# Privacy Statement

Version: 4.1
June 2025

## 1. Introduction

This Privacy Statement describes how Zivver and its related entities ("**we**", "**our**" or "**us**") process your personal data in relation to your use of our digital communications platform and related services (the "**Service**") as well as our website. A proper handling of personal data is of paramount importance to Zivver, which is why we process and secure personal data carefully.

In this Privacy Statement, we explain what personal data we gather and use, for what purposes, and based on what legal grounds. We recommend you closely read this Privacy Statement, as it applies to all Zivver users.

This Privacy Statement applies to the activities for which Zivver B.V. is a controller, which means that Zivver decides why and how personal data is processed. Zivver may also act as a processor (e.g., when we offer business accounts as a service provider to other companies). However, this Privacy Statement does not apply to such processing, which takes place on behalf of our business customers. To learn more about the processing of your personal data in that context, please consult our relevant customer's privacy policy (e.g., if you have a Zivver account from your organisation, we recommend that you consult your organisation's privacy policy).

## 2. Information about the Zivver procedures

### 2.1 The Service

#### *2.1.1 Zivver personal accounts*

For the creation of a Zivver account, you have provided the following data:

- First and last name*
- Email address*
- Profile picture
- Phone number
- Preferred language
- Notification preferences
- E-mail signature
- IP address
- Account ID

* required to complete the registration, as an account cannot be created without this information.

During the use of the Zivver Service, Zivver processes the following data:

- Date and time of sent and received messages (provided that these were sent

through Zivver)
- Sender and recipient email address of the relevant messages
- Subject of sent and received messages
- Content of the sent messages and the attachments (sent messages are encrypted and we take all reasonable steps so that their content cannot be viewed by Zivver)

*2.1.2 Zivver guest-user accounts*

If you receive a message from a Zivver user, a guest-user account is created from which you can securely view your received message. To do this, we process the following some of your personal data:

- First and last name
- Email address
- Phone number (if used for two-factor authentication)
- IP address
- Account ID

*2.1.3 Cookies in the Web App*

For the Zivver Web App to function properly, (the use of) cookies is required. For more information about cookies on the website, we refer to our Cookie Statement.

If you use Zivver, we automatically store your IP address in our web server's log files to properly secure the Service and its proper functioning. If you do not allow the processing of this data (e.g., via browser settings) you unfortunately cannot use our website at http://www.zivver.com.

*2.1.4 Chrome Extension for Gmail*

Zivver's use of information received from Google Restricted Scopes API's will adhere to Google's Limited Use requirements.

*2.1.5 Zivver Secure eSignatures (optional feature)*

In the event that, as part of the Service, you make use of Zivver Secure eSignatures, Zivver will process, next to the data identified above, electronic signatures.

*2.1.6 Zivver Proof of Delivery (optional feature)*

If, as part of the Service, you use Proof of Delivery, Zivver will process the data identified above, as well as:

- Date and time of the decryption of the message by recipient
- Date and time of the decryption of the attachments by recipient

*2.1.7 Zivver Email Threat Protection (optional product)*

If your organization uses Zivver Email Threat Protection, Zivver will process the emails to scan and analyze them to determine the classification (phishing/SPAM/regular email) and apply proper actions like quarantine. To do this, we process the following data:

EML files (email files) including the following personal data:

- Email address sender
- Email address recipient
- IP address sender
- Subject of message
- Attachment names
- Content of the email and attachments
- Data behind embedded links

*2.1.8 Purposes of the Zivver Service*

Zivver processes the aforementioned personal data for the following purposes:

- Having users of the Service log in and verify/authenticate their identity
- Sending and delivering messages and files through the Service
- Informing users of the decryption of messages
- Alerting users to the sensitive content in messages and suggesting when messages should be sent through Zivver
- Communication between Zivver and users
- Delivering support with regard to the Service
- Improving the user experience of the Service based on feedback and testing
- Logging, monitoring, and auditing of the Service
- Digitally signing documentation (feature of Zivver Sign)
- Informing users of the decryption of attachments (feature of Proof of Delivery)
- Making the receipt of the message demonstrable (feature of Proof of Delivery)
- To scan and analyze emails, add classifications (phishing/SPAM/regular email) and apply proper actions like quarantine (Zivver Email Threat Protection)
- To improve detection rules (Zivver Email Threat Protection)
- Finding and preventing fraud, and respond to trust and safety issues that may arise
- For compliance purposes, including enforcing our Terms and Conditions or other legal rights, or as may be required by applicable laws and regulations or requested by any judicial process or governmental agency
- For commercial purposes, such as to see if an individual user is a business that would be interested in converting to a business account
- For other purposes for which we provide specific notice at the time the information is collected.

