can be used for personalized advertising with the help of Google Signals. If you have a Google account, Google Signal's visitor data is linked to your Google account and used for personalized advertising messages. The data is also used to compile anonymized statistics on the user behaviour of our users. We have concluded an order processing contract with Google. The transfer of personal data to Google is based on the adequacy decision (Data Privacy Framework).

The use of this service is based on your consent according to **Art. 6(1)(a) GDPR** and **§ 25(1) TTDSG**. The consent can be withdrawn at any time.

5.6.2. Google Tag Manager

We use the Google Tag Manager. The provider is Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland.

Google Tag Manager is a tool that allows us to embed tracking or statistical tools and other technologies on our website. The Google Tag Manager itself does not create user profiles, does not store cookies and does not perform any independent analyses. It is only used for administering and utilizing the tools integrated via it. However, Google Tag Manager collects your IP address, which may also be transferred to Google's parent company in the United States. The transfer of personal data to Google is based on the adequacy decision (Data Privacy Framework).

The legal basis is your consent according to **Art. 6(1)(a) GDPR**. You can withdraw your consent at any time.

5.6.3. Google Ads

The website operator uses Google Ads. Google Ads is an online advertising programme of Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland. Google Ads allows us to display advertisements in the Google search engine or on third-party websites when the user enters certain search terms on Google (keyword targeting). Furthermore, targeted advertisements can be played on the basis of the user data available at Google (e.g. location data and interests) (target group targeting). As a website operator, we can evaluate this data quantitatively by analyzing, for example, which search terms led to our advertisements being shown and how many ads resulted in corresponding clicks.

The use of this service is based on your consent according to **Art. 6(1)(a) GDPR** and **§ 25(1) TTDSG**. The consent can be withdrawn at any time.

Your data may also be transferred to Google's parent company in the United States. The transfer of personal data to Google is based on the adequacy decision (Data Privacy Framework).

5.6.4. Google reCAPTCHA

We use "Google reCAPTCHA" (hereinafter "reCAPTCHA") on this website. The provider is Google Ireland Limited ("Google"), Gordon House, Barrow Street, Dublin 4, Ireland.

The purpose of reCAPTCHA is to verify whether the data entry on this website (e.g. in a contact form) is made by a human or by an automated program. For this purpose, reCAPTCHA analyzes the behaviour of the website visitor based on various characteristics. This analysis begins as soon as the website visitor agrees to the use of Google reCAPTCHA. For analysis, reCAPTCHA evaluates various information (e.g. IP address, time spent by the website visitor on the website or mouse movements made by the user). The data collected during the analysis is forwarded to Google.

The reCAPTCHA analyses run completely in the background. The storage and analysis of the data is based on **Art. 6(1)(a) GDPR**. Your data may also be transferred to Google's parent company in the United States. The transfer of personal data to Google is based on the adequacy decision (Data Privacy Framework).

5.6.5. Google Maps

This site uses the map service Google Maps. The provider is Google Ireland Limited ("Google"), Gordon House, Barrow Street, Dublin 4, Ireland.

To use the functions of Google Maps, it is necessary to store your IP address. This information is usually transferred to a Google server in the USA and stored there. The transfer of personal data to Google is based on the adequacy decision (Data Privacy Framework). The provider of this site has no influence on this data transmission. If Google Maps is enabled, Google may use Google Web Fonts for the purpose of uniform font display. When you access Google Maps, your browser loads the required web fonts into your browser cache to display text and fonts correctly.

Google Maps is used in the interest of an appealing presentation of our online offers and to make it easy to find the places we indicate on the website. This constitutes a legitimate interest within the meaning of **Art. 6(1)(f) GDPR**. If a corresponding consent has been requested, the processing is carried out exclusively on the basis of **Art. 6(1)(a) GDPR** and **§ 25(1) TTDSG**, insofar as the consent includes the storage of cookies or access to information in the user's terminal device (e.g. device fingerprinting) as defined by the TTDSG. The consent can be withdrawn at any time.

