

Woov Privacy Policy

Version 2.1 – 1st of September 2021

We are Woov. We respect your privacy and private life, but sometimes we need your personal data in order to provide you with the optimal Woov experience. In this privacy policy we explain which data we use and how we save, protect and process this data. This privacy policy applies to our mobile applications Woov and Woov Live (the "Apps"), our websites www.woov.com and www.woov.live (the "Websites"), collectively the services that we offer (the "Services"). We comply with the General Data Protection Regulation and, when implemented, with the relevant provisions under Dutch law (the "Relevant Legislation").

Personal data

To offer our Apps, Websites and Services we process data, some of which can be regarded as Personal Data. Data is considered "personal data" by the relevant legislation when it contains "information or pieces of information that could allow a person to be directly or indirectly identified". This is a very wide definition. The European Court e.g. ruled that even dynamic IP-addresses may qualify as personal data.

Information we collect about you

Woov is a social platform that provides you with personal and relevant suggestions of people, festivals, concerts, parties and other events that you will likely be interested in. Once your personal profile is created, you can choose to share additional information with us such as your personal festival experiences and preferences regarding artists and events. These additional data will be processed by us and added to your profile. This information is used to facilitate our automated decision making processes to find people, events and promotions that are relevant to you. We collect Personal information in a variety of ways:

Information you provide

Woov is a social platform, which is why we ask you to make a profile by creating a Woov account. You may choose not to create an account in which case you can still use some of the features that are not related to social interaction.

To create a Woov account, you will be given the option to sign in with your Facebook account, Apple Sign-in or to create a Woov account with your e-mail address or telephone number. When doing so, you authorize us to access and store personal details like your name / alias, email address, phone number, Country of Residence and date of birth.

We may also ask you to provide us with some additional information that will be publicly visible on our services, such as a profile picture, your hometown and a tagline. If you chat with other Woov users, you provide us the content of your chats, and if you contact us with a customer service or other inquiry, you provide us with the content of that communication. Your group and private chat-conversations are strictly confidential and are only processed by us in order to give you access to your chat-history.

If you choose to make a purchase via our Services we require you to provide your payment information. We will never store any of your payment information without asking your explicit consent. When you make a payment we store (non-personal) information about the transaction like date, price and country code and link this to your account – as well as your email address where you prefer to receive the order confirmation.

Information we collect when you use our Services

When you use our Services, we collect information about which of those services you've used and how you've used them. We might know, for instance, that you visited a particular Event, joined a number of groups and / or actively took part in one of our many communities. The types of information that we might collect when you use our services are:

- **Device Phonebook.** We may ask you to share your phonebook in order to identify which of your contacts already have a Woov account. If you give us explicit permission, we will only use it to match your contacts with our database and we will never store any of your contact information on our servers.
- **Device information.** When you use the App, we automatically collect information from your device. This information could include your device brand and type, your browser type and language, the operating system used by your device, access times and IP-address. We use your mobile device ID (AAID for Android and IDFA for iOS) as a unique identifier to recognize you. We do this to store your preferences and content so we can serve you with personalized information and settings. Device IDs cannot be deleted, but can be reset in your phone's "Settings" overview.
- **Content Information.** When you upload content to our Services, like chat messages, photo's or videos, we store them on our servers. If you want to upload existing Photo's or Videos you will be asked to give us access to your photo library. We will only store the content you select to upload and use.
- **Information about how you use our Services.** In order to improve our product and services, we continuously collect data on how you use the Services including, but not limited to, the number of invites you send, the number of groups you are in, the number of artists that you favourite.
- **Location Information.** At offline events, Woov gives relevant (social) context to your location. In order for us to service you optimally we will ask you to allow Woov to collect your location information from your device when you use the App. If you give us explicit permission, this will allow Woov to collect your mobile device's geographic location while our application is actively running or running in the background. We use either use your rough or specific location to:
 - Find relevant events near you
 - Have the App know when you are at an event to improve user-friendliness.
 - Help you and your friends find each other.
 - Help us determine what your preferences are in order to improve our Services.
 - Provide anonymous and irreversibly aggregated real-time visitor heat maps to festival organisers which helps them respond adequately in terms of crowd control

Information we collect from Third Parties

If another user uploads their contact list, we may combine information from that user's contact list with other your information to determine whether you already know each other. This information will be used to create friend suggestions at that moment and will never be stored by Woov.

