

Organic Response Privacy Policy

Effective Date: 03 Jul 2026

This Privacy Policy explains how Organic Response AB (“Organic Response”) collects, uses, and discloses personal information, along with your choices and rights regarding your data.

Scope of this Privacy Policy

This Privacy Policy governs the personal information Organic Response collects as a controller under the General Data Protection Regulation (GDPR). Such as through <http://www.organicresponse.com> and other Organic Response websites (collectively, the “Websites”), as well as various interactions (e.g., marketing activities, recruitment, customer service inquiries, user conferences, etc.)

A separate agreement governs the provision of Organic Response's subscription services (the “Services”) to customers (the “MSA”), including the processing of personal information contained in the data customers to the Services (“Customer Information”). This Privacy Policy does not apply when Organic Response collects personal information as a processor on behalf of a customer of the Services, nor to any third-party applications, software, products, or services that integrate with the Services (“Third-Party Services”), though it may reference those activities for purposes of clarity.

Obligation to Provide Data

In certain circumstances, you are required to provide personal data to enable us to provide our services, fulfil contractual obligations, comply with legal requirements, or respond to your requests.

Examples of personal data that may be required include:

- Account registration information, such as your name and email address;
- Authentication and login information;
- Contact information required to provide support services;
- Information necessary for contractual, billing, or legal purposes.

If you choose not to provide personal data that is necessary for these purposes, we may be unable to:

- Create or maintain your account;
- Provide requested services;
- Respond to support enquiries;
- Enter into or perform a contract with you; or

- Comply with our legal obligations.

Where the provision of personal data is optional, this will be made clear at the point of collection.

Information Organic Response Collects and Receives

Organic Response is committed to transparency about the personal data we collect and process. We collect only the information necessary to provide, maintain, and improve our building management and lighting system services. The data we collect falls into the following categories:

Personal information submitted or provided to Organic Response

- **Account Data:** When customers subscribe to our services or grant employees' access to the Organic Response Portal ("Authorized Users"), they provide account and profile data. This includes billing and contact information, profile picture, professional details, and account preferences. For example, to create a Portal account, you or your employer supplies an email address, building name, and similar account details.
- **Support and Customer Service:** We collect personal information when you submit a request via our operations support channels, including contact information, details of your issue, and related documentation or screenshots.
- **Marketing and Communications:** We collect names, titles, and contact details submitted through our website forms, surveys, or events to identify potential business leads and support our existing customer base.
- **Cookie information:** Cookies and similar tracking technologies of third parties, which may collect personal information about you and across other websites and online services. For more details about how we use these technologies, and your opt-out opportunities and other options, please see <https://organicresponse.atlassian.net/wiki/x/GIBr9Q>

Personal information Organic Response generates or collects automatically

- **Usage and Sensor Data:** We collect data derived from your use of our services and connected devices, including:
- **Services Metadata:** Contextual data about how Authorized Users interact with the Portal, including SSO connection information to customer Active Directories and API tokens.
- **Log Data:** Our servers automatically record information such as IP addresses, browser types, settings, and the date/time of service use.
- **Device Information:** We collect information about devices accessing our services, including operating system types and unique device identifiers.
- **Location Information:** We receive information that helps us approximate your location, such as building geographical information or IP addresses received from your browser or device.

Personal Information Organic Response collects from other sources

- **Business Partners and Service Providers:** We may receive personal information from partners, analytics providers, and resellers to better understand our customer base.
- **Public and Commercial Databases:** We may collect information from publicly available sources, including professional social networks or company websites, to update our records.

