Zimpler's Privacy Notice

Zimpler AB, org.no 556887-9984, with registered address at Wallingatan 2, 111 60 Stockholm (”**Zimpler**”, “**we**”, “**us**” or “**our**”) is an authorised payment institution that offers payment services under the supervision of the Swedish Financial Supervisory Authority.

Zimpler cares about your privacy and we want you to feel safe in our processing of your personal data, which we need to do in different ways when we perform our services to you. In this notice you will learn about the personal data we collect, how we use it, your rights and how you can invoke them and the measures we take to keep your personal data safe. We continuously work to ensure that your data is processed and protected in accordance with the General Data Protection Regulation (EU) 2016/679 (the “GDPR”) and other applicable legislation.

If you apply for a job at Zimpler, to get information on our processing of personal data please see our privacy notice for job applicants on our webpage.

1. DEFINITIONS

In this privacy notice, personal data, data subject, legal basis, controller, processor and other by the GDPR defined terms have the same meaning as ascribed to them in the GDPR. Undefined terms have the same definition as in our Terms and Conditions. Further, the terms below have the following meaning.

- **Business Representative** – means a natural person who works for, *e.g.,* a service provider that we have hired or a Merchant that has chosen or is considering Zimpler as its payment service provider.
- **End User** – means a natural person who uses our payment service, or any related service provided by us, for payments to or from Merchants, in own capacity or as representative of a legal person.
- **Merchant** – means goods or service providers, as well as collecting partners (such as other payment service providers), that use us as their payment service provider for the purpose of making payment transactions to or from their customers (End Users and Sub-Merchants).
- **Services –** means payment services and any other services provided by Zimpler as described in the Terms and Conditions.
- **Website visitor** – means individuals who visit our website or contact our customer support or sales team.

Personal data is defined in the GDPR as any information relating to an identified or identifiable natural person. In this privacy notice we therefore describe the personal data we collect and process about Business Representatives, End Users, and Website visitors (“you”, “your” or “yours”).

2. ROLES AND RESPONSIBILITIES

Zimpler is the data controller for the personal data we process to perform our business activities, which includes your use of our payment service. Please note that your payment account provider (normally the bank where you hold the account used for payment transactions initiated through Zimpler) and the Merchant you are transacting with are separate and independent controllers for the processing of personal data in connection with their business activities and the products and/or services they provide to you.

3. YOUR RIGHTS

In accordance with the GDPR you have several rights regarding our processing of your personal data, which you can read about below. If you wish to exercise any of your rights, please contact us by sending an e-mail to our support team at privacy@zimpler.com.

You can read more about your rights at the website of the Swedish Privacy Protection Authority ("IMY").

3.1. Right to information and access

You have the right to know if we process personal data about you. If we do, you also have the right to receive information about the personal data we process and why we do it. You also have the right to receive a compilation of all personal data we have about you.

If you are interested in specific information, please indicate so in your request. For example, you can specify if you are interested in a certain type of information (*e.g.,* what contact and identification information we have about you) or if you want information from a certain time period.

3.2. Right to have erroneous data corrected

If the data we have on you is incorrect, you have the right to have it corrected. You also have the right to supplement incomplete information with additional information that may be needed for the information to be correct.

Once we have corrected your data, or it has been supplemented, we will inform those we have shared your data with about the update, if it is not impossible or too cumbersome. If you ask us, we will also tell you who we have shared your data with.

If you request to have data corrected, you also have the right to request that we limit our processing during the time we investigate the matter.

3.3. Right to have data deleted

In some cases, you have the right to have your data deleted. You have the right to have your data deleted if:

- The date is no longer needed for the purposes for which we collected it,
- You withdraw your consent, provided that the processing is based on your consent,
- You oppose the use that is based on our legitimate interest and we cannot show compelling grounds that outweigh your interests,
- The personal data has been used illegally, or
- Deletion is required to fulfil a legal obligation.

If we delete data following your request, we will also inform those we have shared your data with, if it is not impossible or too cumbersome. If you ask us, we will also tell you who we have shared your data with.

