

SOFORT's Open Banking Privacy Notice

Please note that this is a convenience translation only, and that this version does not take precedence over the local language version of this Privacy Notice.

This translation does not, for example, take into consideration national-specific rights you may have under laws in your country of residence, or national-specific legal bases for a particular processing. Please consult the local language version for this, or contact us via the contact information listed below in section 12.

It is important to us that you feel safe when you use our SOFORT Open Banking services (see a full description of the services below). Therefore, we are providing all the information about how we use your personal data in this privacy notice.

1. Who is responsible for your personal data and to which does this Privacy Notice apply?

Sofort GmbH, registered with the Munich Local Court under HRB 218675, with its registered office at Theresienhöhe 12, 80339 Munich, Germany (“**SOFORT**”, “**we**”, “**our**” or “**us**”), is responsible for the processing of your data in accordance with the EU General Data Protection Regulation (the “**GDPR**”). SOFORT is part of the Klarna Group. You can find more information about SOFORT at www.sofort.de. If you have any questions about the processing of your personal data or would otherwise like to contact us for one of the reasons listed below, please send an e-mail to our data protection team on datenschutz@sofort.com.

This Privacy Notice applies to the Open Banking services we provide to you, which include Payment Initiation Services, Account Information Services and Identity Services (as defined below, together, the “**SOFORT's services**”).

“**Payment Initiation Service**” or “**PIS**” means an online service, also known as “*SOFORT Bank Transfer*” or “*Sofortüberweisung*”, that enables you to initiate a payment order at your request with respect to a payment account held and chosen by you at another payment service provider, usually your online bank or other account holding financial institution (the “**Financial Institution**”). We will send your payment order to such Financial Institution for execution, receive information from such Financial Institution regarding whether the payment order has been accepted and (where relevant) pass this information on to the recipient of the payment (usually the partner you chose and are

interacting with in the context of this transaction). For the avoidance of doubt, the Payment Initiation Service is limited to allowing you to initiate a payment in favour of a dedicated Recipient chosen by you.

What SOFORT does when you're using our PIS: SOFORT is the provider of the PIS to you and in relation to your Financial Institution. When a transaction is initiated by logging into your financial account in our user flow and us accepting to proceed with the transaction, SOFORT checks whether or not your payment account is available with the Financial Institution. If the answer is affirmative, we forward your payment initiation request to your Financial Institution by way of electronic transfer for execution by the Financial Institution, and inform you as well as the Recipient chosen by you whether the payment was successfully initiated or not.

“Account Information Service” or “AIS” means an online service that enables us on your request to collect from your Financial Institution(s) consolidated information on one or more payment accounts held by you with such Financial Institution(s) and to provide such information to a Recipient chosen by you. This information is generally collected by us or, as the case may be, the Recipient to supply you with Additional Services or other tailored services, such as providing tailored financial advice or financial aggregated information.

What SOFORT does when you're using our AIS: SOFORT is the provider of the AIS to you and in relation to your Financial Institution. When a transaction is initiated by logging into your financial account in our user flow and us accepting to proceed with the transaction, SOFORT collects as per your request the data and information requested by the Recipient chosen by you directly from your financial account (such as balance, transaction history, etc.) and transfers such collected data and information to such a Recipient.

“Identity Service” means an online service, also known as *“SOFORT Ident”* that enables us or a Recipient on your request to identify you, to verify your identity and/or to collect identity data provided by you. On your request we may share the result of such identification and/or identity verification as well as relevant identity data with the Recipient chosen by you. We may also use such information for our own purposes, e.g. to fulfil our customer due diligence requirements in accordance with applicable AML laws.

What SOFORT does when you're using our Identity Service: SOFORT is the provider of the Identity Service to you which usually combines SOFORT's services and Third Party Services (as defined below). When a transaction is initiated by logging into your financial account in our user flow and us accepting to proceed with the transaction, SOFORT performs general customer due diligence measures on you in accordance with applicable AML laws. This includes without being limited to offering you an identification and identity verification method to collect and verify your identity data (e.g. by combining our PIS and AIS with Third Party Providers' qualified electronic signature and Fotoldent) as well as performing sanction screening and PEP screening in relation to you. On your request, we may allow a Recipient chosen by you to rely on us for all or parts of such general

customer due diligence measures and share the underlying data and information including your identity data and attributes with such Recipient.

“**Additional Services**” are services provided by us that are based on a PIS, an AIS and/or an Identity Service, such as enhancing received data and information, visualising consolidated account information via an app or adding authentication services. Such Additional Services will be described to you separately, e.g. in the app you use or the relevant user flow, and be initiated on your order together with or in the context of a PIS, AIS or Identity Service. Additional privacy notices from us may apply to all or parts of the Additional Services and you will be able to take notice thereof in the relevant user flow.

“**Third Party Services**” are services provided by third parties (the “**Third Party Providers**”) that may be involved in the context of SOFORT’s services (e.g. an app provider, a foto-ident provider or a trust services provider). Such Third Party Providers will act under their own responsibility, at your request only and independently from us. However, we may help you to communicate with such Third Party Providers via our user flows with you and receive data and information in relation to you from such Third Party Providers. E.g. in the context of a Payment Initiation Service the payment itself will be executed by your Financial Institution, in the context of an Account Information Service the visualisation of your account information may be done by an app provider or in the context of the Identity Service the collection of data may be done by a foto-ident provider and the creation of the qualified electronic signature will be provided by a trust services provider. Additional privacy notices from such Third Party Providers may apply to the Third Party Services and you will be able to take notice thereof in the relevant part of the user flow.

2. Your data protection rights as a data subject

You have several rights under the GDPR related to you having control of your personal data and to receive information directly from us on how we process personal data about you. In the following you can read about your rights. If you want to know more or come in contact with us to exercise your rights, the easiest way is to email us on datenschutz@sofort.com. If you want to receive information about the data SOFORT holds about you through so-called subject access, or have certain data deleted, you can send a request to us at the above-mentioned e-mail address.

Your rights

Right to have personal data deleted (“Right to be forgotten”).

In some cases, you have the right to have us delete personal data about you. For example you can request us to delete such personal data that we (i) no longer need for the purpose it was collected for, or (ii) that we process based on your consent and you revoke your consent. There are situations

where SOFORT is unable to delete your data, for example, when the data is still necessary to process for the purpose for which the data was collected, SOFORT's interest to process the data overrides your interest in having them deleted, or because we have a legal obligation to keep it. You can read more about our legal obligations to keep data in section 4 and 9 in this Privacy Notice. The laws described there prevent us from immediately deleting certain data. You also have the right to object to us using your personal data for certain purposes such as direct marketing, which you can read more about in this list of your rights.

Right to be informed.

You have the right to be informed of how we process your personal data. We do this through this privacy notice, by service-specific FAQs, and by answering your questions.

Right to receive access to your personal data (“Subject access”).