How Organic Response Uses Information

Legal Basis for Processing Personal Data

Under the General Data Protection Regulation (GDPR) and applicable privacy laws, Organic Response must have a valid legal basis to collect and process your personal information. The table below outlines how we use your information for our day-to-day business operations and services, the categories of personal data involved, and the respective legal basis under Article 6 GDPR:

Purpose of Processing	Categories of Personal Data	Legal Basis (GDPR Article 6)
Account Information Creating and maintaining user accounts, verifying authorised access, authenticating users, managing account settings, and enabling secure use of the Organic Response Portal and related services.	Contact details (name, email), Account usage, Authentication, access details.	Article 6(1)(b) GDPR – Performance of a Contract: Necessary to create and maintain user accounts and provide access to the Organic Response Portal and related services.
For Billing and Account Management Invoicing, managing subscriptions, and communicating essential service-related notices.	Contact details (name, email), financial/billing details, subscription records	Article 6(1)(b) GDPR – Performance of a Contract: Essential for managing your account and contract administration.

To Provide Operations Support Responding to support tickets, troubleshooting hardware or software issues, and providing technical guidance.	Contact details, support ticket records, technical logs, support communications	Article 6(1)(b) GDPR – Performance of a Contract; and Article 6(1)(f) GDPR – Legitimate Interests: Necessary to respond to customer inquiries and ensure effective customer support.
To Improve and Develop New Features Analysing usage trends and sensor data (such as occupancy and energy metrics) to optimise services and build smart building functionalities.	Contact details, enquiries from customers	Article 6(1)(f) GDPR – Legitimate Interests: Necessary for our legitimate business interest in refining, securing, and developing our smart building technologies.
To Ensure Security and Compliance Investigating security incidents, preventing system abuse, and maintaining continuous security monitoring and compliance.	Contact details, enquiries from customers, vulnerabilities or security issues reported to us.	Article 6(1)(f) GDPR – Legitimate Interests: Necessary to protect network security and customer data; and Article 6(1)(c) GDPR – Legal Obligation: Where monitoring is required by regulatory security frameworks.
For Marketing and Business Development Sending promotional communications about new products, events, or service updates.	Contact details (name, business email), communication preferences	Article 6(1)(a) GDPR – Consent: Where required by law (e.g., opt-in marketing); or Article 6(1)(f) GDPR – Legitimate Interests: For B2B marketing to existing business contacts (with an opt-out option).
As Required by Law Complying with applicable laws, regulations, tax requirements, or governmental requests in our operating jurisdictions.	Identity information, transaction records, governance and legal documentation	Article 6(1)(c) GDPR – Compliance with a Legal Obligation: Necessary to satisfy statutory obligations under applicable EU, Member State, or national laws.

Website Analytics and Cookies

In addition to the business processing activities above, our marketing website collects online telemetry and device identifiers via Google Analytics and other non-essential cookies. The legal basis for setting non-essential cookies is your explicit consent (Article 6(1)(a) GDPR), which you can manage or withdraw at any time via our website cookie banner. For full details on our cookie usage, session cookies, and transfer safeguards, please refer to our [Cookie policy](#).

Data Retention

Organic Response retains your personal information only for as long as necessary to fulfill the purposes for which it was collected, as outlined in this Privacy Policy, or as required by statutory retention laws.

When determining specific retention periods, we consider the amount, nature, and sensitivity of the data, the potential risk of harm from unauthorised use, the purposes for which we process it, and applicable legal, tax, or accounting requirements.

The specific retention schedules applied to each category of personal data are detailed below:

Personal Data Category	Purpose / Description	Specific Retention Period
Financial & Billing Records	Invoices, payment records, tax details, and transaction history	Retained for 7 years following the end of the relevant financial year, in accordance with statutory accounting and tax obligations (e.g., Swedish Accounting Act / local statutory laws).
Customer Support Records	Support tickets, technical inquiry logs, and communication history	Retained for up to 3 years following ticket resolution to assist with ongoing account management, service quality, and dispute resolution.
System Event & Security Logs	System logs, network data flow logs, and audit trails	Retained for 1 year from creation for security monitoring, threat detection, and incident response obligations.

