simpleQR
create. scan. connect.

Privacy Policy of SimpleQR

Last updated: October 07.2024

Dear Users,
Commitment to the privacy of our users is paramount for Veriori SA. This Privacy Policy ("Policy") explains how we process information concerning users of our website www.simpleqr.veriori.com, mobile application, and related services (collectively referred to as the "Services"), as well as in other contexts in which you communicate with us. This document aims to inform you about our privacy practices and your rights.

By using our Services, you agree to the processing of your personal data in accordance with the principles described in this Policy. If you have any questions or concerns about this Privacy Policy or our privacy practices in general, please contact us at: simpleQR@veriori.com.

We would like to emphasize that our Privacy Policy does not cover the actions of external entities that we do not own or control, including third-party websites, services, and applications ("Third-Party Services") that may be accessible through our Services. We encourage you to review the privacy policies of any Third-Party Services you access or use. Please note that we are not responsible for the content or privacy policies of Third-Party Services, and any third-party policies linked to this Policy are for informational purposes only.

Please note that our privacy practices are subject to the applicable laws of the regions in which we operate. Thus, certain region-specific terms will only be applicable to individuals in those specific areas, or as mandated by the relevant laws. If you are a resident of the European Union, your data protection rights are covered under the General Data Protection Regulation (GDPR). For residents of Brazil, the Lei Geral de Proteção de Dados (LGPD) applies. In Singapore, we adhere to the Personal Data Protection Act (PDPA). Japanese residents are protected under the Act on the Protection of Personal Information (APPI).

For Canadian residents, the Personal Information Protection and Electronic Documents Act (PIPEDA) applies, along with any relevant provincial laws. If you are located in any other region with its own data protection laws, we commit to comply with those regulations as well.

For residents of specific U.S. states such as California, Virginia, Colorado, Connecticut, and others, please refer to the sections titled 'California Privacy Rights', 'Virginia/Colorado/Connecticut Privacy Rights', and 'Privacy Rights in Certain Other U.S. States' to learn about disclosures specific to our collection, use, and disclosure of your information, as well as additional rights you may have under U.S. state laws.

Data Controller: VERIORI SA, Aleje Jerozolimskie 142A, 02-305 Warszawa, Poland

Email: simpleQR@veriori.com.

The Data Controller ("Controller") is responsible for processing your personal data in connection with the use of the Services provided by www.simpleQR.veriori.com. We take all necessary measures to ensure the security of your personal data and to process it in compliance with applicable data protection regulations.

If you have any questions regarding the way your personal data is processed by the Controller or if you would like to exercise your rights related to the processing of personal data, please contact us directly through the above communication channels.
We reserve the right to make changes to the Privacy Policy. We will inform you of any changes with sufficient notice, allowing you to familiarize yourself with the updates.

What Data is Collected

Access to our website www.simpleQR.veriori.com does not require providing personal information, however, registration and use of our plans will require you to provide your personal data. The information we collect (personal and non-personal) may vary depending on the context. The data we collect reach us in three ways: 1) automatically, 2) voluntarily provided by the user, 3) provided by third parties.

Automatically Collected Data

These include:

- Data collected using cookies or similar mechanisms stored on your device, always with your consent or on other legal grounds. Detailed information can be found in our Cookies Policy.
- IP from which the connection is made, type of device used and its characteristics, operating system version, type of browser, language, date, country, time of request, source URL and destination URL, or the mobile network used, among others.
- Data on the use of the Service and possible errors detected during its use.
- Additionally, we use Google Analytics, an analytical service provided by Google, LLC. Cookies used by these services collect information, including the user's IP address, which will be transmitted, processed, and stored by Google in accordance with the principles described on www.google.com, including the possible transmission of this information to third parties for legal reasons or when third parties process the information on behalf of Google. You can disable Google Analytics cookies at any time.

Data You Voluntarily Provide Data collected and stored by SimpleQR:

1. **Data collected during registration:**
   a. Email address: used for communication and user account management.
   b. First and last name: used to personalize user experiences and for administrative purposes.
2. **Data collected while using the app:**
   a. Photos: Users may upload photos that can be used as profile pictures or in other app functionalities, for example, on landing pages.
   b. QR code scanning location data: we collect information such as country (code and name), region (code and name), city (name), postal code (ZIP), latitude and longitude, and ISO code.
   c. Subscription status: information about the user's subscription activity, allowing for customization of service access.
3. **Data collected in case of SSO provider login:**
   a. User ID: a unique identifier assigned by the Single Sign-On provider.
4. **Data collected but anonymized:**
   a. IP address and User Agent: These details are

b. collected when scanning QR codes and are anonymized to protect the user's privacy.