Zivver processes the personal data based on the following legal grounds: to perform our contractual obligations (such as providing the Service to you), because Zivver has a legitimate interest (such as in ensuring the proper functioning of the Service), as required by applicable law (e.g. for compliance purposes) or where it has obtained your consent (such as for the use of cookies).

*2.1.9 Support and user feedback*

If a user requests support in the use of Zivver, Zivver will process the following personal data:

- First and last name
- Email address

- Phone number
- Position
- Organization

If a user provides additional feedback (for example, submitting a feature request or responding to a customer satisfaction survey), Zivver will process the following personal data:

- Email address
- The feedback itself

Purposes for processing personal data:

- For purposes related to Customer Support, if feedback shows that the user is having difficulties with the product
- For internal reports
- For identifying and preventing fraud and to respond to trust and safety issues that may arise
- For compliance purposes, including enforcing our Terms and Conditions or other legal rights, or as may be required by applicable laws and regulations or requested by any judicial process or governmental agency
- For other purposes for which we provide specific notice at the time the information is collected

Responses are only shared within Zivver and, where applicable, its service providers, unless a user explicitly consents to having their feedback shared outside of Zivver (for example, by publication on the website).

Participants in user interviews or other research initiatives are informed about how their data is handled and asked for consent up front. They can at all times refuse to answer individual questions or withdraw from participating altogether, without adverse consequences.

*2.1.10 Storage period*

Zivver takes measures to delete your personal data or keep it in a form that does not permit identifying you when it is no longer necessary for the purposes for which we process it, unless we are required by law to keep this information for a longer period.

When we process personal data for our own purposes, we determine the retention period taking into account various criteria, such as the type of services provided to you, the nature and length of our relationship with you, possible re-enrolment with our services, the impact on the services we provide to you if we delete some information from or about you, and mandatory retention periods provided by law and the statute of limitations.

For example, data is stored for as long as necessary for the performance of the contract. Upon termination of the contract, we take reasonable steps to delete your profile data, including the name, phone number, and possible profile picture. In some circumstances we may be unable to delete data (such as your email address) because other users still require access to that data as part of their use of the Zivver services.

The Zivver messages and attachments are stored until:

- The sender has revoked the specific message; or

- The sender and recipient have deleted the message.

The emails scanned by Zivver Email Threat Protection are stored until the Message Retention Time is due, which is set by Zivver's customers.

The support data are stored for a period of two years after completion of the support request. Data gathered through customer satisfaction inquiries or customer interviews is stored for a period of two years.

The above does not apply if we are obliged to store your data on the grounds of a legal obligation or justified business interest for Zivver (such as defense against a legal claim).

### 2.2 Website

You can find several forms on our website, such as the contact form and the download form. The data you provide through these forms is included in our Customer Relations Management (CRM) system. If you are not a Zivver client, this data will not be stored for more than two years after the last moment of contact.

The forms on our website serve, among others, the following purposes:

- Sending you the requested content (such as white papers, blogs)
- Answering your request for contact
- Sending you a quotation
- Planning a demo

Because you file a request with us through filling out the forms, the grounds for the processing mentioned above is an agreement.

Additionally, you can subscribe to our newsletter on our website. When subscribing to our newsletter, you grant us permission for the processing of your personal data as part of the sending of the newsletter. Newsletters you receive from us also contain the option to unsubscribe.

For more information about cookies on the website, we refer to our Cookie Statement.

### 2.3 Job Applications

If you apply for a job at Zivver, we will process your personal data for the application process. This concerns the data you provide and possible notes based on application interviews. These data are solely shared with the persons involved with the application process and will be deleted within four weeks after the process was ended.