Marketing Contacts & Preferences	Contact details for promotional communications and newsletter subscriptions	Retained until you withdraw your consent or opt-out. Upon opt-out, contact details are kept on a suppression list for up to 3 years to ensure compliance with your preference.
Backup & Business Continuity Data	System disaster recovery backups containing encrypted operational data	Retained on a rolling backup schedule for up to 90 days , after which backups are overwritten in the ordinary course of business.
Website & Analytics Cookies	Cookie identifiers and web telemetry (e.g., Google Analytics)	Session cookies are deleted upon closing your browser. Persistent analytics cookies are retained for up to 1, one month (or as detailed in our Cookie Policy).
Recruitment Records	Candidate applications, CVs, cover letters, interview notes, assessment outcomes, reference information, and recruitment communications used to assess suitability for current or future employment opportunities and to manage the recruitment process.	Retained for 2 years after the recruitment process ends (Unsuccessful candidates)

Criteria for Data Erasure

When personal data reaches the end of its retention period, or upon a verified request for erasure under GDPR Article 17, Organic Response will either:

1. **Permanently and securely delete** the data in accordance with our Data Management Policy; or
2. **Anonymise** the data so that it can no longer be associated with or used to identify an individual, in which case it may be retained for statistical and analytical purposes.

How Organic Response Shares and Discloses Information

This section describes how Organic Response AB may share and disclose information.

- **Service Providers and Sub processors:** We engage third-party service providers to process information to support our business operations. This includes, for example, providers of cloud infrastructure, security monitoring, and marketing communications. To the extent necessary and applicable, these parties are bound by confidentiality obligations and are only permitted to process personal information as necessary to provide their services to us. A current list of our sub processors used to deliver our Services is maintained in our Trust Centre at [Trust Centre link]
- **Third-Party Integrations:** Customers may choose to connect third-party services to the Services. When these integrations are enabled, we may share information with those third parties as requested. These third-party services are not controlled by Organic Response and are governed by their own privacy policies.
- **Corporate Affiliates:** Organic Response may share information with our parent company, subsidiaries, or corporate affiliates to support internal business operations, global support, and analytics.
- **Business Transactions:** In the event of a merger, acquisition, reorganisation, or sale of assets, information may be transferred as part of the transaction, subject to standard confidentiality arrangements.
- **Legal Compliance and Law Enforcement:** If we receive a request from a government or law enforcement agency, we will attempt to redirect the agency to the Customer directly. If compelled to disclose information, we will provide the Customer with reasonable notice and cooperation to seek a protective order, unless legally prohibited from doing so. We do not voluntarily disclose customer information to government agencies unless required by law.
- **Protection of Rights and Safety:** We may disclose information to enforce our contracts and policies, protect the safety and property of Organic Response or our users, and to investigate or prevent fraud and security issues.
- **With Your Consent:** We may share personal information with third parties whenever we have received explicit consent to do so.

International Data Transfers

Organic Response primarily processes and store data within the European Economic Area (EEA). Personal data may be transferred to and processed in countries outside the EEA, including countries where Organic Response or its service providers operate. Where such transfers occur, Organic Response ensures appropriate safeguards are in place, including:

- Standard Contractual Clauses approved by the European Commission, or
- Transfers to countries subject to an adequacy decision.

Further information regarding transfer destinations and safeguards may be provided upon request.

Your Rights under GDPR and How to Exercise Them

Depending on your jurisdiction, you may have specific rights in relation to your personal information. Subject to any exemptions provided by law, this includes the rights to:

- **Right of Access (Art. 15):** You have the right to request a copy of the personal data we hold about you.
- **Right to Rectification (Art. 16):** You have the right to request that we correct inaccurate or incomplete personal data.
- **Right to Erasure / "Right to be Forgotten" (Art. 17):** You have the right to request the deletion of your personal data where there is no legal requirement or compelling legitimate reason for us to retain it.
- **Right to Restriction of Processing (Art. 18):** You have the right to request that we temporarily or permanently restrict the processing of your personal data under certain conditions.
- **Right to Data Portability (Art. 20):** You have the right to receive your personal data in a structured, commonly used, and machine-readable format and transfer it to another controller.
- **Right to Object (Art. 21):** You have the right to object to our processing of your personal data based on legitimate interests or for direct marketing purposes.
- **Right to Withdraw Consent (Art. 7(3)):** Where processing is based on consent (such as for non-essential cookies), you have the right to withdraw your consent at any time without affecting the lawfulness of processing conducted prior to withdrawal.
- **Right to Lodge a Complaint:** You have the right to submit a complaint to a supervisory authority (such as the Swedish Authority for Privacy Protection / IMY or your local Data Protection Authority).