5.6.6. Tracking pixel from Netzeffekt

A tracking process based on the cookie counting pixel from Netzeffekt GmbH, Agnes-Bernauer-Straße 90, 80687 München is used on the website. The purpose is to measure leads and sales. This may involve processing your personal data such as order ID; user hash/click ID; IP address; device identifiers and browser information.

The use of this service is based on your consent in accordance with Art. 6 para. 1 lit. a GDPR and § 25 para. 1 TTDSG. Your consent can be withdrawn at any time.

5.7. secupay AG in social media

The processing occurs, for the purpose of providing our fan pages on social networks (company pages) as well as for marketing purposes on the basis of an overriding legitimate interest in accordance with **Art. 6(1)(f) GDPR**. Our legitimate interests are the support of the social media platforms as well as the presentation of our business activities and the implementation of marketing activities.

If you visit our company page on one of the following social media platforms, we determine the purposes and means together with the platform operators. In terms of data protection, we are joint controllers according to **Art. 26 GDPR**.

We have set a link to the respective pages of social networks. No further data exchange takes place with these pages on our website. When the social media element is active, a direct connection is established between your end device and the provider. The provider thereby receives information about your visit to this website. Insofar as consent has been obtained, the above service is used on the basis of **Art. 6(1)(a) GDPR** and **§ 25 TTDSG**. The consent can be withdrawn at any time.

You are under no legal or contractual obligation to provide us with this information. The use of social networks is independent of the provision of your data, however, contacting us or visiting our profile is not possible without the social network provider providing us with this data.

5.7.1. Facebook

Our fan page on Facebook is provided by Meta Platforms Ireland Ltd, 4 Grand Canal Square, Grand Canal Harbour, Dublin 2, Ireland (Meta).

When you visit our fan page, together with Meta, we process information about you that you provide through your visit (e.g. user name, comments, messages) as well as what are known as page insights (statistical analysis of your visit). The processing by Facebook that takes place after the forwarding is not part of being a joint data controller.

When you visit our page on Facebook, we process the following data:

- Your username,
- Comments you post on our page,
- Messages you write to us via Facebook or Instagram,
- Page Insights (page visits, post volume, country/city our visitor is from, gender statistics).

You can find more information about Page Insights here https://www.facebook.com/legal/terms/information_about_page_insights_data

For the processing of personal data with Page Insights on Facebook and Instagram, the purposes and means of the processing are determined jointly with Meta, so that we are joint controllers according to our agreement ([page controller Addendum](#)) ("Joint Responsibility Agreement").

Further information on data protection at Meta can be found [here](#).

Contacting the data protection officer is possible via this form: <https://www.facebook.com/help/contact/540977946302970>

Your information may also be transferred to Meta's parent company in the United States. The transfer of personal data to Meta is based on the adequacy decision (Data Privacy Framework).

5.7.2. X (Twitter)

Functions of the Twitter service are integrated into this website. The provider is Twitter International Company, One Cumberland Place, Fenian Street, Dublin 2, D02 AX07, Ireland.

If you are logged into your account and visit our profile, Twitter can assign this visit to your user account. However, your personal data may also be collected under certain circumstances if you are not logged in or do not have an account with the respective social media portal. In this case, this data collection takes place, for example, through cookies that are stored on your terminal device or through the collection of your IP address.

Our social media presence on Twitter is designed to ensure the broadest possible presence on the Internet. This is a legitimate interest within the meaning of **Art. 6(1)(f) GDPR**.

You can independently adjust your privacy settings on Twitter in your user account. To do so, click on the following link and log in: <https://twitter.com/personalization>.

Your information may also be transferred to Twitter's parent company in the United States. The transfer of personal data to Twitter is based on the adequacy decision (Data Privacy Framework).

5.7.3. LinkedIn

If you, as a registered user, access our profile on the social network "LinkedIn", follow us or interact with us (e.g. message, comment), LinkedIn Ireland Unlimited Company, Wilton Place, Dublin 2, Ireland ("LinkedIn") processes personal data to provide us with aggregated information ("Page Insights"). No information is provided that allows us to track an individual user's behaviour.