How will we use your information

In order to provide you with the best live music event experience, we may use information that we collect about you to:

- deliver and improve our products and services, and manage our business;
- manage your account and provide you with customer support;
- communicate with you and send you receipts of your purchases;
- personalize our services in order to send you relevant suggestions for friends, events, artists or communities for example;
- perform research and analysis about your use of, or interest in, our or others' products, services, or content;
- perform mobile application analytics; and
- perform functions or services as otherwise described to you at the time of collection.

How long do we retain your information

We shall store your personal data as long as your account is active. You can always de-activate your account, after which your personal data will be deleted – as a rule within 30 calendar days. If you want your personal data deleted on a shorter notice, please send us an email via privacy@woovapp.com. Please note that we reserve the right to store data regarding your use of our Services when they are irreversibly anonymized.

How we protect your information

We work hard to protect your personal data from unauthorized or unlawful access, alteration, disclosure, use or destruction. That way, unauthorized persons do not have access to your data. We take the following measures to protect your personal data:

- Account security: We serve our website and our APIs exclusively via HTTPS. We use JWT authentication tokens for API logins to help you protect your account data.
- Servers - Physical security: Our infrastructure runs inside data centers designed and operated by Amazon Web Services (AWS) in Ireland. AWS data centers feature state of the art environmental security controls to safeguard against fires, power loss, and adverse weather conditions. Physical access to these facilities is highly restricted and they are monitored by professional security personnel. We require all personnel to take their laptop computer with them when they leave the office, to prevent theft from our offices. No data is ever stored on these laptops. Laptops are encrypted to prevent data loss when being stolen.
- Software security: Our systems run the latest stable versions of Amazon Linux and our applications run on the latest stable version of docker. Application and database servers are not directly accessible from the internet. We monitor documented threats from public security research databases (such as the Common Vulnerabilities and Exposures catalog). Our developers receive training for secure software development, including Open Web Application Security Project guidelines. All code changes are subject to a multi-point code review with specific attention paid to security.
- DDoS mitigation: User data and specifically location can be charged subjects. We maintain firewalls on our edge servers and origin load balancers to protect against bandwidth and protocol-based attacks, and we use intelligent web application firewalls and elastic scaling of our compute capacity to mitigate attacks at the application layer, including complex and evolving attacks.
- Data security: All customer data is stored encrypted with at least dual redundancy. We store and secure chat messages in a dedicated database with no personal identifiable data attached.
- Logging: We log activity across our platform, from individual API requests to infrastructure configuration changes. Logs are aggregated for monitoring, analysis, and anomaly detection and archived in vaulted storage. We implement measures to detect and prevent log tampering or interruptions.
- Employee access: Woov team access is controlled by a carefully managed security policy. All team members sign non-disclosure agreements to protect your data. All employees receive tools and training for handling sensitive data (including credentials) and for avoiding social engineering and other non-technical attacks. Furthermore we use logging of all database sessions as a protective measure.

- Regular audits: We conduct regular internal security audits to review our hardware, software, and physical security configurations. If we discover a vulnerability, we follow a formal incident response framework to ensure rapid mitigation and transparent customer communication.

How we share information

We may share your information about you in a number of ways.

With other Woov Users

Your profile will be visible to other registered users of our Services. This includes the following information:

- Profile picture (optional)
- Name or Alias
- Events you are going to and have been to
- Your friends / connections on Woov
- Artists and or other performances you like
- Hometown (optional)
- Age (optional)
- Nationality (optional)
- Tagline (optional)
- Secret Identity (optional)
- Gender (optional)

If you have given us permission to share your location with specific users or groups, we use your geolocation to inform them where you are on the event map. You are always able to decide and select for yourself which users and/or groups you want to share your location with.

When you send chat messages to other users who are in the same group as you, they will be able to see the content of these messages.

When you send chat messages, pictures and/or videos to the community, all Woov users will be able to see this content.

Please be aware that other users are always able to take screenshots or make a recording of your Profile, locations and/or chats.