3.4. Right to restriction

In some cases, you have the right to request restriction of our use of your personal data. Restriction means that the data may only be used for certain limited purposes. The right to restriction applies:

- When you believe the data is incorrect and you have requested correction. If so, you can also request that we limit our use while we investigate if the data is incorrect or not,
- If the use is illegal but you do not want the data to be deleted,
- When we no longer need the data for the purposes for which we collected it, but you need it to be able to establish, assert or defend legal claims, or
- If you object to the use. If so, you can request that we limit our use while we investigate if our interest in processing your data outweighs your interests.

Even if you have requested that we restrict our use of your personal data, we have the right to use it for storage, if we have obtained your consent to use it, to assert or defend legal claims or to protect someone's rights. We may also use the information for reasons relating to an important public interest.

We will let you know when the restriction expires. If we limit our use of your data, we will also inform those we have shared your data with, if it is not impossible or too cumbersome. If you ask us, we will also tell you who we have shared your data with.

3.5. Right to access and request a transfer of your personal data to another recipient ("Data portability")

You may request to have your data transferred to another actor in a commonly used machine-readable format. This is also known as *data portability*. You can request data portability if we have collected the data from you and our processing is based on your consent, or if it is processed to enter or fulfil an agreement with you.

3.6. Right to object

You have the right to object to processing that is based on our legitimate interest. If you object to the use, we will, based on your particular situation, evaluate if our interests in using the data override your interests, rights and freedoms. If we are unable to provide compelling legitimate grounds that outweigh yours, we will stop using the data you object to – provided we do not have to use the data to establish, exercise or defend legal claims. If you object to the use, you also have the right to request that we restrict our use during the time we investigate the matter.

You also have the right to object to processing of your personal data for direct marketing purposes, whereby your personal data will no longer be processed for such purpose.

3.7. Right to object against an automated decision-making/profiling

You have the right not to be subject of a decision that is only based on some form of automated decision-making, including profiling, if the decision can have legal consequences for you or in a similar way affect you to a considerable degree.

Automated decision-making is when automated means without human intervention are used for making a decision in relation to you as an individual. In our business this could mean, *e.g.,* automated verifying of your identity. Profiling is when personal data is automatically processed for the purpose of evaluating personal aspects relating to you as an individual, *e.g.,* your economic situation or personal preferences. Automated decisions can be made with or without profiling and contrariwise, profiling can be used without this leading to an automated decision.

3.8. Right to withdraw consent

You have the right to withdraw your consent for a specific processing at any time, whereby we will no longer perform the processing, provided that the applicable processing is based on your consent. Your withdrawal will not affect processing that has already been carried out.

3.9. Complaints

If you have any complaints regarding how we process your personal data even after you have notified us of this, you are always entitled to submit your complaint to the relevant data protection authority in the country where you reside, work or where you believe an infringement of data protection laws have taken place.

In Sweden, the relevant data protection authority is the Swedish Authority for Privacy Protection and you can submit your complaint here.

4. PROCESSING OF PERSONAL DATA WHEN YOU USE OUR SERVICES

Zimpler's Services include payment initiation services, account information services and any other services provided by Zimpler as described in the Terms and Conditions.

When using our Services, we collect personal data directly from you, as well as from your online banking interface (*i.e.,* online bank) or via an API provided to us by your bank. In addition, we also collect personal data from the applicable Merchant and, depending on for which purpose the service is used, from external third-party sources (*i.e.,* when we need to verify your identity and/or update/supplement your contact information via official identity verification service providers or similar providers). Our system will in addition generate personal data such as a user id number when you use our service.

In the table below we describe how we process your personal data when you as an End User use our payment service.