You have the right to know if SOFORT processes personal data about you, and to receive a copy (“data extract”) of such data, so-called subject access. Through the data extract you will receive information about what personal data SOFORT holds about you and how we process it.

Right to access, and request a transfer, of your personal data to another recipient (“Data portability”).

This right means that you can request a copy of the personal data relating to you that SOFORT holds for the performance of a contract with you, or based on your consent, in a machine-readable format. This will allow you to use this data somewhere else, for example to transfer your personal data to another controller/recipient.

Right to rectification.

You have the right to request that we rectify inaccurate information or complete information about you that you consider is inaccurate or incomplete.

Right to restrict processing.

If you believe that your personal data is inaccurate, that our processing is unlawful or that we do not need the information for a specific purpose, you have the right to request that we restrict the processing of such personal data. You also have the possibility to request that we stop processing your personal data while we assess your request. If you *object* to our processing per your right described directly below, you may also request us to restrict processing of that personal data while we make our assessment.

Right to object against our processing of your personal data.

You have the right to object to processing of your personal data which is based on our legitimate interest (Article 6(1)(f) GDPR), by referencing your personal circumstances. You can also always object to our use of your personal data for direct marketing purposes. When you let us know that you no longer wish to receive direct marketing from us, we will turn off marketing for you, and stop sending it to you.

Right to object to an automated decision that significantly affects you.

You have the right to object to an automated decision made by SOFORT if the decision produces legal effects or significantly affects you in a similar way. See section 6 on how SOFORT makes use of automated decisions.

Right to withdraw one's consent.

As described in section 5 below, where we process your personal data based on your consent or explicit consent, you have the right to revoke that consent at any time. When you revoke your consent we will stop processing your data for such purposes.

Right to lodge a complaint.

If you have complaints about SOFORT processing of your personal data, you can lodge a complaint with the competent data protection authority.

3. What kind of personal data do we collect?

In this section, we describe the types of personal data that we collect or create. In section 4, we describe for what purposes we use these types of personal data.

Contact and identification data - Name, place of birth, date of birth, social security number, title, gender, address, e-mail address, mobile phone number, nationality, age, audio recordings, photos and video recordings of you and your ID card etc.

Information about goods/services - Details concerning the goods/services you have bought or ordered, such as type of item, use case or context provided to us by the Partner (see also under section 7) chosen by you in the context of our Services.

Information about your financial standing - Information about, for example, your income, any credits, negative payment history and previous credit approvals.

Payment information - Bank account number, bank name.

Information about your use of SOFORT's services - Which service(s) and what different functions in these services you have used and how you have used them. This includes information about outstanding and historical debt, your payment history, and your personal preferences.

Technical information generated through your use of SOFORT's services - Technical data such as response time for web pages, transaction errors and date and time when you used the service.

Information about your contacts with SOFORT's customer service - Recorded phone calls, chat conversations and email correspondence.

Your contacts with the Partners chosen by you in the context of our services - Information about how you interact with such Partner, the use case you use our services for, your contact and identification data.

Device information - Device ID, IP address, language settings, browser settings, time zone, operating system, platform, screen resolution and similar information about your device and device settings/usage.

Information from external sanction lists and PEP lists - Sanction lists and lists of persons constituting politically exposed persons ("PEP") include information such as name, date of birth, place of birth, occupation or position, and the reason why the person is on the list in question.

Special category data - Special category data are data that reveal religious beliefs, political or philosophical views, trade union membership, or constitute information about health, sex life or sexual orientation as well as biometric data.

Service-specific personal data - Within the framework of our Services, we use additional personal data that are not covered by the types listed above. Information regarding each service is listed here:

(i) **Payment Initiation Service** - Financial information including financial account and transaction data, such as account holder, IBAN/BIC/account number, remitted amount, transaction reference etc.), and verification data (whether the sum of the bank balance on the one hand and the overdraft

limit on the other hand covers the amount to be transferred. In addition, we can collect and store a User-ID generated by us and allocated to your online-banking access (e.g. user number, contract number) in a shortened version as so-called “hash value”.

(ii) **Account Information Service** - Financial information including financial account and transaction data, such as available financial accounts, chosen financial account(s), account holder, IBAN/BIC/account number, client number, account balance, overdraft limit, pending transfers, account history (i.e. historical transactions), amounts, counterparty of specific transactions etc.

(iii) **Identity Service** - Financial Information (as for PIS/AIS above), sensitive personal data including biometric data, copies of ID documents, data and information from ID documents, as well as data from Third Party Services, such as eID, qualified electronic signatures, Fotoldent or Videoldent procedures etc., including any underlying data and information collected by the Third Party Providers for the purpose of providing their Third Party Services, which may include ID documents and/or biometric data.

4. What personal data are used for what purposes and with which legal basis?

In the tables below you can read about,

1. what we will use your personal data for (the purpose),
2. which types of personal data we use for that purpose, and if the personal data comes directly from you or from another source. In the cases where we have received personal data about you from another source, we provide the name of that source in brackets,
3. what legal rights we have under current data protection legislation, such as the GDPR, to process the data about you, referred to as our “legal basis”, and
4. when SOFORT stops using the personal data for each purpose.

4.1. Purposes for which your personal data is *a/ways* used, regardless of the service you use.

Purpose of the processing - what we do and why.	Type of personal data used for the purpose, and where they come from (the source). See section 3 to read more about the	Legal basis for processing according to the GDPR.	When the purpose of using the personal data ends. See section 9 for when SOFORT deletes the data.
--	--	--	--

different types of personal data.

To manage our customer relationship with you in accordance with our agreements, for each service you use. This includes creating and sending information to you in electronic format (not marketing).

From you:

- Contact and identification data.
- Payment information.
- Special category data.

From other sources:

- Information about goods/services. (The Partner)
- Information about your financial standing. (SOFORT and credit information bureaus)
- Information about your use of SOFORT's services. (SOFORT)
- Technical information generated through your use of SOFORT's services. (SOFORT)
- Your contacts with the Partner in the context of SOFORT's services. (The Partner)

The processing is necessary for SOFORT to perform a contract with you (Article 6(1)(b) GDPR).

If the service processes information that constitutes sensitive personal data (e.g., from materials you choose to upload), our processing takes place based on your explicit consent (Article 9(2)(a) GDPR).

When the contract between you and SOFORT terminates.

- Device information. (Your device)
- Service-specific personal data (see section 3).

To be able to perform customer satisfaction surveys and market surveys as well as ask for reviews from you, through email, text messages, phone or via other communication channels. If you do not want us to perform this processing, please contact us to let us know. See section 2 for more information about your rights. See section 12 for our contact information.

From you:

- Contact and identification data.
- Information about your use of SOFORT's services.

From other sources:

- Information about goods/services. (The Partner)
- Information about your use of SOFORT's services. (SOFORT)
- Technical information generated through your use of SOFORT's services. (SOFORT)
- Your contacts with the Partner in the context of SOFORT's services. (The Partner)

The processing is based on a balancing of interests (Article 6(1) (f) GDPR). When balancing interests, SOFORT has determined that we have a legitimate interest in being able to perform the personal data processing, that the processing is necessary to achieve that purpose, and that our interest outweighs your right not to have your data processed for this purpose. You may contact us for more information about how the determination was made. See section 12 for our contact information. For calls, we process your personal data based on your explicit consent.