For the processing of personal data for the purpose of providing site insights, we and LinkedIn are joint controllers according to **Art. 26 GDPR**. For more information about the processing of your personal data as a joint controller, please visit the following external link directly from LinkedIn: <https://legal.linkedin.com/pages-joint-controller-addendum>.

In addition, if you as a registered user interact with our profile or posts shared by us (e.g., read, follow, comment) or we access your profile, LinkedIn processes your information as an independent controller (operation of the social network) and shares with us all information that is necessary for the operation of the social network according to LinkedIn's terms of use.

In this case, we collect user data (e.g., name, location), qualification data (e.g., occupation, position, education), and communication data (e.g., message content) directly from you or through the use of LinkedIn's social network.

For more information about LinkedIn's processing of personal data, please visit the following external link: <https://de.linkedin.com/legal/privacy-policy>.

Your data may also be transferred to LinkedIn's parent company – Microsoft Corporation, in the United States. The transfer of personal data to Microsoft is based on the adequacy decision (Data Privacy Framework).

5.7.4. XING

If, as a registered user, you call up our profile on the social network "XING", follow us or interact with us (e.g. message, comment), or we call up your profile, New Work SE, Am Strandkai 1, 20457 Hamburg ("XING") processes your information as an independent controller (operation of the social network) and shares with us all information that is required to operate the social network in accordance with XING's terms of use.

In this case, we collect user data (e.g. name, location), qualification data (e.g. occupation, position, training) and communication data (e.g. message content) directly from you or by using the XING social network.

For more information on the processing of personal data by XING, please refer to the following external link: <https://privacy.xing.com/de/datenschutzerklaerung/druckversion>.

5.7.5. YouTube

Our YouTube channel is provided by Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland, a subsidiary of Google LLC, 1600 Amphitheatre Parkway Mountain View, CA 94043, USA. The transfer of personal data to Google is based on the adequacy decision.

Google operates YouTube as the data controller in terms of data protection. When you view, subscribe, comment, or react to our channel or individual videos, Google collects information about you that you provide through your visit (e.g., username, comments, subscriptions, likes, dislikes to our videos). Google analyzes your response and behaviour in relation to our channel and videos and provides us with statistical information in anonymized form via YouTube Analytics. The provision of this analysis data is carried out by Google as the processor within the meaning of **Art. 28 GDPR**.

This website also embeds videos from YouTube.

We use YouTube in extended data protection mode. According to YouTube, this mode causes YouTube not to store information about visitors to this website before they watch the video. The transfer of data to YouTube

partners, on the other hand, is not necessarily excluded by the extended data protection mode. So, regardless of whether you watch a video, YouTube connects to the Google Double Click network.

As soon as you start a YouTube video on this website, a connection to YouTube's servers is established. This tells the YouTube server which of our pages you have visited. If you are logged into your YouTube account, you enable YouTube to associate your browsing behaviour directly with your personal profile. You can prevent this by logging out of your YouTube account.

Furthermore, YouTube may store various cookies on your end device after starting a video or use comparable recognition technologies (e.g. device fingerprinting). In this way, YouTube can obtain information about visitors to this website. This information is used, among other things, to collect video statistics, improve the user experience, and prevent fraud attempts. If necessary, further data processing operations may be triggered after the start of a YouTube video, over which we have no control.

The basis is consent in accordance with **Art. 6(1)(a) GDPR** and **§ 25 TTDSG**. The consent can be withdrawn at any time.

For more information about privacy at YouTube, please see their Privacy Policy at: <https://policies.google.com/privacy?hl=en>.

5.8. Inquiries by email, contact form and phone

If you send us inquiries by email, telephone or contact form, we will store your data for the purpose of processing the inquiry and in case of follow-up questions. We do not disclose this data without your consent. The processing of this data is based on **Art. 6(1)(b) GDPR**, provided that your request is related to the performance of a contract or is necessary for the implementation of pre-contractual measures. In all other cases, the processing is based on our legitimate interest in the effective handling of the requests addressed to us (**Art. 6(1)(f) GDPR**) or on your consent (**Art. 6(1)(a) GDPR**) if this has been requested; the consent can be revoked at any time.