Data subject	Purpose	Categories of personal data	Legal basis	Collected from	Time of retention
End User	To provide our Services, such as payment initiation and account information services	Name, social security number, address, phone number, email, IP-address, date of birth, bank account number, transaction information, direct debit (autogiro) mandate (if applicable)	Performance of contract	From you, your bank, the Merchant and a third-party providers	During the period we have an active relationship with you/you use our Services
End User	To fulfil our bookkeeping requirements for Services	Name, social security number, bank account number, transaction information, direct debit (autogiro) mandate (if applicable)	Legal requirement (Bokföringslag (1999:1078))	From you, your bank, the Merchant and a third-party providers	Seven years from the time of the transaction
End User	To improve your experience and enable faster transactions, such as refreshing your data on a 180-day interval	Name, social security number, address, phone number, email, IP-address, date of birth, bank account number, transaction information	Legitimate interest to provide you with a faster and better service	From you, your bank and a third-party providers	During the period we have an active relationship with you/you use our Services
End User	To troubleshoot, safeguard and increase the performance of our Services and to anonymise your data to perform data analysis for testing and product development	Name, social security number, address, phone number, email, IP-address, date of birth, bank account number, transaction information	Legitimate interest in troubleshooting, safeguarding and increasing the performance of our Services to provide you with a working service and	From you, your bank, the Merchant and a third-party providers	During the period we have an active relationship with you/you use our Services (in some cases longer if data is anonymised)

			offer better products		
End User	To provide customer support to you and to handle any request/ problem	Name, social security number, address, phone number, email as well as other information you provide to us to identify you and resolve your errand	Performance of a contract for specific transactions Legitimate interest (or contract if entered into) for general errands	From you, your bank and third-party data provider	Up to ten years due to statutes of limitations (Preskriptionslag)
End User	To cater to your data protection rights pursuant to GDPR and other applicable data protection legislation	Name, social security number, address, phone number, email as well as other information needed to identify you and resolve your errand	Legal requirement (General Data Protection Regulation Chapter III) and legitimate interest of verifying your identity to prevent unauthorised disclosure	From you	Up to ten years due to statutes of limitations (Preskriptionslag)
End User	To handle any complaints or establish, exercise and/or defend Zimpler against legal claims	Name, social security number, address, phone number, email as well as other information needed to identify you and resolve the matter in hand	Legitimate interest of handling complaints or establish, exercise and/or defend legal claims	From you, your bank, the Merchant and third-party providers	Up to ten years due to statutes of limitations (Preskriptionslag)
End User	To provide registration and verification services to improve your experience and enable faster transactions, as applicable, that includes sharing know your customer data with Merchants	Name, social security number, address, phone number, email, IP-address, date of birth, bank account number, transaction information, user ID	Legitimate interest to provide you with a faster and better service by facilitating your transactions and Merchants' process of verifying the identity of End User to prevent money laundering, fraud or other criminal act or to meet other potential legal	From you, your bank and a third-party provider	During the time of the transaction

			and/or regulatory requirements imposed on the Merchant and to fulfil our contractual obligations with the Merchant as applicable		
End User	To fulfil our legal obligation under applicable anti-money laundering rules and regulations. This includes screening against sanction lists and may include profiling and automated decision-making	Name, social security number, bank account number, transaction information, address, phone number, IP-address, screening against PEP/sanction lists, criminal records	Legal requirement (lag (2017:630) om åtgärder mot penningtvätt och finansiering av terrorism)	From you, your bank, third-party data provider and open sources	Five years (in some seldom cases ten years) from the time of the transaction
End User	To manage incidents and prevent that our service is used for fraudulent or other illicit actions. This may include profiling and automated decision-making	Name, social security number, bank account number, transaction information, address, phone number, IP-address, screening against PEP/sanction lists, criminal records	Legal requirement (lag (2017:630) om åtgärder mot penningtvätt och finansiering av terrorism)	From you, your bank, third-party data provider and open sources	Five years (in some seldom cases ten years) from the time of the transaction
End User	To recognise a recurring user by connecting a unique identifier to a reusable AIS consent for faster payment experience by increasing performance, minimising user drop and analytics	Unique identifier that enables reuse of AIS consent (i.e. remove step having to select and login to the bank	Consent	From you	Until withdrawal of end user consent

5. PROCESSING OF PERSONAL DATA FOR POTENTIAL AND EXISTING BUSINESS RELATIONSHIP WITH ZIMPLER

Zimpler also processes personal data regarding Business Representatives of existing and potential Merchants in accordance with what is set out in the table below.