When the contract between you and SOFORT terminates.

To ensure network and information security in SOFORT's services.

From you:

- Contact and

The processing is based on a balancing of interests (Article 6(1)

This processing lasts for as long as you are using a service.

<p>identification data.</p> <p>From other sources:</p> <ul style="list-style-type: none"> • Information about your use of SOFORT's services. (SOFORT) • Technical information generated through your use of SOFORT's services. (SOFORT) • Your contacts with the Partner in the context of SOFORT's services. (The Partner) • Device Information. (Your device) 	<p>(f) GDPR). When balancing interests, SOFORT has determined that we have a legitimate interest in being able to ensure network and information security, that the processing is necessary to realise that purpose, and that our interest outweighs your right not to have your data processed for this purpose. It is also in your interest as a customer that we ensure good information security. You may contact us for more information about how the determination was made. See section 12 for our contact information.</p>
---	---

To be able to help you as a vulnerable customer (i.e. if you need extra support when contacting us due to particular circumstances). This means that we can offer you special support, for example, when you contact customer service.

- From you:
- Contact and identification data.
 - Special category data (in the form of biometric data processed solely to identify you).
- From other sources:
- Information about your use of

Based on your consent (Article 6(1)(a) and Article 9(2)(a) GDPR).

When you notify us that you are no longer a vulnerable customer or withdraw your consent. We also cease this processing if and when you notify us that you no longer want to be a SOFORT customer.

SOFORT's services.
(SOFORT)

To be able to perform risk analysis, prevent fraud, and carry out risk management. We perform the processing to confirm your identity and that the data you provide is correct, as well as to counter criminal activities. This processing constitutes profiling and automated decision-making. We use automated decision-making for this purpose, to be able to determine if you constitute a risk of fraud. See section 6 for more information about profiling and automated decisions.

- From you:
- Contact and identification data.
 - Payment information.
- From other sources:
- Information about goods/services. (The Partner)
 - Information about your financial standing. (SOFORT and credit information bureaus)
 - Information about your use of SOFORT's services. (SOFORT)
 - Technical information generated through your use of SOFORT's services. (SOFORT)
 - Your contacts with the Partner in the context of SOFORT's services. (The Partner)
 - Device information. (Your device)

The processing is necessary for SOFORT to be able to execute and perform a contract with you (Article 6(1)(b) GDPR). We are also required by law to establish the identity of our customers (Article 6(1)(c) GDPR). (The German Money Laundering Act (*Geldwäschegesetz - GwG*)). Special category data are processed based on your explicit consent.

This processing will take place while you use any SOFORT service. If SOFORT has identified a risk in how you use SOFORT, we will continue to use your information for this purpose and continuously update our risk assessment if there is a risk of fraud. This processing lasts as long as we are required by law to keep your information. See section 9 for more information on our obligations and right to retain information according to law.

- Special category data.

To perform data analysis for product development and testing to improve our risk and credit models and to design our services (if possible, we first anonymise the data, which means that no personal data processing is performed thereafter).

From you:

- Contact and identification data.
- Payment information.

From other sources:

- Information about goods/services. (The Partner)
- Information about your financial standing. (SOFORT and credit information bureaus)
- Information about your use of SOFORT's services. (SOFORT)
- Technical information generated through your use of SOFORT's services. (SOFORT)
- Your contacts with the Partner in the context of SOFORT's services. (The Partner)
- Device information. (Your device)

The processing is based on a balancing of interests (Article 6(1) (f) GDPR). When balancing interests, SOFORT has determined that we have a legitimate interest in performing data analysis for product development and testing purposes. We ensure that the processing this entails is necessary to achieve the purpose of the processing, and that our interest outweighs your right not to have your data processed for this purpose. Furthermore, our customers benefit from the processing because it helps us deliver error-free and sustainable services. You may contact us for more information about how the determination was made. See section 12 for our contact information.

This processing takes place for the entire period during which SOFORT must retain the information in its systems, for example, to perform the contract executed with you or to comply with applicable law. See section 9 for more information on our obligations and right to retain information according to law.

- Service-specific personal data (see section 3).

<p>To produce statistics and reports for economic analysis or analysis of payment trends or payment volumes in certain regions or industries (if possible, we first anonymise the data, which means that no personal data processing takes place thereafter).</p>	<p>From you:</p> <ul style="list-style-type: none"> • Contact and identification data. • Payment information. <p>From other sources:</p> <ul style="list-style-type: none"> • Information about goods/services. (The Partner) • Information about your financial standing. (SOFORT and credit information bureaus) • Information about your use of SOFORT's services. (SOFORT) • Your contacts with the Partner in the context of SOFORT's services. (The Partner) • Service-specific personal data (see section 3). 	<p>The processing is based on a balancing of interests (Article 6(1)(f) GDPR). When balancing interests, SOFORT has determined that we have a legitimate interest in obtaining statistical data and reports for this purpose. We ensure that the processing this entails is necessary to achieve the purpose of the processing, and that our interest outweighs your right not to have your data processed for this purpose. You may contact us for more information about how the determination was made. See section 12 for our contact information.</p>	<p>This processing takes place for the entire period during which SOFORT must retain the information in its systems, for example, to perform the contract executed with you or to comply with applicable law. See section 9 for more information on our obligations and right to retain information according to law.</p>
---	---	--	---

To check and verify your identity.

- From you:
- Contact and identification data.

The processing is necessary for SOFORT to perform a contract with you (Article 6(1)(b) GDPR).

As long as you use one of SOFORT's services.

<p>To share your personal data with the categories of recipients described in section 7.1 (suppliers and subcontractors, companies within the Klarna Group, persons with authority over your financial transactions, authorities and buyers of receivables, businesses or assets).</p>	<ul style="list-style-type: none"> • All types mentioned in section 3. 	<p>Varies depending on the recipient (see section 7.1).</p>	<p>This processing takes place for the entire period during which SOFORT must retain the data in its systems, for example, to fulfil the agreement with you or to comply with applicable law. See section 9 for more information on our obligations and right to retain information according to law.</p>
<p>To decide what kind of marketing we will provide to you.</p>	<p>From you:</p> <ul style="list-style-type: none"> • Contact and identification data. 	<p>The processing is based on a balancing of interests (Article 6(1) (f) GDPR). When</p>	<p>If you notify us that you are not interested in this processing.</p>
<p>If you do not want us to perform this processing of your data, please contact us. We will then cease to use your data for marketing. Contact information is available in section 12.</p>	<p>From other sources:</p> <ul style="list-style-type: none"> • Information about goods/services. (The Partner) • Information about your use of SOFORT's services. (SOFORT) 	<p>balancing interests, SOFORT has determined that we have a legitimate interest in identifying which type of marketing we should provide to you. We ensure that the</p>	
<p>The processing may constitute profiling. See section 6 for more information about profiling.</p>	<ul style="list-style-type: none"> • Technical information generated through your use of SOFORT's services. (SOFORT) • Your contacts with the Partner in the context of SOFORT's services. (The Partner) 	<p>processing this entails is necessary to pursue that interest, and that our interest outweighs your right not to have your information processed for this purpose. We have also considered the fact that marketing is listed as an example of legitimate interest in the GDPR.</p>	

- Device information. (Your device)
 - Service-specific personal data (see section 3).
- You may contact us for more information about how the determination was made. See section 12 for our contact information.