With Third Parties

Woov can share generic aggregated data with our business partners, trusted affiliates and advertisers – which will in general be companies active in the music scene. NB: These data will be presented in reports and consist out of aggregated and irreversibly anonymized and do not contain any of your personal data.

Secondly, we may share your data with third parties when we reasonably believe that disclosing the information is needed to:

- Comply with any valid legal process, governmental request, or applicable law, rule, or regulation.
- Investigate, remedy, or enforce potential Terms of Service violations.
- Protect the rights, property, and safety of us, our users, or others.
- Detect and resolve any fraud or security concerns.

Finally, we may share your data with third parties as part of a merger or acquisition. If Woov Holding BV gets involved in a merger, asset sale, stock sale, share sale, financing, liquidation or bankruptcy, or acquisition of all or some portion of our business to another company, we may share your information with that company before and after the transaction closes.

With Data Processors

We may share your personal data with companies that process data as a service to Woov. In a data processing agreement, we shall agree with those parties that they shall use your data carefully and they shall only receive the data that is relevant for their services. These parties use your data in accordance with our instructions and not for their own purposes. These parties are "processors" within the meaning of the Relevant Legislation. In the following table we have listed these Processing parties, and explain to you – in their words – what data is processed, why and where. We take care to keep this table up to date, however if you find any inconsistencies please let us know via privacy@woovapp.com.

Company	Functionality	What data	Why	Country / Transfer mechanism
Amazon Web Services Inc	Servers	- All user data	Storage of data	Ireland / GDPR
Mapbox Inc	Maps	- Anonymized location and usage data	Whenever your application causes the user's location to be gathered it is sent to Mapbox. Users can opt-out of this individually through Settings.	U.S.A. / Standard Contractual Clauses for Data Transfer
Google LLC	Firebase Cloud Messaging	- Instance IDs	Firebase Cloud Messaging uses Instance IDs to determine which devices to deliver messages to.	U.S.A. / Standard Contractual Clauses for Data Transfer
	Firebase Realtime Database	- IP addresses - User agents	Realtime Database uses IP addresses and user agents to enable the profiler tool, which helps Firebase customers understand usage trends and platform breakdowns.	U.S.A. / Standard Contractual Clauses for Data Transfer
	Google Analytics for Firebase	- Mobile ad IDs - IDFVs/Android IDs - Instance IDs - Analytics - App Instance Ids	Google Analytics uses the data to provide analytics and attribution information. The precise information collected can vary by the device and environment.	U.S.A. / Standard Contractual Clauses for Data Transfer

Other considerations

Links

You may find third party, advertising or other content on our Services that link to other websites. We do not control the content on these websites and are not responsible for the content or the privacy protection of these websites. We advise you to read the privacy policies of those websites.

Modifications to this privacy policy

We may update our privacy policy from time to time. When we change this privacy policy in a significant way, we will post a notification on our Services along with a link to the updated privacy policy. If you are not registered as user we advise you to visit the Website and this policy regularly.

Are you under the age of sixteen?

Although our Services are general audience Service, we restrict the use of our service to individuals age 16 and above. We do not knowingly collect, maintain, or use personal information from children under the age of 16.

Your rights

We consider the data we collect to be personal. Therefore, you have the following rights:

- You may request access to the personal data we process about you;
- You may request us to correct, update, shield or delete your personal information in our records. In the event of fraud, non-payment, or other wrongful act, we can keep some data in a register on a black list;
- You may request a copy of the personal data we have processed about you. We can - on your request - send this copy to another party, so you don't have to send the data yourself;
- You may file a complaint against processing your data;
- You may file a complaint to the Dutch Data Protection Authority (Autoriteit Persoonsgegevens), if you are under the impression that we process your data unlawfully;
- You may always withdraw your consent to process your data. We cannot process your data from the moment you withdraw your consent. Please be aware that when you revoke your consent we will keep your data that was stored up and onto that moment in time. If you want us to delete your data please specify this in your request.

You can exercise these rights by sending an email to privacy@woovapp.com, to which we will respond in less than 30 days. Should you have further questions regarding this privacy policy, please contact us via the information below.

Contact information

Data Protection Officer
privacy@woovapp.com

Woov BV
Overhoeksplein 31
1031KS AMSTERDAM
The Netherlands