Data subject	Purpose	Categories of personal data	Legal basis	Collected from	Retention
Business representatives of existing Merchants	To manage and maintain a business relationship with existing Merchants and to communicate important information regarding our services that is not considered marketing	Name, title, address, email address, phone number, company of employment	Performance of contract and legitimate interest to communicate with existing Merchants	From you, Merchant, third-party providers and open sources	Two years from the latest contact and/or active business relationship
Business representatives of existing and potential Merchants	To market and sell our services, to disseminate news about Zimpler as well as educational content about the industry, to existing and potential Merchants, e.g. send newsletters or contact after visiting our website and/or events	Name, title, address, email address, phone number, company of employment	Legitimate interest to promote our services to and communicate with potential and existing Merchants	From you, Merchant, third-party providers and open sources	Two years from the latest contact and/or active business relationship
Merchant's beneficial owners, representatives, board of directors and other key personnel	To fulfil our legal obligation under applicable anti-money laundering rules and regulations. This may include profiling and automated decision-making.	Name, social security number, passport number, addresses, phone number, ownership details, copy of ID, IP-address, criminal records, information from PEP/sanction lists	Legal requirement (lag (2017:630) om åtgärder mot penningtvätt och finansiering av terrorism)	From legal entity and third-party provider	Five years (in some seldom cases ten years) from when the business relationship terminates

6. PROCESSING OF PERSONAL DATA WHEN YOU VISIT OUR WEBSITE OR OFFICES

Zimpler may process personal data when you visit our website as well as when you contact us through our customer support or sales team.

Data subject	Purpose	Categories of personal data	Legal basis	Collected from	Retention
Website visitor	To assist you with any issue you may have had with our service or other request connected to your use of our service or website	Name, email address and other information we require to manage your request	Our legitimate interest of solving your issue or request	From you and open source	Up to ten years due to statutes of limitations (Preskriptionslag)
Office visitor	To prevent and detect crimes and ensure safety and security of our staff and visitors	Camera surveillance images and video recordings	Our legitimate interest in safeguarding our premises, business operations and the security of our staff and visitors	From CCTV	Up to 60 days (in some seldom cases longer)
Individuals who contact our customer support or sales team on Zimpler's webpage	To contact you in order to promote and/or market our services, as well as to use the data for marketing and customer analysis, market research, statistics, follow-up on business operations, etc. This may include profiling and automated decision-making	Name, email address, company information (name, industry and website) and other information we require to manage your request	Our legitimate interest in promoting our services and provide relevant information to persons who have contacted us as well as to do follow-up and analyses on sales	From you and open source	During time period of communication or for as long as we have an active relationship

When you visit our website, we may set cookies on your device to deliver to you a well-functioning and personalized experience of our website. The data generated from the cookies is used to provide you with a better user experience. For more information on the cookies we use, please see our cookie notice.

7. HOW LONG WE STORE YOUR DATA

How long we store your personal data is stated in the tables above and is dependent on the following factors:

- The purpose for which we collected the personal data
- The type of relationship we have with you
- Any legal obligations to store the personal data for a certain amount of time

In general, personal data used for the performance of the contractual relationship between you and Zimpler is stored by us for as long as the agreement is valid and thereafter for a maximum of ten (10) years due to the Swedish and other statutes of limitations as applicable. Personal data that we must save due to applicable legislation, such as anti-money laundering and bookkeeping rules and regulations, is normally stored for five (5) and seven (7) years, respectively.

Please note that not all data will be stored for the maximum time as provided above. Different time periods apply depending on the purpose the data was collected for. For instance, some information such as your contact information will be processed for several purposes and may for some purposes be processed only for a very short period but for other purposes for longer periods of time. The personal data that we do not need to keep for the purpose it was collected will be deleted.