<p>If you agree, provide you with information about our products or services, and about deals offered in cooperation with our partners. If you do not want to receive marketing from us, you can opt-out anytime.</p>	<p>From you:</p> <ul style="list-style-type: none"> • Contact and identification data. <p>From other sources:</p> <ul style="list-style-type: none"> • Information about your use of SOFORT's services. (SOFORT) • Your contacts with the Partners in the context of SOFORT's services. (The Partners) 	<p>The processing is based on your consent (Article 6(1)(a) GDPR).</p>	<p>When you unsubscribe or if you notify us that you are not interested in this processing.</p>
---	---	--	---

<p>To provide marketing materials and offers to you about other products and services we offer that are similar to those you have already used and that are part of SOFORT general consumer offering. If you do not want to receive marketing from us, please contact us to let us know. We will then stop processing your data for sending marketing. See section</p>	<p>From you:</p> <ul style="list-style-type: none"> • Contact and identification data. <p>From other sources:</p> <ul style="list-style-type: none"> • Information about your use of SOFORT's services. (SOFORT) • Your contacts with the Partners in the context of SOFORT's services. (The Partner) 	<p>The processing is based on a balancing of interests (Article 6(1) (f) GDPR). When balancing interests, SOFORT has determined that we have a legitimate interest in sending you marketing about our services and offers. We ensure that the processing this entails is necessary to pursue that interest, and that our interest outweighs your right not to have</p>	<p>When the contract between you and SOFORT terminates, or if you notify us that you are not interested in this processing.</p>
--	--	--	---

12 for our contact information.

your data processed for this purpose. We have also considered the fact that marketing is listed as an example of legitimate interest in the GDPR.

You may contact us for more information about how the determination was made. See section 12 for our contact information.

To protect SOFORT from legal claims and safeguard SOFORT's legal rights.

- All types mentioned in section 3.

In the event of a dispute, SOFORT may also collect other types of personal data concerning you if we need them to exercise our rights.

The processing is based on a balancing of interests (Article 6(1) (f) GDPR). When balancing interests, SOFORT has determined that we have a legitimate interest in being able to protect ourselves from legal claims. We ensure that the processing this entails is necessary to achieve the purpose of the processing, and that our interest outweighs your right not to have your data processed for this purpose.

You may contact us for more information about how the determination was made. See section 12

This processing takes place for the entire period during which SOFORT must retain the information in its systems, for example to perform the contract executed with you or to comply with applicable law. See section 9 for more information on our obligations and right to retain information according to law.

for our contact information.

4.2. Purposes for which your personal data is used when you use PIS and/or AIS.

Purpose of the processing - what we do and why.	Type of personal data used for the purpose, and where they come from (the source). See section 3 to read more about the different types of personal data.	Legal basis for processing according to the GDPR.	When the purpose of using the personal data ends. See section 9 for when SOFORT deletes the data.
To share your personal information with the categories of recipients described in section 7.2 (Partners, financial institutions, fraud prevention agencies and companies providing identity information and credit information bureaus).	From you: <ul style="list-style-type: none">• Contact and identification data.• Payment information.• Special category data. From other sources: <ul style="list-style-type: none">• Information about goods/services. (The Partner)• Information about your financial standing. (Financial Institutions and credit information bureaus)• Information about your use of SOFORT's services. (SOFORT)	Varies depending on the recipient (see section 7.2).	Primarily when the payment initiation takes place or when we retrieve your account information, but it also occurs during the entire period that SOFORT has the data in its systems, i.e. until the data is deleted. See section 9 for more information on our obligations and right to retain information according to law.

- Technical information generated through your use of SOFORT's services. (SOFORT)
- Your contacts with the Partner in the context of SOFORT's services. (The Partner)
- Device information. (Your device)
- Information from external sanction lists and PEP lists. (Sanction lists and PEP lists)
- Special category data. (Financial institutions, Trust services providers or (other) identity attribute providers, PEP lists)
- Service-specific personal data. (see section 3 for information about SOFORT's Services)

To prevent SOFORT's operations from being used for money laundering or terrorist financing, by monitoring and

From you:

- Contact and identification data.
- Payment information.

To comply with law (Article 6(1)(c) GDPR). (The German Money Laundering Act (*Geldwäschegesetz - GwG*)).

When the agreement between you and SOFORT is terminated. See section 9 for more information on our

reviewing transactions. SOFORT also conducts ongoing risk assessments and creates risk models to counter money laundering and terrorist financing.

This processing constitutes profiling and automated decision making. See section 6 for more information about profiling and automated decisions.

- Special category data.
From other sources:
- Information about goods/services.
- Information about your financial standing. (SOFORT and credit information bureaus)
- Information about your use of SOFORT's services. (SOFORT)
- Technical information generated through your use of SOFORT's services. (SOFORT)
- Your contacts with the Partner in the context of SOFORT's services. (The Partner)
- Device information (Your device)
- Information from external sanction lists and PEP lists. (Sanction lists and PEP lists)
- Special category data. (Financial institutions, Trust

As regards sensitive personal data, the basis is that the processing is necessary for reasons of the public interest (Article 9(2)(g) GDPR). However, if you have supplied us with sensitive personal data, it is processed based on your explicit consent.

obligations and right to retain information in accordance with the law.

services providers or (other) identity attribute providers, PEP lists)

- Service-specific personal data (see section 3 for information about SOFORT's Services).

To perform a fraud prevention assessment before providing SOFORT's services is accepted. This processing constitutes profiling and automated decision-making. We use automated decision-making for this purpose, to be able to determine if you constitute a risk of fraud. See section 6 for more information about profiling and automated decisions. Also see section 7.2.3 on our use of fraud prevention agencies to which your information may be shared, and our legal basis for that sharing.

From you:

- Contact and identification data.
- Payment information.

From other sources:

- Information about goods/services. (The Partner)
- Information about your use of SOFORT's services. (SOFORT)
- Technical information generated through your use of SOFORT's services. (SOFORT)
- Your contacts with the Partner in the context of SOFORT's services. (The Partner)

To enter into and perform the agreement (Article 6(1)(b) GDPR).

When the fraud assessment is performed.

- Device information.
(Your device)

In addition to the above, SOFORT receives information from fraud prevention agencies on whether your information indicates an attempt at fraud.