With your permission, we can store your personal data in our talent pool. This means your data will be stored for a maximum of one year.

### 2.4 (Potential) Clients

For (potential) clients, limited personal data of our contacts is processed. This concerns contact data and payment data. Zivver processes this data because it has a justified interest

to do so. The data is deleted if Zivver no longer requires it and does not have a legal obligation to store the data.

Calls with potential clients may also be monitored for internal coaching purposes. If a call is monitored, it can be either listened to or recorded, and Zivver will process personal data such as voice, name, phone number and any additional data discussed in the call. In these situations, information is always granted before the monitoring starts and the data subject is granted an opportunity to exercise their rights. In the event consent is granted and calls are recorded, they will be stored for 180 days.

### 2.5 Testimonials

Your name will only be posted with your testimonial with your permission. If you want to adjust or delete your testimonial, you can contact us via support@zivver.com.

## 3. How Zivver shares information

We only share the data you provide us with other parties when this is necessary as part of the Service, the execution of the agreement we have with you or your organisation, and/or when such transfer of data is required by law.

### 3.1 Affiliates

We may share any information we receive with our affiliates for any of the purposes described in this Privacy Statement.

### 3.2 Vendors and service providers

We may share any information we receive with vendors and service providers retained in connection with the provision of the Service.

### 3.3 Analytics Partners

We use analytics services such as Google Analytics to collect and process certain analytics data. These services may also collect information about your use of other websites, apps, and online resources. You can learn more about Google's practices by visiting https://www.google.com/policies/privacy/partners/.

### 3.4 As Required By Law and Similar Disclosures

We may access, preserve, and disclose your information if we believe doing so is required or appropriate to: (a) comply with law enforcement requests and legal process, such as a court order or subpoena; (b) respond to your requests; or (c) protect your, our, or others' rights, property, or safety. For the avoidance of doubt, the disclosure of your information may occur if you post any objectionable content on or through the Service.

### 3.5 Merger, Sale, or Other Asset Transfers

We may transfer your information to service providers, advisors, potential transactional partners, or other third parties in connection with the consideration, negotiation, or completion of a corporate transaction in which we are acquired by or merged with another company or we sell, liquidate, or transfer all or a portion of our assets. The use of your information following any of these events will be governed by the provisions of this Privacy Statement in effect at the time the applicable information was collected.

3.6 Consent

We may also disclose your information with your permission.

3.7 Miscellaneous

If you sign up with an email address belonging to an organisation, we may disclose the email address to that organisation for Marketing and Sales purposes.

## 4. International data transfers

4.1 Zivver Messages

Zivver does not transfer data contained in the messages sent through the Zivver service out of the European Economic Area (the "**EEA**"), the United Kingdom (the "**UK**") or Switzerland.

4.2 Zivver Email Threat Protection (Optional product)

Limited data within emails scanned and analyzed by Zivver Email Threat Protection may be processed outside the European Economic Area for the purposes of product integrations and product detection improvements

4.3 Prospect & Customer Account Data

Data on customer accounts or prospects can be transfered to the parent company of Zivver ; Kiteworks USA, LLC en Accellion, Inc., acting under the joint name Kiteworks.

Kiteworks can be contacted via email on privacy@kiteworks.com, or via mail via:
Kiteworks USA, LLC
1510 Fashion Island Boulevard, Suite 100
San Mateo, CA 94404
Attn: Privacy Compliance

The personal data being transferred includes:

- Contact information of potential customers, including email addresses, phone numbers, company name, and job title.
- Interactions of potential customers with Zivver, including registrations for webinars, events, newsletters, etc.
- Contact information of customers, including email addresses, phone numbers, job title, notes, and bank account numbers (of the organization, not individuals).
- Contract and subscription information, including rates, contract terms, names, and signatures.

- Support requests, including email addresses, problem descriptions as provided by the customer, and resolutions.

Contractual safeguards are in place to ensure the protection of personal data transfers.

4.4 Other Data

We may transfer personal data (such as the data captured in our CRM system) to other countries than the country in which the data was collected for storage and processing in connection with storage and processing of data, fulfilling your requests, and operating the Service. These countries may have different privacy protection standards than your country of residence.

