

Privacy Policy

Flux Tailor LLC — UtiliPub™

Effective Date: July 27th, 2026 **Last Updated:** July 27th, 2026

Introduction

Flux Tailor LLC (“Flux Tailor,” “we,” “us,” or “our”) operates UtiliPub™, a software platform for utility rate plan management and publication. This Privacy Policy describes how we collect, use, disclose, and safeguard information in connection with our website at fluxtailor.com and related properties (including product-specific subdomains), our marketing and business operations, and the UtiliPub™ platform itself.

We respect the privacy of individuals who interact with our business. Where we process personal information on behalf of one of our customers (for example, utilities that deploy UtiliPub™ widgets on their own websites), we do so as a processor under that customer’s direction, governed by our Master Subscription Agreement and Data Processing Agreement with that customer.

Scope of this Policy

This Policy covers:

- Visitors to our websites and product properties;
- Prospective customers, business contacts, and professional correspondents who interact with us directly;
- Authorized users at our customers who access UtiliPub™ to manage rate plan data and related workflows; and
- End users (for example, utility ratepayers) who interact with UtiliPub™ widgets that our customers embed on their own websites — subject to the separate responsibility of the deploying customer described below.

What this Policy does not cover

When a customer embeds a UtiliPub™ widget on its own website, the customer controls what data is collected from end users and how that data is used in the customer’s own systems. The customer’s own privacy policy governs the customer’s data practices, including cookies and analytics the customer sets on its own domain. This Policy covers only the information that we, as the service provider, receive and process in our role operating the platform.

Information We Collect

Website visitors and business contacts

When individuals interact with our websites or correspond with us directly, we may collect:

- Contact information you provide (name, employer, job title, email, phone, postal address);
- Correspondence content (emails, form submissions, inbound support messages);
- Website-usage information (pages visited, referring URLs, browser type, device type, approximate location derived from IP address, timestamps);
- Event and marketing-list information (event registrations, newsletter subscriptions).

Customer personnel using UtiliPub™

When an individual is provisioned as an authorized user of our customer’s UtiliPub™ subscription, we collect:

- Account credentials and associated profile information (name, employer, work email, role);
- Authentication and session information (log-ins, IP addresses, user-agent strings, session timestamps);
- Activity logs describing actions performed within UtiliPub™ (rate plan edits, exports, API calls, calibration runs), which we use to provide, secure, and improve the platform.

Widget end users (for example, utility ratepayers)

When our customer deploys a UtiliPub™ rate plan explorer widget on the customer's website, the widget may collect information entered by end users into cost calculators (for example, monthly consumption values, zip code, service class) and technical information necessary to deliver the widget (such as browser type and IP address, for performance and security purposes). Widget end users are not required to create an account and we do not knowingly collect account credentials or direct identifiers (such as names or addresses) from widget end users unless the customer configures the widget to request such information and has obtained any consents required by Applicable Law.

Information we do not collect

We do not build cross-site advertising profiles. We do not use advertising pixels, third-party ad networks, or advertising identifiers on our websites or in the UtiliPub™ widgets. We do not sell personal information to third parties, and we do not use widget end-user data for marketing purposes. We do not knowingly collect personal information from children under the age of 13 (or under 16 in the European Economic Area and United Kingdom).

How We Use Information

We use the information described above to:

- Provide, maintain, secure, and improve our websites, the UtiliPub™ platform, and related services;
- Authenticate users, provision and manage accounts, and prevent unauthorized access;
- Respond to inquiries, support requests, and business correspondence;
- Provide service communications (service notices, security alerts, updates to Documentation or terms);
- Conduct analytics necessary to understand service performance and to improve the platform;
- Meet legal, regulatory, and contractual obligations, including responding to lawful requests from governmental authorities;
- Enforce our agreements, protect our rights and those of our customers, and investigate suspected misuse of the Services.

Where we generate aggregated and anonymized data from information processed on behalf of our customers, we use that data as permitted by our agreement with the applicable customer. Our customer agreements give the customer the ability to opt out of the use of aggregated and anonymized data derived from customer data for the future training of machine-learning models. This opt-out is a feature of our customer relationship and is handled through the customer's Order Form.