From you:

- Contact and identification data.
- Payment information.

From other sources:

- Information about goods/services. (The Partner)
- Information about your use of SOFORT's services. (SOFORT)
- Information about your contacts with SOFORT's customer service. (SOFORT)
- Your contacts with the Partner in the context of SOFORT's services. (The Partner)

To comply with law (Article 6(1)(c) GDPR). (The German Accounting Rules).

During the period in which the bookkeeping is recorded and for as long as required in accordance with German Accounting Rules. See section 9 for more information on our obligations and right to retain information according to law.

To perform bookkeeping and accounting in accordance with accounting laws and preserve them in compliance with the applicable law.

4.3. Purposes for which your personal data is used when you use Identity Services.

<p>Purpose of the processing – what we do and why.</p>	<p>Type of personal data used for the purpose, and where they come from (the source). See section 3 to read more about the different types of personal data.</p>	<p>Legal basis according to the GDPR.</p>	<p>When the purpose of using the personal data ends. See section 9 for when SOFORT deletes the data.</p>
<p>To share your personal information with the categories of recipients described in section 7.2 (Partners, financial institutions, fraud prevention agencies and companies providing identity information, credit information bureaus, trust services providers and (other) identity attribute providers.</p>	<p>From you:</p> <ul style="list-style-type: none"> • Contact and identification data. • Payment information. • Special category data. <p>From other sources:</p> <ul style="list-style-type: none"> • Information about goods/services. (The Partner) • Information about your financial standing. (Financial Institutions and credit information bureaus) • Information about your use of SOFORT’s services. (SOFORT) • Technical information generated through your use of SOFORT’s services. (SOFORT) 	<p>Varies depending on the recipient (see section 7.2).</p>	<p>Primarily when identifying you or when we are verifying your identity, but it also occurs during the entire period that SOFORT has the data in its systems, i.e. until the data is deleted. See section 9 for more information on our obligations and right to retain information according to law.</p>

- Your contacts with the Partner in the context of SOFORT's services. (The Partner)
- Device information. (Your device)
- Information from external sanction lists and PEP lists. (Sanction lists and PEP lists)
- Special category data. (Financial institutions, Trust services providers or (other) identity attribute providers, PEP lists)
- Service-specific personal data. (see section 3 for information about SOFORT's Services)

To prevent SOFORT's operations from being used for money laundering or terrorist financing, by monitoring and reviewing transactions. SOFORT also conducts ongoing risk assessments and creates risk models to counter money

From you:

- Contact and identification data.
- Payment information.
- Special category data.

From other sources:

- Information about goods/services.

To comply with law (Article 6(1)(c) GDPR). (The German Money Laundering Act ((*Geldwäschegesetz - GwG*)). As regards sensitive personal data, the basis is that the processing is necessary for reasons of the public interest (Article 9(2)(g) GDPR).

When the agreement between you and SOFORT is terminated. See section 9 for more information on our obligations and right to retain information in accordance with the law.

laundering and terrorist financing. This processing constitutes profiling and automated decision making. See section 6 for more information about profiling and automated decisions.

- Information about your financial standing. (SOFORT and credit information bureaus)
- Information about your use of SOFORT's services. (SOFORT)
- Technical information generated through your use of SOFORT's services. (SOFORT)
- Your contacts with the Partner in the context of SOFORT's services. (The Partner)
- Device information (Your device)
- Information from external sanction lists and PEP lists. (Sanction lists and PEP lists)
- Special category data. (Financial institutions, Trust services providers or (other) identity attribute providers, PEP lists)
- Service-specific personal data (see

However, if you have supplied us with sensitive personal data, it is processed based on your explicit consent.

section 3 for information about SOFORT's Services).

To perform a fraud prevention assessment before providing SOFORT's services is accepted.

This processing constitutes profiling and automated decision-making. We use automated decision-making for this purpose, to be able to determine if you constitute a risk of fraud. See section 6 for more information about profiling and automated decisions. Also see section 7.2.3 on our use of fraud prevention agencies to which your information may be shared, and our legal basis for that sharing.

From you:

- Contact and identification data.
- Payment information.

From other sources:

- Information about goods/services. (The Partner)
- Information about your use of SOFORT's services. (SOFORT)
- Technical information generated through your use of SOFORT's services. (SOFORT)
- Your contacts with the Partner in the context of SOFORT's services. (The Partner)
- Device information. (Your device)

In addition to the above, SOFORT receives information from fraud prevention agencies on whether

To enter into and perform the agreement (Article 6(1)(b) GDPR).

When the fraud assessment is performed.

your information indicates an attempt at fraud.

From you:

- Contact and identification data.
- Payment information.

From other sources:

- Information about goods/services. (The Partner)
- Information about your use of SOFORT's services. (SOFORT)
- Information about your contacts with SOFORT's customer service. (SOFORT)
- Your contacts with the Partner in the context of SOFORT's services. (The Partner)

To comply with law (Article 6(1)(c) GDPR). (The German Accounting Rules).

During the period in which the bookkeeping is recorded and for as long as required in accordance with German Accounting Rules. See section 9 for more information on our obligations and right to retain information according to law.

To perform bookkeeping and accounting in accordance with accounting laws and preserve them in compliance with the applicable law.

4.4. SOFORT's processing when you contact SOFORT's customer service.

Purpose of the processing - What we do and why.

Type of personal data used for the purpose, and where they come from (the source). See section 3 to read more about the

Legal basis for processing in accordance with the GDPR.

When the purpose of using the personal data ends. See section 9 for when SOFORT deletes the data.

different types of personal data.

<p>To handle all matters that come to SOFORT's customer service. This includes retaining various forms of written conversations to document customer issues, as well as for security purposes and to counter fraud.</p>	<p>From you:</p> <ul style="list-style-type: none"> • Information about your contacts with SOFORT's customer service. <p>From other sources:</p> <ul style="list-style-type: none"> • Information about your contacts with SOFORT's customer service. (SOFORT) 	<p>Performance of contracts (Article 6(1)(b) GDPR).</p>	<p>Up to ten years, based on the statute of limitations. See section 9 for more information on our obligations and right to retain information according to law.</p>
<p>Quality and service improvement (to ensure satisfactory customer service). We may record telephone conversations as well as screen sharing sessions between you and our employees for quality purposes in order to deliver better products and services to you.</p>	<p>From you:</p> <ul style="list-style-type: none"> • Information about your contacts with SOFORT's customer service. <p>From other sources:</p> <ul style="list-style-type: none"> • Information about your contacts with SOFORT's customer service. (SOFORT) 	<p>Based on your consent (Article 6(1)(a) GDPR).</p>	<p>We process the recordings of telephone conversations for up to 90 days for quality assurance purposes, and the recorded screen sharing sessions for up to 30 days for quality assurance purposes.</p>
<p>Documenting what has been said when talking to our customer service (to ensure we have documented what has been agreed or discussed). We use recorded telephone conversations between you and our employees as well as</p>	<p>From you:</p> <ul style="list-style-type: none"> • Information about your contacts with SOFORT's customer service. <p>From other sources:</p> <ul style="list-style-type: none"> • Information about your contacts with SOFORT's customer service. (SOFORT) 	<p>The processing is based on a balancing of interests (Article 6(1)(f) UK GDPR). When balancing interests, SOFORT has determined that we have a legitimate interest to document communications with SOFORT's customer service. We ensure</p>	<p>90 days from the day when the recording was made.</p>

our employees' notations to document what has been said.

that the particular processing this entails is necessary to achieve that purpose, and that our interest outweighs your right not to have your data processed for this purpose. As a customer, you also have an interest in ensuring impartial means of documenting what has been discussed. You may contact us for more information about how the determination was made. Please see the contact information in section 12.