Data stored by an external service (Stripe):

- Payment data: Information about payments, including the last four digits of the payment card number, is processed and stored by the Stripe payment system.
- Invoice data and the invoices themselves: Information needed for invoicing and the documents themselves are also stored by Stripe.

Summary:

In connection with the use of our services, we directly store the following categories of data: location, email, first and last name, photos uploaded by users, and subscription status. We anonymize the IP address and User Agent of those scanning QR codes. The external payment system Stripe manages payment data, invoices, and subscription information.
We encourage you to review our Cookie Policy, which provides detailed information about the cookies and other similar technologies we use, and how users can manage their preferences in this area.

Purpose of Data Processing

SimpleQR uses the collected data for the following purposes:

1. **Managing and updating Services:**
- Legal basis: our legitimate interests in maintaining and updating our Services to keep them current and functioning properly.
2. **Responding to user inquiries:**
- Legal basis: our legitimate interests in handling inquiries and doubts of our users.
3. **Processing payments made by users:**
- Legal basis: performance of a contract.
4. **Providing the service in accordance with the contract:**
- Legal basis: performance of a contract.
5. **Maintaining the security of Services, investigating illegal activities, enforcing our terms and conditions, and supporting state security forces in the course of their possible investigations:**
- Legal basis: our legitimate interests in ensuring and maintaining the security of the Services and its users.

7. **Marketing purposes:**

- Marketing communication: We may use contact details, such as email addresses, to send information about news, promotions, or special offers that may interest you, provided you have given your consent.
- Personalized advertising: We may also process data to tailor advertisements to your interests and preferences based on our legitimate interest in promoting our Services.
- Legal basis: user consent or our legitimate interests in promoting our Services.

8. **Communication with users:**

- We may use your contact details to convey important information about the Services, such as changes in the Privacy Policy, terms of service, or other necessary administrative communications.
- Legal basis: our legitimate interests in ensuring proper communication and user support.

SimpleQR does not use automated decision-making, although we may generate basic user profiles, which constitute our legitimate interests for commercial purposes and providing personalized offers.

Moreover, SimpleQR may use information about users in the form of aggregated and anonymized data to present to third parties. We may also share statistics and demographic information about users and their use of the Services with third parties. However, none of these activities will allow these third parties to personally identify users.

Legal Basis for Data Processing

The processing of your personal data by SimpleQR is in accordance with the General Data Protection Regulation (GDPR) for residents of the European Union, relevant state and federal laws of the United States for US residents, as well as other local and international data protection regulations. We respect and comply with the applicable laws in every country where we operate. Consequently, if there are additional local data protection laws for your region, such as the LGPD in Brazil, PDPA in Singapore, PIPA in Japan, PIPEDA in Canada, or other relevant legislations, SimpleQR commits to adjusting its practices in accordance with these requirements.

Legal Basis for Data Processing according to the General Data Protection Regulation (GDPR) for the residents of the European Union:

1. **Consent:** In cases where we have asked for and obtained your explicit consent to process personal data for a specific purpose, such as direct marketing, the processing is based on Article 6(1)(a) of the GDPR.
2. **Performance of a contract:** When the processing of personal data is necessary for the conclusion or execution of a contract, such as providing our Services or managing a subscription, the legal basis is Article 6(1)(b) of the GDPR.
3. **Legal obligations:** In situations where we are obliged to process data to fulfill legal obligations, for example in the area of tax or accounting law, the processing is based on Article 6(1)(c) of the GDPR.
4. **Legitimate interests:** In some cases, data processing may be based on legitimate interests pursued by SimpleQR or by a third party, provided that these interests do not override the interests or fundamental rights and freedoms of the data subject.

The legal basis in these situations is Article 6(1). (f) of the GDPR.

Legal Basis for Data Processing for Residents of Various Jurisdictions In addition to complying with the General Data Protection Regulation (GDPR) for residents of the European Union, SimpleQR also adheres to the following data protection laws for residents of other jurisdictions: For residents of the United States:

- **Consent:** In cases requiring explicit consent, we act in accordance with relevant state laws, such as the California Consumer Privacy Act (CCPA) for California, the Virginia Consumer Data Protection Act (VCDPA) for Virginia, and other similar regulations.
- **Performance of a contract:** Similar to the GDPR, we process personal data necessary for the performance of a contract with the user.
- **Legal obligations:** We process personal data in accordance with US federal and state law when it is required to fulfill legal obligations.
- **Legitimate interests:** In cases where our legitimate interests are not overridden by the rights of the user, we process data on the basis of such interests.