The data collected from you will remain with us until you request us to erase it, withdraw your consent to store it, or the purpose for storing the data no longer applies (e.g. after we have completed processing your request). Mandatory legal provisions – in particular retention periods – remain unaffected.

To contact us, you are neither contractually nor legally obligated to provide the data. However, the processing of the request is not possible without the communication of certain data about your person (mandatory fields), so that the contact cannot be made without providing this information.

5.9. Your application with us

Processing for the purpose of carrying out application procedures is carried out to decide on establishing an employment relationship and, after the employment relationship has been established, for its implementation in accordance with **§ 26(1) German Data Protection Law (Bundesdatenschutzgesetz "BDSG")**.

In addition, if an application is rejected, processing may be carried out to safeguard overriding legitimate interests in accordance with **Art. 6(1)(f) GDPR**. Our legitimate interest is the assertion, exercise or defence of legal claims.

Insofar as you expressly agree in the case of an unsolicited application or a rejection of the application to store and consider it for a later date, the processing will be based on your consent according to **Art. 6(1)(a) GDPR**. According to **Article 7(3) GDPR** you have the right to withdraw consent you have given for the processing of your personal data at any time. The lawfulness of processing based on your consent pursuant to **Art. 6(1)(a) GDPR** or **Art. 9(2)(a) GDPR** remains unaffected until withdrawal.

When you apply to us, we collect all of your personal data that you provide to us as part of the application. You can apply on your own initiative or on the basis of a job advertisement published by us. Subsequently, we process your personal data in the application process in order to invite you to a personal interview, if applicable, and to decide on establishing an employment relationship. When you use one of our contact forms to apply, we collect the data you enter.

If we are unable to make you a job offer, if you reject a job offer or withdraw your application, we reserve the right to retain the data you have provided on the basis of our legitimate interests (**Art. 6(1)(f) GDPR**) for up to 6 months from the end of the application process (rejection or withdrawal of the application). Subsequently, the data is deleted and the physical application documents are destroyed. The storage serves, in particular, evidence purposes in the event of a legal dispute. If it is evident that the data will be required after the expiration of the 6-month period (e.g. due to an impending or pending legal dispute), the data will only be erased when the purpose for continued storage no longer applies.

It may be stored for a longer period if you have given corresponding consent (**Art. 6(1)(a) GDPR**) or if legal storage obligations oppose the erasure.

In the event that you have consented to the processing of your personal data by our affiliated companies, we will share your data with hp.weber GmbH & Co. POS-cash KG and/or secucard GmbH.

5.10. Use of our services and business communication

The processing for the purpose of providing our services and business communication is carried out for the fulfilment of contracts according to **Art. 6(1)(b) GDPR**, for the fulfilment of legal obligations according to **Art. 6(1)(c) GDPR** as well as for the exercise of overriding legitimate interests according to **Art. 6(1)(f) GDPR**. Our legitimate interests are the performance of the contract, insofar as we have concluded the contract with a third party for whom you are acting, and the assertion, exercise and defence of legal claims. In addition, in certain cases, about which we inform separately, the processing may also be based on your consent according to **Art. 6(1)(a) GDPR** or **Art. 9(2)(a) GDPR**.

If you conclude a contract directly with us as a natural person, we collect all personal data required to establish, perform or terminate the contract. This also applies if you negotiate or conclude a contractual agreement on behalf of another natural person or legal entity.

Insofar as we do not collect the data directly from you, we receive information about your person (name, position), contact data (e.g. email, telephone) and contractual data (e.g. performance obligations) from third parties whom you have named as contact persons or persons responsible for establishing, implementing or terminating the contractual agreement.

For performing the contract, managing the customer relationship, processing requests and providing documentation and billing of services, we process the personal data to the extent necessary. In addition, we process this data to enable appropriate risk management as well as controlling and compliance with other legal requirements (e.g. commercial and tax law) as a legal entity.

As a legal entity, we are obliged to comply with various legal regulations, in particular commercial and tax law. In addition, our activities may also require us to take measures to combat money laundering, to ensure IT security for critical infrastructure, or to assist in audits as a material outsourcing for the purposes of financial supervision.