If you contact us via social media such as Facebook or Twitter, your personal data will also be collected and processed by these companies, in accordance with their privacy notices. The same is true for the answer you get from us. SOFORT processes this information to answer your questions.

From you:

- Contact and identification data.
- Information about your contacts with SOFORT's customer service.

From other sources:

- Information about your contacts with SOFORT's customer service. (SOFORT)

Performance of contracts (Article 6(1)(b) GDPR).

When we have answered your question.

To handle voluntary blocks for using

From you:

Based on your consent (Article 6(1)(a)).

When you notify us that you no longer

SOFORT's services, i.e. if you contact us and ask us to prevent you from being able to use our services. Your voluntary block can be lifted by you at any time by contacting us again.

- Contact and identification data.
- Information about your contacts with SOFORT's customer service.

want to be blocked from using our services or withdraw your consent. We also cease this processing if and when you notify us that you no longer want to be a SOFORT customer at all.

5. How do you withdraw your consent?

When SOFORT uses your personal data based on your consent, you can withdraw your consent at any time. You can do this by sending an e-mail to datenschutz@sofort.com or via the contact information you find in section 12.

Lastly: As described in section 2 above you also have the right to *object* against certain personal data processing (for example you may turn off marketing). You also have a right to have certain personal data *erased*, which is also described in section 2.

6. SOFORT's profiling and automated decisions that significantly affect you.

6.1. SOFORT's profiling of you as a customer.

"Profiling" means an automated processing of personal data to evaluate certain personal matters, for example, by analysing or predicting your personal preferences, such as the bank account or identification method chosen by you in the context of SOFORT's services. At the same time, we compare your data with what our other customers, with similar use of our services, have preferred.

The purpose of SOFORT's profiling and the personal data types used for each occasion and for each profiling are described in detail in section 4 above. The profiling for these purposes does not have a significant impact on you as a customer.

We use profiling for the following purposes:

to deliver our customised services, which customise their content based on what we think is most

interesting to you (this applies to the SOFORT user flow and its various functions), and

to deliver customised marketing to you across both our own and external platforms and services.

If you have any questions about how the profiling process works, please contact us. Contact information is available in section 12. You may object to our marketing profiling at any time by contacting us (and we will then cease profiling for marketing purposes). You may also end our profiling for our services by terminating the service.

6.2. SOFORT's automated decisions that significantly affect you.

Automated decisions with legal effect, or automated decisions that similarly significantly affect you, means that certain decisions in our services are completely automated, without our employees being involved. These decisions have a significant effect on you as a customer, comparable to legal effects. By making such decisions automatically, SOFORT increases its objectivity and transparency in the decision to offer you these services. At the same time, you have the right to object to these decisions at all times. You can read about how to object to these decisions at the end of this section 6.2.

Automated decisions that significantly affect you also mean that profiling is performed based on your data before the decision is made. This profiling is made to assess your financial situation (before the decision to initiate a payment) or to identify whether your use of our services involves a risk of fraud or money laundering. We profile your user behaviour and financial standing and compare this data with behaviours and conditions that indicate different risk levels for us.

When does SOFORT take automated decisions that significantly affect you?

We make this kind of automated decision when we:

decide to approve your application to use a SOFORT service.

decide *not* to approve your application to use a SOFORT service.

decide to initiate a payment with your bank on your behalf.

decide *not* to initiate a payment with your bank on your behalf.

decide to allow you to identify with SOFORT and to share your identity data with a recipient chosen by you.

decide *not* to allow you to identify with SOFORT and to share your identity data with a recipient

chosen by you.

(These automated decisions are based on the data you provide to us, data from external sources such as credit bureaus and SOFORT's own internal information.)

decide whether you pose a risk of fraud, if our processing shows that your behaviour indicates possible fraudulent conduct, that your behaviour is not consistent with previous use of our services, or that you have attempted to conceal your true identity. Automated decisions whereby we assess whether you constitute a fraud risk are based on information you have provided yourself, data from fraud prevention agencies (see section 7.2.3. for details of which ones we use), and SOFORT's own internal information.

decide whether there is a risk of money laundering, if our processing shows that your behaviour indicates money laundering. In relevant cases, SOFORT also investigates whether specific customers are listed on sanction lists.

The personal data types used in each decision are described in section 4. See section 7 for more information about whom we share information with as regards profiling during automated decisions.

If you are not approved under the automated decisions described above, you will not have access to SOFORT's services, such as our PIS, AIS or Identity Services. SOFORT has several safety mechanisms to ensure the decisions are appropriate. These mechanisms include ongoing overviews of our decision models and random sampling in individual cases. If you have any concern about the outcome, you can contact us, and we will determine whether the procedure was performed appropriately. You can also object in accordance with the following instructions.

Your right to object to these automated decisions

You always have the right to object to an automated decision with legal consequences or decisions which can otherwise significantly affect you (together with the relevant profiling) by sending an e-mail message to datenschutz@sofort.com. A SOFORT employee will then review the decision, taking into account any additional information and circumstances that you provide to us.

7. Who do we share your personal data with?

When we share your personal data, we ensure that the recipient processes it in accordance with this notice, such as by entering into data transfer agreements or data processor agreements with the recipients. Those agreements include all reasonable contractual, legal, technical and organisational measures to ensure that your information is processed with an adequate level of protection and in accordance with applicable law.

7.1. Categories of recipients with whom SOFORT will always share your personal information, regardless of the service you use.

7.1.1. Suppliers and subcontractors.

Description of the recipient: Suppliers and subcontractors are companies that only have the right to process the personal data they receive from SOFORT on behalf of SOFORT, i.e. data processors. Examples of such suppliers and subcontractors are software and data storage providers, payment service providers and business consultants.

Purpose and legal basis: SOFORT needs access to services and functionality from other companies where it cannot perform them itself. SOFORT has a legitimate interest in being able to access these services and functionality (Article 6(1)(f) GDPR). We ensure that the processing this entails is necessary to pursue that interest, and that our interest outweighs your right not to have your information processed for this purpose. You are entitled to object to this processing, for reasons connected to the circumstances in your particular case. See section 2 for more information about your rights.