For residents of Japan:

- We comply with the "Act on the Protection of Personal Information" (APPI), acting on the basis of user consent or other legal bases allowed by law to process personal data for clearly defined purposes.

For residents of Singapore:

- We adhere to the Personal Data Protection Act (PDPA), which requires us to collect, use, or disclose personal data only with consent, for the performance of a contract, or for other allowed purposes.

For residents of Brazil:

- We comply with the General Law for the Protection of Personal Data (LGPD), which requires consent to process personal data unless there are other legal bases, such as the performance of a contract, legal obligations, or legitimate interests.

For residents of Canada:

- We comply with the Personal Information Protection and Electronic Documents Act (PIPEDA) and relevant provincial laws, which require consent for the processing of personal data unless there are other legal bases. In each of these jurisdictions, SimpleQR commits to adhering to local data protection laws, and your data is processed only when there is an appropriate legal basis. We ensure that all data processing activities are in line with applicable local regulations and international standards of privacy protection. At any time, you have the right to withdraw your consent to the processing of personal data. Withdrawing consent does not affect the legality of processing that has occurred based on consent before its withdrawal. All activities related to the processing of personal data are conducted with full respect for your privacy and in compliance with applicable data protection laws.

Data Recipients Personal data collected by

SimpleQR may be shared with the following categories of recipients:

1. **Processing Entities:** Your personal data may be shared with companies we collaborate with to process data on our behalf. These entities act as data processors and include IT service providers, cloud service providers, audit services, and providers of analytical and marketing tools. We commit to collaborating only with those processors who ensure an adequate level of personal data protection and comply with data protection regulations.
2. **Business Partners:** In some cases, we may share specific personal data with our trusted business partners with whom we conduct joint promotions or offer related products and services. Any data sharing is strictly limited to the purposes for which you have given your consent and is carried out in compliance with applicable law.

3. **External Entities:** Personal data may also be disclosed to external advisors (such as lawyers, accountants, auditors) to the extent necessary for them to perform their professional duties on our behalf.
4. **Governmental Authorities:** In response to lawful requests, we may be required to disclose personal data to regulatory bodies, law enforcement, or other public authorities. In such cases, we disclose only the data that is strictly required by law.
5. **Potential Buyers:** In the event of a sale, merger, or other reorganization of the company, personal data may be shared with potential buyers under the condition that they will adhere to this Privacy Policy.

   In each case of data sharing, SimpleQR takes appropriate measures to ensure that any disclosures are compliant with applicable data protection laws and that there are adequate data protection agreements in place to ensure the security of your information.

Transfer of Data Outside the European Economic Area (EEA)

SimpleQR is aware of the importance of personal data protection and adheres to the General Data Protection Regulation (GDPR) as well as other local regulations concerning the transfer of personal data outside the EEA. In cases where personal data are transferred to countries outside the EEA that do not provide the same level of data protection as EU member states, SimpleQR applies the following safeguards:

1. **Adequacy decisions:** We prefer to transfer data to countries that have been recognized by the European Commission as providing an adequate level of personal data protection.
2. **Standard contractual clauses:** In the absence of an adequacy decision, we use standard contractual clauses approved by the European Commission, which commit the data recipients to ensure an adequate level of protection.
3. **Binding corporate rules (BCRs):** For transferring data within our global organization, we use BCRs that have been approved by the relevant data protection authorities and ensure the protection of personal data at an appropriate level.

4. **Other protective measures:** In specific situations, we may apply other protection mechanisms provided by the GDPR, such as compliance with privacy protection principles when transferring data to the USA (e.g., Privacy Shield) or obtaining explicit consent from the individuals concerned. SimpleQR always informs users of the intention to transfer data outside the EEA and the safeguards that will be applied to protect their personal data. With each data transfer outside the EEA, SimpleQR commits to adhering to applicable legal regulations and applying appropriate protective measures.

Data Retention Period

SimpleQR stores users' personal data only for the period necessary to achieve the purposes for which they were collected, or to comply with legal requirements. The data retention period is determined based on the following criteria:

1. **Registration data:** We keep registration data, such as first and last name and email address, for the duration of the user's account activity and for the period necessary for tax and legal settlements after the end of the use of our services.

3. **Customer service-related data:** Correspondence with the user regarding support and inquiries is kept for the period necessary to provide proper service and for evidential purposes in the event of disputes.
4. **System logs and analytical data:** These data are stored for the period necessary to analyze trends, manage and improve the system, and protect security and manage risk.
5. **Marketing data:** Data used for marketing purposes are kept until the user withdraws consent or after the marketing campaign for which they were needed has been completed. After the retention period has expired, personal data are anonymized, archived for statistical or historical purposes, or securely deleted. SimpleQR complies with applicable legal regulations regarding the minimum and maximum periods for data retention.