4.5 Protective Measures

We only transfer personal data across borders in accordance with applicable law, for example by relying on contractual protections (such as Standard Contractual Clauses issued by the EU Commission) or adequacy decisions of competent authorities. You may contact us as specified in the "Contact information" section included in clause 5.3 below to obtain a copy of the overview of the safeguards that we use to transfer your personal data outside the EEA or UK.

**5. How you can keep control of your information**

5.1 Your privacy rights

If you are located in the EEA or the UK, you have the following rights:

- You may request access to the personal data we maintain about you, update and correct inaccuracies in your personal information, restrict or object to the processing of your personal information, have the personal data anonymized or deleted, as appropriate, or exercise your right to data portability to easily transfer your personal data to another company. In addition, you also have the right to lodge a complaint with a supervisory authority, including in your country of residence, place of work or where an incident took place.
- You may withdraw any consent you previously provided to us regarding the processing of your personal information, at any time and free of charge. We will apply your preferences going forward and this will not affect the lawfulness of the processing before you withdrew your consent.
- You may exercise these rights by contacting us using the contact details in clause 5.3 of this Privacy Statement. Before meeting your request, we may ask you to provide reasonable information to verify your identity. Please note that there are exceptions and limitations to each of these rights, and that while any changes you make will be reflected in active user databases instantly or within a reasonable period of time, we may retain information for backups, archiving, prevention of fraud and abuse, analytics, satisfaction of legal obligations, or where we otherwise reasonably believe that we have a legitimate reason to do so.

We specify below the possible ways that you can exercise some of these rights with regard to different parts of our Service. If you have any further questions or you wish to exercise your rights, you can do it by contacting privacy@zivver.com.

We also collect some personal data through the use of cookies. You can find more information about the data we collect this way in our Cookie Statement. You can also alter your cookie preferences whenever you like, by clicking the cookie settings link in the footnote of any page on the website. Please note that your web browser could offer the possibility to file a Do Not Track request via your browser. Given that our Service does not function optimally without the functionalities we have installed, we will not accept such requests.

In addition, if you have a personal Zivver account or receive the requested information from Zivver, you can also exercise certain of your rights in your account as follows: (i) change your personal data; and/or (ii) have your account deleted (and, as a result, your personal data along with it). Such changes to or termination of your account are effective immediately.

Please note that these rights may be limited in some circumstances by local law. Also, we may need to retain certain information for recordkeeping or legal compliance purposes or to continue to perform our obligations under the employment relationship.

For requests regarding business accounts that fall under the responsibility of an organization, you have to contact your organization. For example, if your personal data are incorrect, you should ask your organization to have the data changed or deleted.

### 5.2 Security and certificates

We have taken appropriate technical and organizational measures to secure your personal data against loss or other forms of illegitimate processing. More information about our security measures and certifications can be found on our website.

### 5.3 Contact information

Zivver B.V., with its registered office at Spaklerweg 52, 1114 AE, Amsterdam, the Netherlands, and registered with the Dutch Chamber of Commerce under number 64894665 is responsible for the processing of your personal data (also referred to as a 'controller').

You can contact Zivver via email at privacy@zivver.com. You can also contact our data protection officer via dpo@zivver.com.

## 6. Third parties

The Service may contain links to other websites, products, or services that we do not own or operate. We are not responsible for the privacy practices of these third parties. Please be aware that this Privacy Statement does not apply to your activities on these third-party services or any information you disclose to these third parties. We encourage you to read their privacy policies before providing any information to them.

## 7. Children's privacy

We do not knowingly collect, maintain, or use personal data from children under 13 years (or under 16 years for children in Europe) of age, and no part of the Service is directed to children. If you learn that a child has provided us with personal data in violation of this Privacy Statement, then you may alert us at privacy@zivver.com.

## 8. Revision of this Privacy Statement

We reserve the right to amend this Privacy Statement. If we amend this Privacy Statement, we will inform you on our website and through our newsletter. We recommend frequently consulting this Privacy Statement, so that you are up to date with any possible changes.

***