7.1.2. Klarna Group.

Description of the recipient: SOFORT is part of the Klarna Group and SOFORT may share your personal data with other companies in the Klarna Group.

Purpose and legal basis: This is required for SOFORT to be able to provide you with its services and functionalities. SOFORT has a legitimate interest in being able to access and provide these services and functionalities (Article 6(1)(f) GDPR). We ensure that the processing this entails is necessary to pursue that interest, and that our interest outweighs your right not to have your information processed for this purpose. You are entitled to object to this processing, for reasons connected to the circumstances in your particular case. See section 2 for more information about your rights.

When you use our Services with a foreign Partner (meaning a Partner located outside of the EU/EEA area) that has an agreement with another company within the Klarna Group, the disclosure of your personal information between Klarna companies is required in order for the two Klarna companies to manage your payment and enable the foreign store to administer your purchase. The legal basis for this processing is the performance of a contract (Article 6 (1)(b) GDPR). The receiving Klarna Group company will handle your personal data in accordance with the privacy notice that applies in your country (see [list](#)). You can read more about how SOFORT safeguards your personal data when transferred outside of the EU/EEA in Section 8.

7.1.3. A person who holds a power of attorney for your financial affairs.

Description of the recipient: SOFORT may share your personal information with a person who has the right to access it under a power of attorney.

Purpose and legal basis: This processing is carried out to facilitate your contact with us (through agents), and takes place based on your consent (Article 6(1)(a) GDPR).

7.1.4. Authorities.

Description of the recipient: SOFORT may provide necessary information to authorities such as the police, financial authorities, tax authorities or other authorities and courts of law.

Purpose and legal basis: Personal data is shared with the authority when we are required by law to do so, or in some cases if you have asked us to do so, or if required to manage tax deductions or counter crime. An example of a legal obligation to provide information is when it is necessary to take measures against money laundering and terrorist financing. Depending on the authority and purpose, the legal bases are the obligation to comply with the law (Article 6(1)(c) GDPR), to fulfil the agreement with you (Article 6(1)(b) GDPR), or SOFORT's legitimate interest in protecting itself from crime (Article 6(1)(f) GDPR).

7.1.5. Divestment of business or assets.

Description of the recipient: In the event that SOFORT sells business or assets, SOFORT may hand over your personal information to a potential buyer of such business or assets. If SOFORT or a significant part of SOFORT's assets is acquired by a third party, personal information about SOFORT's customers may also be shared.

Purpose and legal basis: SOFORT has a legitimate interest in being able to perform these transactions (Article 6(1)(f) GDPR). We ensure that the processing this entails is necessary to pursue that interest, and that our interest outweighs your right not to have your information processed for this purpose. You are entitled to object to this processing, for reasons connected to the circumstances in your particular case. See section 2 for more information about your rights.

7.2. Categories of recipients with whom SOFORT shares your personal information when you use one of SOFORT's Services.

7.2.1. Partners.

Description of the recipient: By Partners we mean companies that have embedded our Service on their website or app. They are chosen by you when you interact with them and choose to use our Services generally for their benefit, e.g. on a merchant's website you choose our PIS to initiate a payment for the benefit of such merchant.

Purpose and legal basis: Your Personal Data is shared with the Partner you chose in order for such Partner to be able to perform and manage its relationship with you, e.g. by confirming your identity, sending goods, handling questions and disputes, in order to prevent fraud and, where appropriate, send relevant marketing. The Partner's privacy notice applies to the processing of your personal data that has been shared with the Partner and that the Partner processes. Normally, you will find a link to

the Partner's privacy notice on the Partner's website. The legal basis for sharing data with Partners is partly the performance of a contract (Article 6(1)(b) GDPR), insofar as the data sharing takes place to perform the contract between you and the Partner, and partly for SOFORT to comply with the law (Article 6 (1) (c) GDPR), insofar as the data sharing takes place to perform the Identity Services, and the Partners's legitimate interest (Article 6(1)(f) GDPR), or your consent (Article 6(1)(a) GDPR). We ensure that the processing this entails is necessary to pursue that interest, and that our interest outweighs your right not to have your information processed for this purpose. You are entitled to object to this processing, for reasons connected to the circumstances in your particular case. See section 2 for more information about your rights.

7.2.2. Financial institutions.

Description of the recipient: Financial institutions hold the payment account you choose in the context of PIS and AIS.

Purpose and legal basis: SOFORT shares your information with your financial institution to fulfil the SOFORT's Services as requested by you. For the PIS, SOFORT will provide your financial institution with the information you supply when you initiate the payment. If the PIS requires an input of an additional security code (for example to activate specific countries for EU SEPA placements), SOFORT also transfers this security code to your financial institution. If you initiate a payment to a SOFORT account, SOFORT will process the information we receive from your financial institution, such as contact and identification data and payment information. If you initiate payments to accounts in other financial institutions (e.g. the financial institution of a Partner), SOFORT will also pass on some of your contact and identification data as well as payment initiation information to the recipient and also to the recipient's financial institution. For the AIS, SOFORT may transfer the account login data to your financial institution for it to be able to provide access. SOFORT may also share your information with your financial institution to improve its services. For both the PIS and AIS, SOFORT may provide your financial institution with the financial information that was processed when SOFORT was providing SOFORT's Services to you in order to perform data analysis for the purpose of product improvement and product testing (for example to improve fraud models). The legal basis for sharing data with financial institutions is partly the performance of a contract (Article 6(1)(b) GDPR), insofar as the data sharing takes place to initiate and perform the PIS and/or AIS, and partly based on SOFORT's and the financial institution's legitimate interest (Article 6(1)(f) GDPR), or your consent (Article 6(1)(a) GDPR), insofar as the data sharing takes place to perform data analysis for the purpose of product improvement and product testing. We ensure that the processing this entails is necessary to pursue that interest, and that our interest outweighs your right not to have your information processed for this purpose. You are entitled to object to this processing, for reasons connected to the circumstances in your particular case. See section 2 for more information about your rights.

7.2.3. Fraud prevention agencies and companies providing identity checks.

Description of the recipient: Your personal data are shared with fraud prevention agencies and companies that provide identity checks.

Purpose and legal basis: SOFORT shares your information to verify your identity, the accuracy of the data you have provided, and to combat fraudulent and criminal activities. You can find out which companies we cooperate with [here](#). Please note that these companies process your data in accordance with their own data privacy notices.

SOFORT shares your information based on SOFORT's legitimate interest in conducting its business (Article 6(1)(f) GDPR), as the fraud prevention agencies and the companies providing identity checks have information on fraud activities and identity confirmation which are important for SOFORT to use as input to decrease its level of fraudulent transactions. We ensure that the processing this entails is necessary to pursue that interest, and that our interest outweighs your right not to have your information processed for this purpose. You are entitled to object to this processing, for reasons connected to the circumstances in your particular case. See section 2 for more information about your rights.

7.2.4. Credit information bureaus.

Description of the recipient: If you apply to use a service from SOFORT, we may share your personal data with credit information bureaus. Sharing does not take place in the event of small amounts or where we already have sufficient information.

