Privacy Policy

OVERVIEW
The ROAR Experience Intelligence Platform
EFFECTIVE DATE 25 MAY, 2018
UPDATED 28 JUNE, 2020

INTRODUCTION
This notice addresses the data ROAR collects to provide our SaaS platform and services to our clients. Clients use this platform to collect customer feedback through different channels, including surveys and integrations with other platforms. ROAR also provides reporting applications that allow our clients to view and analyze the collected feedback.

In our privacy notice, we use the following terms:

- "ROAR Experience Intelligence Platform" refers to the SaaS platform and provision of professional services for implementation of this platform we provide to our clients.
- "client" refers to a business to which ROAR provides its services and SaaS platform
- "customer" refer to an individual who has had an interaction with a ROAR client and whose feedback is collected through the ROAR Experience Intelligence Platform. Customer interactions can span a wide variety, and include interest in, or, purchasing of goods or services, contacting customer support, checking in to a hotel or property, and visiting a client's web page or using its mobile app.
- "respondent" refers to an individual who is prompted to provide feedback to one of ROAR's clients through the ROAR Experience Intelligence Platform.

WHAT DATA WE COLLECT AND HOW WE COLLECT IT
ROAR's and our Clients' Roles in Data Collection. In providing the ROAR Experience Intelligence Platform to our clients, ROAR collects data only according to our clients' instructions and the data processing agreement between ROAR and our clients. Our clients specify what customers we should contact to provide feedback, when we should contact them (for example, after completing a purchase at a client's retail store), how we should contact them (for example, email or SMS), how often we should send them reminders to provide feedback, and what questions are asked. ROAR's clients also decide whether to use inbound or outbound data integrations, and how to use or respond to feedback that is collected.

ROAR enters into agreements with our clients that legally obligate ROAR to protect data we receive or are directed to collect, and use it only to provide the products and services specified by the client. Under many data protection laws, including the EU's General Data Protection Regulations, ROAR is considered a "data processor" to our clients, and our clients

are considered “data controllers.”

As data controllers, ROAR clients are responsible for complying with laws that may require notice, disclosure or consent from end-customers related to the transfer of data to ROAR or data use in the ROAR Experience Intelligence Platform.

For more information on the types of data collected by a particular ROAR client, refer to the privacy notice or communications of that specific ROAR client. Our clients’ privacy notices are commonly located in the ROAR survey invitation (for web-based surveys).

Legal Basis for Processing. ROAR clients provide instructions with regard to the upload, collection, transfer, and access of personal data in the ROAR Experience Intelligence Platform. As such, ROAR clients determine the legal basis they have for data processing. ROAR clients can use legitimate interest or consent as a legal basis for processing personal data in the ROAR Experience Intelligence Platform, although other regulations may apply. For more information, refer to the privacy notice or communications of the ROAR client.

Identity of the Data Controller. As data controllers, ROAR clients are responsible for identifying themselves, where appropriate, in communications sent by the ROAR Experience Intelligence Platform. For example, ROAR survey invitations sent by email or SMS should identify the name of the ROAR client directing us to conduct the survey. If you are having trouble identifying the data controller (client) associated with a particular ROAR survey, please contact ROAR survey support at info@roarinc.com.

Web-based Surveys. In web-based surveys offered by the ROAR Experience Intelligence Platform, customers or employees receive a survey invitation and respond to the survey in a web interface. To send survey invitations ROAR clients can, for example, provide the ROAR Experience Intelligence Platform customer names, email addresses, and information about the customers’ interactions with their business (e.g., the name of the client’s store where the customer shopped). In addition, ROAR clients can provide the ROAR Experience Intelligence Platform with information that segments customers into groups, such as the type of account the customer holds, the type of product or service purchased, or the whether the customer is enrolled in a loyalty program.

When a respondent navigates to a ROAR web-based survey, ROAR may collect the respondent’s IP address, the date and time the respondent accessed the survey, survey responses (typically numerical scores and narrative text responses), how far the user has navigated in the survey, and the type of device and web browser the customer used to access the survey. In some surveys, clients also direct ROAR to collect the geographical location of the customer’s device that is used to access the survey.

Digital Surveys. In these surveys, customers are prompted to respond to a survey within a client’s digital channels, such as a web page or mobile application. Clients can configure these surveys to:

- prompt customers for information such as name, email, a survey score, and a narrative text response to a prompt;

- collect analytics information (such as the customer's IP address and type of web browser or mobile device);
- collect customer ID (such as the login name or email the customer uses to access the client's web site or mobile application); and
- allow customers to take a screenshot that captures portions of the client's web page or mobile application.