8. WHO WE SHARE YOUR DATA WITH

Zimpler does not sell your personal data to third parties and we do not share your personal data with just anyone. However, in some cases we need to share your personal data with selected and trusted third parties to perform our business. If so, we make sure that the transfer of personal data is safe to protect your privacy.

Here you can read more about the categories of recipients with whom we share personal data with in regard to our End Users, Business representatives, Websites visitors and individuals contacting our customer support or sales team.

8.1. End Users

Suppliers and sub-suppliers

To provide our Services to you we need to collaborate with third parties in terms of functions which we cannot provide ourselves, such as other entities within the Zimpler group of companies, technical partners of Merchant, software and data storage suppliers, business consultants and official identity verification service providers.

The sharing of personal data with such third parties is carried out on the basis that it is necessary to fulfil our contractual obligations with you, our legitimate interest to carry out the transaction and/or our legal obligation to verify your identity. When you use our Services we may also need to share your personal data with providers of sanctions or PEP lists in order to screen your personal data against such lists. The sharing of personal data is then carried out on the basis that it is necessary for us to comply with our legal obligations. Additionally, we need to share personal data with software and data storage suppliers which is done for the purpose of providing and improving our services in accordance with our contractual obligations with you.

When your personal data is shared with such a third party, the third party will typically act as data processor in relation to your personal data, meaning that it will process your personal data on our behalf and only in accordance with our instructions. We have entered into data processing agreements with all our data processors guaranteeing a high level of safety for the personal data and, where applicable, the European Commission's standard contractual clauses (please see more information in section 9 below regarding transfers to third countries).

Merchants

Information regarding your identity as well as information on transactions is shared with the applicable Merchant for the Merchant to be able to register you, verify your identity, account and transactions. We share this information with the Merchant to improve your experience and enable faster transactions and provide registration and verification services as applicable based on our legitimate interest to provide you with a faster

and better service, by facilitating your transactions and Merchants' process of verifying the identity of End User to prevent money laundering, fraud or other criminal act or to meet other potential legal and/or regulatory requirements imposed on the Merchant and to fulfil our contractual obligations with the Merchant as applicable.

Banks

To carry out a transaction when using our Services, we need to transfer some of your personal data to your bank as well as other banks that are part of the payment chain. This processing is carried out on the basis that it is necessary to fulfil our contractual obligations with you and the applicable banks. We may also need to share your personal data and information on payments to your bank and/or other banks that are part of the payment chain to investigate payment transactions, for the purposes of preventing and disclosing breaches against anti-money laundering legislation, fraudulent use of our payment service and other criminal acts. When sharing your personal data for this purpose with your bank and/or other banks, this is carried out based on our legitimate interest to prevent frauds and other criminal acts.

Authorities

Zimpler may need to share personal data with authorities, such as the Swedish Financial Supervisory Authority, the police as well as tax and other relevant authorities. This is done for the purpose of preventing and disclosing breaches against anti-money laundering and terrorism financing legislation, by suspicion of fraudulent use of the service or other criminal acts. When sharing your personal data for these purposes with authorities, this is carried out to fulfil our legal obligations.

8.2. Business Representatives

If you are a Business Representative, we may share your personal data with providers of sanctions or PEP lists to screen your personal data against such lists. The sharing of personal data is carried out on the basis that it is necessary for us to comply with our legal obligations. We may also need to share your personal data with cloud-based service providers which is done for the purpose of providing and improving our services to you as well as to provide you with marketing regarding our services. The sharing of personal data is carried out based on our legitimate interest in providing you with the services and marketing thereof. We may share your personal data with our bank partners to ensure your company is approved by our banks. The sharing of personal data is carried out on the basis that it is necessary to fulfil our contractual obligations with you.

8.3. Websites and office visitors and individuals contacting our support or sales team.

We may share your personal data to other third-party providers of analytical tools based on our legitimate interest of providing you with a pleasant user experience when interacting with our websites. We may also need to share your personal data with cloud-based service providers, which is done for the purpose of providing and improving our services to you as well as to provide you with marketing regarding our services.