Purpose and legal basis: Your personal information is shared with credit bureaus in order to assess your creditworthiness, to confirm your identity and your contact information, and to protect you and other customers from fraud. This data sharing constitutes a credit report.

In Germany, SOFORT sends the credit bureau your name, address, date of birth and phone number in order to receive the lookup on you. Our credit lookup does not affect your credit rating.

SOFORT may transfer unpaid debt to debt collection agencies which in turn may share information about your late payments to the credit bureau, which may affect your credit rating.

The credit bureau will process your information in accordance with their own privacy notices and you can find out which ones we cooperate with [here](#).

SOFORT shares your information based on SOFORT's legitimate interest in conducting its business (Article 6(1)(f) GDPR), as the credit information bureaus have information on your financial standing which is important for SOFORT to use as input to ensure a correct credit assessment. We ensure that the processing this entails is necessary to pursue that interest, and that our interest outweighs your right not to have your information processed for this purpose. You are entitled to object to this processing, for reasons connected to the circumstances in your particular case. See section 2 for more information about your rights. You can also contact the entities listed in the link above, to exercise the same rights as stated in section 2 also against those entities.

SOFORT retains credit information about you that we have received from a credit information bureaus only in script data format. If you would like to have a readable version, we recommend that you directly contact the credit bureau that informed you that SOFORT requested a credit report.

7.2.5. Trust services provider and (other) identity attribute providers

Description of the recipient: Trust services providers and (other) identity attribute providers provide services to you, Partners or SOFORT to implement and administer trust services including electronic identification and identity verification methods as well as identity attributes collection and provision, such as qualified electronic signatures, video ident, foto ident, etc.

Purpose and legal basis: Some Partners and/or SOFORT use trust services providers and (other) identity attribute providers with whom they share your information for managing the trust services provided by such trust services providers or (other) identity attribute providers to you, the Partners or SOFORT. This sharing takes place in accordance with the Partner's own privacy notices or this Privacy Notice. Partners may also let SOFORT share your information with the trust services providers or (other) identity attribute providers they use for processing the trust services. Some trust services providers or (other) identity attribute providers also collect and use your information independently, in accordance with their own privacy notices. In addition, SOFORT may share your information with the trust services providers or (other) identity attribute providers when providing the Identity Service or Additional Services to you. Sharing with trust services providers or (other) identity attribute providers is done to fulfil the agreement with you (Article 6 (1) (b) GDPR).

8. When can we transfer your personal data outside of the EU, and how do we protect it then?

We always strive to process your personal data within the EU/EEA area. But in certain situations, such as when we share your information within the Klarna Group or with a supplier, subcontractor or Partner which operates outside the EU/EEA, your personal data may be transferred outside the EU/EEA. SOFORT always ensures that the same high level of protection applies to your personal data according to the GDPR, even when the data is transferred outside of the EU/EEA. Your rights in respect to your personal data (described in detail in section 2), are not affected when data is transferred outside of the EU/EEA. More information about the recipients SOFORT shares your data with you can find in section 7.

If you want more information about our safety measures you can always contact us. You can find our contact information in section 12. You find more information about which countries are deemed to have an “adequate level of protection” on the [European Commission's website](#), and you can read more about the European Commission's standard clauses [here](#).

Safety measures which SOFORT uses when transferring personal data outside of the EU/EEA

Countries outside of the EU/EEA may have laws that allow public authorities to request access to personal data stored in the country for the purpose of combating crime or safeguarding national security. Regardless of whether we or any of our providers process your personal data, we will ensure that a high level of protection is guaranteed when transferring that data and that appropriate protection measures have been taken, in accordance with applicable data protection requirements (such as the GDPR). Such appropriate safeguards include, but are not limited to, ensuring:

if the European Commission has decided that the country outside of the EU/EEA to which your personal data are transferred has an adequate level of protection, which corresponds to the level of protection afforded by the GDPR. This means for example that the personal data is still protected from unauthorised disclosure, and that you may still exercise your rights in regards to your personal data, or

the European Commission's standard clauses have been entered into between SOFORT and the recipient of the personal data outside the EU/EEA. This means that the recipient guarantees that the level of protection for your personal data afforded by the GDPR still applies, and that your rights are still protected. In these cases, we also assess whether there are laws in the recipient country that affect the protection of your personal data. Where necessary, we take technical and organisational measures so that your data remain protected during the transfer to the relevant country outside the EU/EEA.

9. How long we store your personal data

How long SOFORT stores your personal data depends on the purposes for which SOFORT uses the personal data:

Personal data used for the contractual relationship between you and SOFORT is generally stored for the duration of the contractual relationship and thereafter for a maximum of 10 years based on statutes of limitations.

Personal data that SOFORT is under a legal obligation to retain, for example under anti-money laundering laws or bookkeeping laws, is generally retained for 5 years or 7 years and in any case for as long as required in accordance with German anti-money laundering laws or bookkeeping laws.

Personal data which is not used for the purposes of your contractual relationship with SOFORT or where SOFORT does not have a legal obligation to retain the data is only retained as long as

necessary to fulfil the respective purpose for our data processing (usually 3 months). More information can be found in the table in section 4.

In some limited cases, the personal data may need to be stored for a longer period because of capital adequacy laws which SOFORT has to comply with.

The legal obligations referred to above means that SOFORT can not delete your personal data, even if you request us to delete it, as described in section 2. If we don't have a legal obligation to retain the personal data, we instead have to make an assessment if we may require the personal data in order to protect SOFORT from legal claims.

Please note that just because we have a legal obligation to store your personal data, this does not mean that we are also permitted to use this data for any other purpose. SOFORT will make an assessment for each specific purpose of how long we may use your personal data. You can read more about this in section 4.

10. How we use cookies and other types of tracking technology

To provide a tailored and smooth experience, SOFORT uses cookies and similar tracking technologies in our multiple interfaces, such as our website or our user flow screens. You can find information about the tracking technology that SOFORT uses, and information about how you accept or decline the tracking technology, in each interface.

11. Updates to this privacy notice

We are constantly working to improve our services so that you have a smooth user experience. This may involve modifications of existing and future services. If that improvement requires a notice or consent in accordance with applicable law, you will be notified or given the opportunity to give your consent. It is also important that you read this privacy notice every time you use any of our services, as the processing of your personal data may differ from your previous use of the service in question.

12. SOFORT contact information

Sofort GmbH, registered with the Munich Local Court under HRB 218675, with its registered office at Theresienhöhe 12, 80339 Munich, Germany.

SOFORT has a data protection officer and a team of data protection specialists. We also have a customer service team that handles data protection issues. You can reach all of these individuals at datenschutz@sofort.com. If you specifically wish to contact SOFORT's data protection officer, enter this on the subject line.

Sofort GmbH complies with German data protection laws. Please visit www.sofort.de for more information about SOFORT.

This privacy notice was last updated on the 20th of September 2023.