Integrations. Clients can integrate other tools, processes or platforms as inbound sources of data for the ROAR Experience Intelligence Platform, such as CRM platforms or marketing tools.

Clients can also configure the ROAR Experience Intelligence Platform as an outbound source of data for other tools, processes, or platforms, such as collaboration tools. Clients and any third parties associated with those tools, processes, or platforms are responsible for managing personal data outside the ROAR Experience Intelligence Platform. For example, clients can configure surveys to prompt customers to write reviews on third-party websites. If a customer chooses to submit a review for publication on that third-party site, any information the customer provides on that site is governed by the privacy notice or communications of that site.

ROAR Reporting Applications. ROAR provides clients web-based and mobile applications that are used by employees of ROAR clients to review and analyze customer feedback (referred to as "reporting applications" in this notice). To provide their employees access to these applications, clients can send ROAR employee names, identifiers (e.g., an employee ID, e-mail address, or cell phone number), job title or function, and the store or business location they are associated with.

When an employee accesses a ROAR reporting application, ROAR collects the employee's user name, IP address of the device used to access the reporting application, geographic area associated with the IP address, type of web browser and mobile device, time and date that the reporting application was accessed, and areas of the reporting application that were visited. Employees can also leave notes on feedback records.

Social Media Features and Widgets. Clients can configure surveys and Lead Alerts and ROAR Alerts to include social media data. ROAR uses customer e-mail addresses to collect social information available online where permissible. Clients can also have ROAR configure surveys to include social features, such as the Facebook Like button and widgets, such as the "share this" button. This feature may collect your IP address, which page you are visiting on our site, and may set a cookie to enable the feature to function properly. Your interactions with these features are governed by the privacy notice or privacy-specific communications of the company providing them.

Information ROAR Does Not Collect. The ROAR Experience Intelligence Platform does not collect sensitive data, such as credit card numbers or government identification numbers, nor does it collect information defined as "sensitive personal data" under EU law, such as race, sexual orientation, or union membership.

HOW PERSONAL DATA IS USED

By ROAR and Partners. ROAR adheres to GDPR and Privacy Shield Principles. ROAR uses personal data uploaded from clients and customer input from surveys and social media gathered in the ROAR Experience Intelligence Platform to provide the SaaS platform and services for which the client has engaged ROAR.

These uses can include contacting a client's customers to provide feedback for web-based and digital surveys, providing gathered feedback to clients and assisting the client in managing data in the ROAR Experience Intelligence Platform, and analyzing the data gathered to improve the client's business.

ROAR Clients. ROAR clients can use personal data collected in the ROAR Experience Intelligence Platform to improve their customers' experiences with their business. Clients can use ROAR's reporting applications to provide customer feedback to their front line employees, as well as managers and executives. Clients can also perform analysis in customer feedback to prioritize and make operational changes to their business, and use personal data gathered in the ROAR Experience Intelligence Platform to send follow-up communications customers.

WHO ACCESSES PERSONAL DATA

ROAR Helpdesk and Develop Systems Support. If there is a support request, troubleshooting issue, or technical error (e.g., bug or product malfunction) that requires access to personal data, ROAR support and engineering staff who are needed to address the issue will access that data.

Access to personal data stored in the ROAR Experience Intelligence Platform is provided using systems, procedures and controls approved by ROAR's security team and audited by ROAR's Data Protection Officer. Access is provided only as long as needed to perform the necessary work.

Third Party Professional Services, Servicing and Support. If permitted by a client, ROAR can use third parties to provide survey call interviews, and support for respondents and employees. ROAR clients can also provide access to the ROAR Experience Intelligence Platform to third party partners to perform systems integration, consulting, market research or servicing. Should problems or damage be suffered by customers from the use of the 3rd party providers, ROAR assumes liability only within the scope of the agreed upon contract with the 3rd party. Any additional liability related to issues or problems arising outside the scope of services contracted with the 3rd party will not be the responsibility of ROAR.

ROAR Clients. ROAR clients can provide their employees, and franchisees' employees access to the ROAR Experience Intelligence Platform so that they can view and analyze gathered feedback. For more information, please contact the appropriate ROAR client.

Third-Party Technology Providers. ROAR transfers personal data as needed to vendors who support our technical operations, assist with data transmission (including SMS and E-Mail delivery), and provide cloud services, including data storage. These third-party providers include Microsoft, Mailgun, Zero Bounce, and Twilio. Depending on the technology integrations or features chosen by a ROAR client, we also transfer personal data of our client's respondents as needed to provide the integrations or features (including, for example, interactive voice response, SMS, machine translation, or screen capture features).

Security. ROAR maintains a security program with appropriate organizational and technical security measures to protect data stored in the ROAR Experience Intelligence Platform.