Organic Response may require verification of the requester's identity before processing a request to ensure the protection of personal data. Requests will be handled in accordance with applicable data protection laws and our internal compliance procedures.

In addition, if Personal Data is to be used for a new purpose that is materially different than what it was collected or authorised for, or disclosed to third parties other than our agents, Organic Response will communicate that and allow you to choose to have your Personal Data so used or disclosed.

To exercise these rights please contact at privacy@organicresponse.com.

Data Protection Authority

Organic Response has identified the Swedish Authority for Privacy Protection (Integritetsskyddsmyndigheten - IMY) as its Lead Supervisory Authority in the EEA. If you

are a resident of the EEA and believe we maintain your Personal Data within the scope of the General Data Protection Regulation (GDPR), you may direct questions or complaints to privacy@organicresponse.com or our lead supervisory authority at imy@imy.se or visit www.imy.se.

If you are a resident of the United Kingdom and believe we maintain your Personal Data within the scope of applicable laws relating to personal data in the United Kingdom, you may direct questions or complaints to the UK supervisory authority, the [Information Commissioner's Office](#).

Consent Collection and record-Keeping

Where consent is required as the legal basis for processing personal data, Organic Response obtains consent through clear affirmative actions, such as opt-in mechanisms, cookie banners, or explicit user interactions.

Records of consent are maintained in accordance with applicable legal requirements and internal compliance policies to demonstrate when and how consent was obtained.

You have the right to withdraw your consent at any time. Consent may be withdrawn using the same method by which it was provided, or by contacting us using the details set out in this Privacy Policy.

Withdrawal of consent does not affect the lawfulness of any processing carried out before the consent was withdrawn.

For further information regarding your rights, including the right to withdraw consent, please refer to the section titled "Your Rights and Choices".

Children's Privacy

Our Service is not intended for children under 13 years of age (or the relevant age of consent in your jurisdiction). We do not knowingly collect data from children under this age. In the case we discover that a child under 13 has provided us with personal information, we immediately delete this from our servers. If you believe a child has provided us with personal data, please contact us for removal.

Automated Decision-Making

Organic Response does not use automated decision-making or profiling to make decisions that have legal or similarly significant effects on individuals. Decisions affecting individuals are reviewed and made by people, not solely by automated systems.

Security

Security is fundamental to our mission. We use industry-standard technical and organisational measures to protect your data from loss, misuse, and unauthorised access. Our security framework is managed through our ISO 27001-certified ISMS, which includes encryption, strict access controls, and continuous monitoring.

While we take extensive steps to protect your information, no system is 100% secure. We cannot guarantee absolute safety from all intrusions during transmission or storage.

Links to Other Sites

Our Service may contain links to other sites. If you click on a third-party link, you will be directed to that site. Note that these external sites are not operated by us. Therefore, we strongly advise you to review the Privacy Policy of these websites. We have no control over, and assume no responsibility for the content, privacy policies, or practices of any third-party sites or services.

We are not responsible for Third Parties which customers connect to our Services via an API.

Changes to This Privacy Policy

We may update our Privacy Policy from time to time. Thus, we advise you to review this page periodically for any changes. We will notify you of any changes by posting the new Privacy Policy on this page. These changes are effective immediately upon posting. If you disagree with this Privacy Policy, you should cease interacting with the Websites.

Contact Us

Organic Response AB

Registration number 559388-1690

Postal & Visiting Address: Drottninggatan 23, 582 25 Linköping, Sweden

Telephone Number: +46 73 317 71 04 (073-317 71 04)

Global / Australian Office: Level 1, 70 Trenerry Crescent, Abbotsford VIC 3067, Australia

Email: privacy@organicresponse.com

Website: <https://www.organicresponse.com/contact-us>