Legal Bases for Processing

For individuals in the European Economic Area, the United Kingdom, and Switzerland, we rely on the following legal bases under the EU and UK General Data Protection Regulation (together, "GDPR"):

- Contract — to deliver services to our customers and to provide platform access to authorized users;

- Legitimate interests — to operate, secure, and improve our business; to understand website and platform usage; and to communicate with business contacts, in each case balanced against the rights and freedoms of the individual;
- Consent — where required by Applicable Law, for example for certain marketing communications or for non-essential cookies;
- Legal obligation — to meet applicable regulatory and legal requirements.

Where we process personal information on behalf of a customer (for example, personal information contained in bill data submitted to the Calibrator Layer), our legal basis flows from our customer's lawful basis, and we act as a processor under our Data Processing Agreement with that customer.

How We Share Information

We share personal information only in the limited circumstances described below.

Service providers (subprocessors)

We engage third-party service providers to support our operations in functional categories including cloud hosting and infrastructure, email delivery, customer-relationship management, security monitoring, product analytics, payment processing, and professional services (including accounting and legal). These service providers process personal information on our behalf under written obligations consistent with this Policy and, where applicable, as subprocessors under our Data Processing Agreement with customers. We maintain a current list of subprocessors that we make available to customers on request; we do not name subprocessors in this Policy because the list changes from time to time.

Customers

Where we act as a processor for one of our customers, we share personal information with the relevant customer as necessary to deliver the service. We do not share information between our customers, and we do not share personal information with one customer for use in marketing to another customer's users.

Legal compliance and protection

We may disclose personal information where required by law or legal process, in response to lawful requests from governmental authorities, to protect our rights or the rights of our customers, to investigate or respond to suspected security incidents, or to protect the health or safety of any person.

Business transfers

If we are involved in a merger, acquisition, financing, corporate reorganization, or sale of all or substantially all of our assets, personal information may be transferred as part of that transaction, subject to contractual protections and applicable notice requirements.

No sale of personal information; no advertising partners

We do not sell personal information within the meaning of the California Consumer Privacy Act (as amended, the "CCPA") or analogous state laws, and we do not share personal information for cross-context behavioral advertising. We do not use advertising partners for any data covered by this Policy.

Cookies and Similar Technologies

On our websites, we use a limited set of cookies and similar technologies: strictly necessary cookies required for core website functionality (for example, load balancing, security, and session continuity); and analytics cookies used to understand aggregated website usage patterns. We do not use advertising cookies, retargeting pixels, or cross-site tracking technologies on our websites. Where required by Applicable Law, we provide a cookie notice and obtain consent for non-essential cookies.

Individuals may control cookies through browser settings; disabling strictly necessary cookies may impair website functionality.

When our customer embeds a UtiliPub™ widget on the customer's own website, cookie practices on that website are controlled by the customer, not by us.

Aggregated and Anonymized Data

We may generate aggregated and anonymized data from information processed on our platform. Aggregated and anonymized data is data that has been aggregated with data from other sources and stripped of information that could reasonably be used to identify an individual or our customer. Aggregated and anonymized data is not treated as personal information under this Policy. Our customer agreements grant each customer the ability to opt out of the use of aggregated and anonymized data derived from that customer's data for the future training of machine-learning models; the opt-out applies only to future training and does not require us to unwind or retrain any model for which such data was used prior to the opt-out.

Data Retention

We retain personal information only as long as reasonably necessary for the purposes described in this Policy, including the following retention principles:

- Website-visitor analytics and server logs: retained for no more than 24 months, subject to security-investigation needs;
- Business contact information: retained for the duration of the business relationship and for a reasonable period thereafter for legitimate follow-up and legal-compliance purposes;
- Account credentials and user-profile information for customer personnel: retained for the duration of the customer's subscription and for a limited post-termination period, as set out in our customer agreements;
- Customer data processed on behalf of a customer, including any personal information contained therein: retained per our Data Processing Agreement with the customer and, for Calibrator Layer bill data processed in Cloud Mode, deleted from production systems as part of the ordinary post-processing workflow;
- Information required for legal, regulatory, or tax purposes: retained for the period required by Applicable Law.