You are not legally or contractually obligated to provide the personal data. However, without the information requested from us, the use of our services is not possible or only possible to a limited extent.

5.11. Exercising your rights as a data subject

The processing is carried out for the purpose of guaranteeing data subject rights on the basis of the fulfilment of legal obligations according to **Art. 6(1)(c) GDPR** as well as for the exercise of overriding

legitimate interests according to **Art. 6(1)(f) GDPR**. Our legitimate interest is the assertion, exercise and defence of legal claims.

When you contact us to exercise your rights as a data subject, we will collect from you any personal data that you provide to us as part of the request. Alternatively, we may receive the data from third parties if you have instructed someone to assert your rights on your behalf (e.g., deputy, attorney, guardian) or have contacted other agencies in advance (e.g., data protection officer).

We process this data to ensure your identity, to verify the applicability of the respective rights, to implement your rights and to communicate with you.

There is no legal or contractual obligation for you to provide your data. However, without the provision of certain information that enables us to identify you or to implement your rights, it will not be possible to process your request, or only to a limited extent.

6. Disclosure of personal data

At secupay AG, only those persons receive knowledge of personal data if they are responsible for the processing (e.g. administrators, clerks).

Certain activities are not carried out by ourselves, but by contracted service providers as processors according to **Art. 28 GDPR**. These are carefully selected by us, contractually bound and regularly reviewed.

In certain individual cases, we disclose personal data to third parties (e.g. legal advisors, auditors, data protection officers, authorities, courts, our affiliated companies) to the extent necessary for processing and legally permissible.

Transfers to recipients in third countries outside the EU/EEA or to international organizations only take place if this is necessary and legally permissible for the respective processing. In these cases, the transfer is made on the basis of an EU adequacy decision or, in the absence thereof, on the basis of agreed standard contractual clauses or binding internal data protection rules. To the extent that the aforementioned guarantees are not in place, the transfer to third countries outside the EU/EEA is based on an exception according to **Art. 49(1) GDPR** (explicit consent, performance of contract, assertion, exercise or defence of legal claims).

If necessary for the provision of our services, your data will be passed on to the following companies:

- Creditreform Boniversum GmbH
- Concardis GmbH
- infoscore Consumer Data GmbH, Baden-Baden, Germany
- Payone GmbH
- Transact electronic payment systems GmbH
- SIT Solution for IT-Payment GmbH
- HIT Hanseatische Inkasso-Treuhand GmbH
- Bluro GbR ("Serverspot")
- professional bearer of secrets such as Financial Auditors, tax consultants and lawyers
- secucard GmbH
- hp.weber GmbH & Co. POS-cash KG

In the event that the purchase price claim has been assigned to secupay AG, the data may be passed on to the following companies for the purpose of enforcing the purchase price claim:

- Creditreform Dresden Aumüller KG
- Creditreform Munich Ganzmüller, Groher & Kollegen KG

7. Is there automated decision-making in individual cases (including profiling)?

When you use our payment services, we transmit your data (name, address and date of birth) for checking your creditworthiness and verifying your address to the associations Creditreform e. V., Hammfelddamm 13, 41460 Neuss, Creditreform Boniversum GmbH, Hammfelddamm 13, 41460 Neuss, Creditreform München Ganzmüller, Groher & Kollegen KG, Machtlfinger Str. 13, 81379 Munich and Creditreform Dresden Aumüller KG, Augsburger Str. 4, 01309 Dresden.

The legal basis for these transfers is Art. 6 paragraph 1 Letter b of the General Data Protection Regulation.

Information on particularly sensitive data in accordance with Art. 9 General Data Protection Regulation is not processed.

8. Fraud Prevention with Device Fingerprinting

For the purposes of fraud prevention and investigation, the data provided may be used to verify the existence of an atypical payment transaction. In principle, we have a legitimate interest in carrying out such a check. The legal basis for processing is Art. 6 Para. 1 lit. f GDPR.

Therefore we make use of the services of Risk.Ident GmbH, Am Sandtorkai 50, 20457 Hamburg ("Risk.Ident") when operating our services. Risk.Ident collects and processes data using cookies and other tracking technologies to determine the terminal used by the user and other data on the use of our services. The data is not assigned to a specific user. If IP addresses are collected by Risk.Ident, they are immediately encrypted.