User Data Rights

As a SimpleQR user, you have a number of rights related to your personal data that we process. Below are the basic rights that apply depending on the jurisdiction:

1. **Right of Access:** You have the right to obtain confirmation from us as to whether personal data concerning you are being processed, and access to such data.
2. **Right to Rectification:** If personal data are incorrect or incomplete, you have the right to request their update or rectification.
3. **Right to Erasure ("Right to be Forgotten"):** In certain circumstances, you have the right to request the deletion of personal data concerning you.
4. **Right to Restriction of Processing:** In certain conditions, you may request the restriction of processing of your personal data.
5. **Right to Data Portability:** You have the right to receive personal data in a structured, commonly used format and to transmit those data to another controller.

7. **Rights Related to Automated Decision Making, Including Profiling:** You have the right not to be subject to a decision based solely on automated processing, including profiling, which has legal effects on you or similarly significantly affects you.
8. **Right to Withdraw Consent:** If processing is based on your consent, you have the right to withdraw it at any time, but this will not affect the lawfulness of processing based on consent before its withdrawal.
9. **Right to Lodge a Complaint with a Supervisory Authority:** If you believe that the processing of personal data violates GDPR or other local data protection laws, you have the right to lodge a complaint with the relevant supervisory authority. For residents of California, Virginia, Colorado, Connecticut, and other US states, you have additional rights under state laws, such as the right to request information about the categories of personal data we collect, the purposes of processing, and the categories of recipients to whom the data are disclosed.

Data Security

At SimpleQR, we make every effort to ensure the security of your personal data. We have implemented a range of organizational, technical, and physical measures to protect data from unauthorized access, alteration, disclosure, or destruction. Here are the main safeguards we use:

1. **Data Encryption:** Sensitive data, such as financial information and login details, are encrypted during transmission using SSL (Secure Socket Layer) technology and stored in encrypted form.
2. **Access Management:** Access to personal data is strictly limited to those employees and external entities who need this data to perform their tasks. We provide appropriate data protection training to all employees and external entities.
3. **Regular Security Audits:** We regularly conduct security audits to identify and rectify potential weaknesses in our systems and processes.
4. **Data Breach Procedures:** We have established procedures to be followed in the event of a data security breach, including notifying the relevant supervisory authorities and users in accordance with applicable laws.

5. **Internal Policies and Training:** We have introduced data protection policies and regular training for our employees to increase awareness and understanding of the importance of protecting personal data.
6. **Physical Security**: The physical protection of our servers and IT infrastructure includes security measures such as access control, monitoring systems, and fire protection.
7. **Technical Safeguards:** We use firewalls, intrusion detection and prevention systems, and other advanced technologies to help protect your data from unauthorized access or unwanted actions.

Cookies and Tracking Technologies

SimpleQR uses cookies and various tracking technologies to improve the quality of our services, personalize user experiences, and analyze website traffic. Detailed information on this matter is as follows:

1. **Cookies:** These are small text files that can be placed on your device by our website. We use cookies to remember user preferences, facilitate navigation on the site, and collect analytical data that helps us optimize our site.
2. **Session and Persistent Cookies:** We use session cookies (which expire after closing the browser) and persistent cookies (which remain on your device until they expire or are deleted) to ensure continuity of experiences and functionality of our services.
3. **Tracking Technologies:** These may include beacons, tags, and scripts used to collect and track information and to improve and analyze our Services.
4. **Third-Party Cookies:** In addition to our own cookies, we may also use cookies provided by third parties that enable the provision of additional services such as analysis of our website usage or advertising.
5. **Cookie Management:** Most web browsers allow you to control cookies through the browser settings. You can decide to accept or reject cookies and also delete cookies that have already been stored. Please be aware that if you choose to

block cookies, it may affect the availability and functionality of our Services.

6. **Cookie Policy:** For more detailed information about the specific cookies we use, their methods of use, and management options, please refer to our Cookie Policy.

Changes to the Privacy Policy

SimpleQR reserves the right to update and change this Privacy Policy as our services evolve and as data protection laws change. Any significant changes will be communicated to you via our website or, where appropriate, directly by email. We recommend regularly reviewing the Privacy Policy to stay informed about our privacy protection practices. The date of the last update will always be found at the top of the document.

Contact Information

If you have any questions or concerns regarding our Privacy Policy or practices related to data protection, please contact us:
Email: simpleQR@veriori.com