Your Privacy Rights

Depending on where you live and the nature of our relationship with you, you may have the following rights with respect to your personal information. We honor these rights to the extent required by Applicable Law, and we offer the core rights on a unified basis to all individuals covered by this Policy regardless of jurisdiction.

- Access — request confirmation of whether we process personal information about you, and a copy of that information;
- Correction — request that we correct inaccurate or incomplete personal information;
- Deletion — request that we delete personal information, subject to exceptions under Applicable Law (for example, information we are required to retain for legal or tax reasons);
- Portability — request a machine-readable copy of personal information you have provided to us, where required by Applicable Law;
- Objection and restriction — object to or request restriction of certain processing, including processing based on our legitimate interests;
- Withdraw consent — where we process personal information based on your consent, withdraw that consent at any time (without affecting the lawfulness of processing before the withdrawal);

- Opt out of sale or sharing — under CCPA and analogous state laws, opt out of the sale or sharing of personal information. We do not sell or share personal information for cross-context behavioral advertising, so there is nothing to opt out of in this respect, but we honor requests in case our practices change;
- Non-discrimination — we will not discriminate against you for exercising any of these rights.

How to exercise your rights

Submit a request to privacy@fluxtailor.com. We will verify your identity using information reasonably necessary to confirm that the request is being made by or on behalf of the individual to whom the personal information relates, and we will respond within the timeframes required by Applicable Law (generally within 30 days for GDPR requests and 45 days for CCPA requests, with permitted extensions where circumstances require).

Requests directed to a customer

Where we process personal information on behalf of a customer (for example, as a processor under our Data Processing Agreement), the customer is responsible for responding to data subject requests in the first instance. We will cooperate with the customer and provide assistance required by our contractual and legal obligations. If you contact us directly with a request that relates to information we process on a customer's behalf, we will forward the request to the customer and notify you accordingly.

Complaints and supervisory authorities

You have the right to lodge a complaint with a supervisory authority. In the European Economic Area and the United Kingdom, you may contact the data protection authority in your country of residence. In California, you may contact the California Privacy Protection Agency or the Office of the Attorney General. In New York, you may contact the Office of the New York State Attorney General. We encourage you to contact us first so that we have the opportunity to address your concern.

Customer Bill Data (Calibrator Service)

If you license the Calibrator Service, the Service processes utility bill data and related billing-period information that you supply ("Customer Bill Data") for the purpose of validating rate plans against actual consumption. **Customer Bill Data is processed session-only and is not retained by Flux Tailor.** Specifically: (a) Customer Bill Data is held only in transient memory for the duration of the user's active session; (b) at session end, all Customer Bill Data is purged from the Service's production infrastructure; (c) Customer Bill Data is not used to train any machine-learning model, generate analytics, or develop derivative data sets; and (d) Customer Bill Data is not shared with any third party other than (i) the Utility Bill Processor at the moment of retrieval (see the section titled "Utility Bill Processor" below) and (ii) cloud infrastructure sub-processors strictly necessary to host the transient session in which calibration processing occurs, each of whom processes such data solely on Provider's instructions and subject to the same session-only constraints described in this section.

If you require persistence of Calibrator outputs (e.g., calibration reports), those outputs are stored separately as Customer Data subject to the standard retention terms described elsewhere in this Policy. In the event of a security incident that affects Customer Bill Data during an active session, we will notify affected customers within forty-eight (48) hours of becoming aware of the incident, regardless of whether the session has ended by the time we discover it. Our standard seventy-two (72) hour notification period under our Data Processing Agreement applies to all other categories of personal data.

URPX Validator Network

If you participate in the URPX Validator Network as a validator (which requires an active Calibrator Service seat), Flux Tailor maintains a credit-redemption record that captures: (a) the identifier of the rate plan validated; (b) the validator identifier; (c) the validation outcome; (d) the credit value earned; and (e) any subsequent redemption of credits for Studio Transcription Tokens or, where eligible, cash conversion. These records form a functional ledger of validator activity and are retained for the longer of (i) the duration of your Subscription Term plus seven (7) years; or (ii) the period required by tax or other Applicable Law (whichever is longer). Validator activity records are not used in Flux Tailor's product analytics and are not shared with other validators or Customers, except to the minimum extent necessary to resolve disputes or comply with tax reporting obligations. Because validator activity records that relate to reportable cash conversion payments may be required for tax reporting obligations under applicable law, we are unable to delete such records in response to an individual erasure request for the period required by applicable tax law. Erasure requests relating to validator activity records that do not involve reportable payments will be honored within thirty (30) days of the request. To submit an erasure request, contact [_____].