The data is stored by Risk.Ident in a database for fraud prevention. Data transmitted by us to Risk.Ident on end devices, which have already been used to (attempted) commit fraud, are also stored in the database. In this respect, too, there is no allocation to specific users. When using our services, we retrieve a risk assessment from the Risk.Ident database to the user's terminal device. This risk assessment of the probability of an attempted fraud takes into account, among other things, whether the terminal device has dialed in via various service providers, whether the terminal device has a frequently changing geo-reference, how many transactions were made via the terminal device and whether a proxy connection is used. The legal basis for processing is Art. 6 Para. 1 lit. f GDPR.

9. Time limits for storage

To ensure the principle of storage limitation according to **Art. 5(1)(e) GDPR**, we store personal data in a form that permits data subjects to be identified only for as long as is necessary for the respective legitimate purposes.

We have set the following storage periods:

- Server log files are stored for 1-30 days depending on the IT system and then automatically deleted;
- Technically necessary cookies are deleted after the end of a session (e.g. closing the browser) or after reaching the specified maximum age (max-age) or manually by the user in the browser;
- Unnecessary cookies are deleted after the specified maximum age (max-age) or manually by the user in the browser.
- Application documents of rejected applicants will be deleted 6 months after rejection without existing consent for permanent storage.

Personal data that must be retained due to commercial or tax regulations in accordance with **§ 147 AO** (German Tax Act), **§ 257 HGB** (German Commercial Code) will not be deleted before 6 years or 10 years have passed. Further storage takes place for the assertion, exercise or defence of legal claims, e.g. in the case of incomplete tax, audit or administrative proceedings.

Personal data that we process for the assertion, exercise or defence of legal claims are generally deleted after 3 years (regular statute of limitations pursuant to **§ 195 BGB** (German Civil Code)); in certain cases (e.g. claims for damages), the statute of limitations is 10 years or 30 years from the date the claim arose pursuant to **§ 199**

BGB, with the maximum storage period being 30 years from the date on which the act, breach of duty or other event that caused the damage occurred.

10. Your rights as a data subject

Right to information

Under the conditions of **Art. 15 GDPR**, you have the right to request confirmation from us as to whether personal data concerning you is being processed. If this is the case, you have the right to information pursuant to **Art. 15(1) GDPR**, including a copy of your data according to **Article 15(3) GDPR**, insofar as the rights and freedoms of other persons are not affected. This includes trade secrets, intellectual property rights or copyrights.

The right to information can be restricted or refused in accordance with **§ 34 BDSG**. In this case, we will inform you of the reasons for the rejection.

Right to rectification

Under the conditions of **Art. 16 GDPR**, you have the right to demand that we immediately correct any inaccurate personal data concerning you and, depending on the purpose of the processing, complete any incomplete data.

Unless this is impossible or involves a disproportionate effort, we will notify all recipients to whom we have disclosed your personal data of the correction. According to **Art. 19(2) GDPR**, you have the right to be informed about these recipients.

Right to erasure

Under the conditions of **Art. 17 GDPR**, you have the right to demand that we erase personal data concerning you without delay. We are obliged to erase your data if one of the reasons according to **Article 17(1) GDPR** applies.

If we have made data relating to you public and an obligation to erase it exists, we shall take appropriate measures in accordance with **Article 17(2) GDPR** to inform other data controllers if you have requested the erasure of all links to this data or of copies and replications.

Unless this is impossible or involves a disproportionate effort, we will notify all recipients to whom we have disclosed your personal data of the deletion. According to **Art. 19(2) GDPR**, you have the right to be informed about these recipients.

The right to erasure exists pursuant to **Article 17(3) GDPR**, insofar as the processing of your personal data is necessary for the reasons stated therein. This applies in particular if the storage of your data is still required due to legal retention obligations (**Art. 17(3)(b) GDPR**) or if your data is needed for the assertion, exercise or defence of legal claims (**Art. 17(3)(e) GDPR**).