Storage Period. The data of a ROAR client is retained in the ROAR Experience Intelligence Platform until the termination of the client's subscription, unless earlier deleted or modified per the client's request, including the case of employee or franchisee terminations, or changed client usage requirements.

Data Subject Rights (for EU individuals) The ROAR Experience Intelligence Platform provides clients tools and processes for data modification, export, or deletion. If you are a respondent who wants to modify, access, or delete personal data associated with you in the ROAR Experience Intelligence Platform, please contact the appropriate ROAR client. If you have difficulty contacting the appropriate client please contact ROAR's European Legal Representative, Charles Mills, or ROAR's Data Privacy Officer, Corrado Luppi at info@roarinc.com

Opt Out and Withdrawal of Consent.ROAR offers its clients opt-out mechanisms to include in communications to individuals. Respondents who exercise an opt-out will be added to ROAR's opt-out list for the relevant client as required by applicable law. For each client, ROAR does not send survey invitations to any cellphone number or e-mail address on the applicable opt-out list. ROAR may also provide its opt-out lists to clients and their agents on a timely basis so that they may, where appropriate, update their records. If you are a respondent who wishes to withdraw your consent from all data processing by a particular ROAR client, please contact the client.

INTERNATIONAL DATA TRANSFER AND ADEQUACY LAWS

Personal data of data subjects will not be processed by ROAR or third parties outside of countries that have data protection laws different from those applicable to the data subjects. To satisfy adequacy requirements related to this international data transfer (such as those in the EU), ROAR is compliant with General Data Protection Regulations (GDPR) and Privacy Shield governing the collection, usage, storage, and distribution of personal data. When requested by legal authorities to disclose personal information, ROAR will inform the court of various factors justifying confidentiality and respondent anonymity. ROAR will communicate with the affected client or individual as soon as possible, unless prohibited by law or court order.

Disclosure of Data for Merger, Acquisition or Sale. If ROAR is involved in a merger, acquisition or sale of all or a portion of its assets, ROAR may transfer data discussed in this notice to the buyer or new parent company. In this circumstance, the appropriate clients will be notified

about the change in ownership and choices they may have regarding personal data.

Collection of Personal Data of Minors. ROAR clients can use the ROAR Experience Intelligence Platform to gather feedback from individuals under 16. Such clients are responsible for complying with any applicable laws that require notice, disclosure or consent to individuals under 16.

For more information, refer to the privacy notice or privacy-specific communications of the ROAR client.

Complaints.You have the right to complain to a data protection authority about our collection and use of your personal information. For more information, please contact your local data protection authority. Further questions regarding ROAR data protection or data privacy can be forwarded to the ROAR Data Protection Officer, Corrado Luppi at privacy@roarinc.com

ROAR, LLC complies with the *EU-U.S. Privacy Shield Framework and/or the Swiss-U.S. Privacy Shield Framework(s)* as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal information transferred from the *European Union and/or Switzerland* to the United States. ROAR, LLC has certified to the Department of Commerce that it adheres to the Privacy Shield Principles. If there is any conflict between the terms in this privacy policy and the Privacy Shield Principles, the Privacy Shield Principles shall govern. To learn more about the Privacy Shield program, and to view our certification, please visit https://www.privacyshield.gov/.

In compliance with the Privacy Shield Principles, ROAR, LLC commits to resolve complaints about our collection or use of your personal information. EU and Swiss individuals with inquiries or complaints regarding our Privacy Shield policy should first contact *privacy@ROARINC.com*

Privacy complaints received by ROAR undergo the following process for resolution:

1. Review of the complaint internally
2. Review of the complaint with the client
3. Contacting the complainant to address concerns, including removal of all customer personal information in ROAR databases
4. Conclude case
5. Forward unclosed case to executives for further resolutions

ROAR's Privacy Shield activities and processes are governed by, and capable of being investigated by, the Federal Trace Commission (FTC) of the US.

ROAR, LLC has further committed to refer unresolved Privacy Shield complaints to International Centre for Dispute Resolution, an alternative dispute resolution provider located in the United States. If you do not receive timely acknowledgment of your complaint from us, or if we have not addressed your complaint to your satisfaction, please visit https://go.adr.org/privacyshield.html for more information or to file a complaint. The services of International Centre for Dispute Resolution are provided at no cost to you. Under certain conditions, individuals may have the right to invoke binding arbitration on ROAR.

Under certain, highly specific conditions, ROAR may be required to disclose personal information of US citizens in response to lawful requests by public authorities, including to meet national security or law enforcement requirements.

Please forward further questions or comments on ROAR, LLC privacy to info@roarinc.com.