When visiting our offices we share your personal data with processors delivering the camera surveillance and supporting our activity in general. Zimpler may also need to share and process your data to investigate crimes and internal policy breaches, with police authorities and other relevant stakeholders.

9. TRANSFER OF PERSONAL DATA

Zimpler takes all reasonable measures to only process personal data within the EU/EEA. However, for some parts of our business, as described above, data may be transferred to third parties located outside of the EU/EEA. This is namely the US, which is the location of hosting for some of our service providers. Regardless of if the data is transferred and processed within or outside of the EU/EEA, we will take all reasonable measures to ensure that your data is processed with a high level of security with an adequate level of protection maintained, and that suitable safeguards are adopted in line with the GDPR.

Your rights, as described above, will never be affected by where the personal data is processed.

The safeguard we use in our business is the implementation of the European Commission's standard contractual clauses (the "SCC"), which can be found here: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en.
By entering the SCC, Zimpler and the recipient of the personal data guarantee that the protection of your personal data provided by the GDPR also applies outside of the EU/EEA. In this regard we also assess whether there is legislation in the recipient country that affects the protection of your personal data. When so is required, we implement necessary technical, organizational and contractual measures to ensure that the data is protected with a high level of security that is appropriate to the risks associated with the processing and transfer to the recipient country. What is necessary is assessed on a case-by-case basis and if you wish to know more, please feel free to contact us.

10. AUTOMATED DECISION-MAKING AND PROFILING

Zimpler sometimes uses profiling and automated decision-making when providing our services to you as an End User. For instance, we use automated decision-making for the purpose of risk management of you and your transactions, to verify your identity, assess your financial information and to ensure that you reside in a country where we offer our service. This is done for the fulfilment of our legal obligations to conduct know your customer (KYC) checks in relation to our anti-money laundering obligations. The outcome of the automated decisions may be change of risk classification, denial of service, blocking, holding or releasing transactions.

As a Business Representative, we may use profiling and automated decision making for the purpose of screening your personal information against sanctions or PEP lists on the basis of fulfiling our legal obligations to conduct know your customer (KYC) checks.

11. CONTACT INFORMATION

Data controller

Name: Zimpler AB
Reg. no: 556887-9984
Postal address: Wallingatan 2, 111 60 Stockholm
E-mail address: privacy@zimpler.com

Zimpler has a Data Protection Officer (DPO) who is responsible for monitoring our compliance with applicable data protection legislation. If you have any questions to us, or feel you need any part of this notice explained, please contact us by sending an e-mail to privacy@zimpler.com. If you want to reach our DPO specifically, please state this in your request or email.

Generally, Zimpler AB is the data controller when personal data are processed in connection with providing the group's services, which includes your use of our payment service, and associated business activities, e.g., marketing activities and contract maintenance. However, where one of our agent subsidiaries in the EU/EEA has a legal obligation to perform a certain processing activity, Zimpler AB and the subsidiary will be joint controllers for that specific processing activity, e.g., AML/KYC controls. Regardless of how the roles are allocated between us, you may always contact Zimpler AB in case of questions, if you want to exercise any of your rights or if you want to submit a complaint.

Please note that your payment account provider (usually the bank where you hold the account used for payment transactions initiated through Zimpler) and the Merchant you are transacting with are separate and independent controllers for their processing of your personal data. For information on their processing of your personal data, please contact them directly.

12. VERSIONS IN OTHER LANGUAGES THAN ENGLISH

The original version of this privacy notice is written in English. To the extent that a translated version of this privacy notice conflicts with the English version, the English version shall prevail.

13. CHANGES TO THIS PRIVACY NOTICE

We reserve the right to change this privacy notice from time to time. We will inform you of any changes by posting the updated notice on our website. If we make any material changes to our notice, we will push a notification through a banner on our website and/or by e-mail (if we have your e-mail address and you have not opted-out from such use). We encourage you to contact us if you have any questions about the notice or about how we process your personal data.

This Privacy Notice was last updated January 2024.