The right to deletion also does not exist according to **§ 35(3) BDSG** if the storage of your data is required due to statutory or contractual retention obligations. In addition, the right to erasure may also be restricted pursuant to **§ 35(1) BDSG**. In this case, the processing of your data pursuant to **Art. 18 GDPR** is restricted.

Right to restriction of processing

Under the conditions of **Art. 18 GDPR**, you have the right to demand that we restrict processing if one of the conditions mentioned therein applies.

If the processing of your data has been restricted, your data will continue to be stored in accordance with **Art. 18(2) GDPR**, but will only be processed in a different way if you consent to this or if this is done to assert, exercise or defend legal claims, to protect the rights of another natural or legal person or for reasons of important public interest of the EU or a Member State.

If your data has been restricted, you will receive a notification before the restriction is lifted. Unless it is impossible or involves a disproportionate effort, we will notify all recipients to whom we have disclosed your

personal data of the restriction. According to **Art. 19(2) GDPR**, you have the right to be informed about these recipients.

Right to data portability

Under the conditions of **Art. 20 GDPR**, you have the right to receive the personal data concerning you that you have provided to us in a structured, common and machine-readable format, and you have the right to transfer this data to another controller without hindrance from us, provided that the processing is based on your consent pursuant to **Art. 6(1)(a) GDPR** or a contract pursuant to **Art. 6(1)(b) GDPR** and the rights and freedoms of other natural persons are not affected

Right to object

Under the conditions of **Art. 21 GDPR**, you have the right to object to the processing of your personal data at any time on grounds relating to your particular situation, provided that this is based on our legitimate interest according to **Art. 6(1)(f) GDPR**.

The right of objection according to **Article 21(1) GDPR** does not apply if we demonstrate that we have legitimate grounds for processing that override your interests, rights and freedoms, or if the processing is necessary for the establishment, exercise or defence of legal claims.

Irrespective of this, according to **Article 21 (2) GDPR**, you have the right to object at any time to the processing of your data for the purpose of direct marketing, including profiling in connection with direct marketing. In this case, we will no longer process your data for the purpose of direct marketing.

Withdrawal of consent

If the processing of your personal data is based on your consent pursuant to **Art. 6(1) GDPR**, you have the right to withdraw your consent at any time with effect for the future pursuant to **Art. 7(3) GDPR**.

Automated decision making according to Art. 22 GDPR

According to **Article 22(1) GDPR**, you have the right not to be subject to a decision based solely on automated processing – including profiling – where this produces legal effects concerning you or similarly significantly affects you.

We do not process personal data by means of automated decision-making in individual cases, including profiling according to **Art. 22(1), (4) GDPR**.

Right to complain according to Art. 77 GDPR

Without prejudice to any other administrative or judicial remedy, you have the right to lodge a complaint with a supervisory authority pursuant to **Art. 77 GDPR** if you consider that the processing of your personal data infringes the GDPR. You may contact any supervisory authority, in particular in the Member State of your habitual residence, place of work or place of the alleged infringement, including the supervisory authority responsible for us – Sächsische Datenschutz- und Transparenzbeauftragte, Devrientstraße 5, 01067 Dresden, <https://www.datenschutz.sachsen.de/>.

11. Protection of personal data

We have implemented a comprehensive information security programme that includes technical and organizational measures to secure and protect your information. In particular, we use the following security measures to help protect your personal information from unauthorized access, disclosure, use or alteration:

- Encryption of personal data
- You can recognize an encrypted connection by the fact that the browser address bar changes from "http://" to "https://" and by the lock symbol in your browser bar. If SSL or TLS encryption is activated, the data you transmit to us cannot be read by third parties.
- Storage of important information such as passwords after their encryption
- Countermeasures against hacker attacks
- Creation and implementation of the internal safety management plan
- Installation and operation of an access control system
- Measures to prevent the falsification or modification of access data

Nevertheless, due to ever-changing technology and other factors beyond our control, we cannot guarantee that communications between you and our servers will be free from unauthorized access by third parties or that we will not be affected by security breaches.

This Privacy Policy is effective as of 05.12.2023 and supersedes all previous versions.