Additional terms governing validator participation are set out in the URPX Validator Network Participation Terms. Those terms control over this Privacy Policy with respect to operational and procedural matters of validator participation; provided, however, that the URPX Validator Network Participation Terms will not reduce the substantive privacy protections afforded to individuals under this Policy, which serve as a minimum floor. In the event of any conflict that would reduce those substantive protections, this Policy controls.

Utility Bill Processor (Calibrator Connector)

The Calibrator Service includes Connector access to a third-party utility bill processor (the "Utility Bill Processor") for retrieving Customer Bill Data on your behalf. The Utility Bill Processor identity is disclosed in your Order Form at execution. The Utility Bill Processor processes data under its own privacy practices and contractual terms, separately disclosed at the time of vendor selection.

For the moment of retrieval, the Utility Bill Processor acts as a sub-processor of Flux Tailor under our Data Processing Agreement. Once Customer Bill Data is delivered into your active Calibrator session, the Customer Bill Data session-only carve-out described above governs Flux Tailor's treatment of the data. Flux Tailor does not retain Customer Bill Data beyond the active session, regardless of the Utility Bill Processor's retention practices.

If you maintain a direct account relationship with the Utility Bill Processor (e.g., an authorized-third-party authorization for your utility account), that relationship is governed by your separate agreement with the Utility Bill Processor.

Community Tier Eligibility Data

If you apply for or maintain Community Tier pricing under your MSA (see Exhibit B, Section 3 of the MSA), Flux Tailor collects and retains the following: (a) documentation supporting eligibility (IRS determination letter or equivalent, institutional affiliation web link, mission statement, etc.); (b) the basis of eligibility you elect; (c) annual re-verification confirmations; and (d) any correspondence about eligibility appeals.

Eligibility documentation is retained for the duration of your Subscription Term plus one (1) year and is not used for purposes other than verifying and re-verifying eligibility. For categories (1) U.S. 501(c)(3) status, (2) non-U.S. equivalent status, and (3) accredited educational/research affiliation, Flux Tailor may consult a third-party verification service. The third-party verification service's processing of your documentation is governed by this Policy and by our Data Processing Agreement.

Machine-Readable Privacy Terms (IEEE 7012-2025)

Flux Tailor supports the principles of IEEE 7012-2025, IEEE Standard for Machine Readable Personal Privacy Terms, which describes a framework in which individuals (acting as first parties) may proffer their privacy requirements as contractual terms drawn from a roster of standard-form agreements

maintained by an independent neutral entity. As of the Last Updated date of this Policy, the IEEE 7012 ecosystem — including the standardized roster of agreements and the neutral roster authority — is still in early adoption, and no operational roster authority has yet been designated.

When a roster authority and standard-form agreements become operational, Flux Tailor will:

- publish a machine-readable manifest (for example, at [/.well-known/privacy-terms](#)) identifying the standard-form agreements we accept;
- accept and record IEEE 7012-conformant agreements proffered by website visitors and widget end users that match those we accept; and
- maintain matching electronic records of any agreement reached, available to the individual and to us for retrieval, audit, or dispute resolution under the rights described in “Your Privacy Rights” above.

This commitment does not modify the rights and obligations described elsewhere in this Policy or in our Master Subscription Agreement with customers. Where an IEEE 7012-conformant agreement that we have accepted provides the individual greater protection than this Policy or our default contractual terms, the IEEE 7012-conformant agreement controls with respect to that individual.

Children

Our services are not directed to children, and we do not knowingly collect personal information from children under 13 (or under 16 in the European Economic Area and the United Kingdom). If we become aware that we have collected personal information from a child without verified parental or guardian consent, we will delete that information.

International Data Transfers

We are based in the United States. If you access our services from outside the United States, your personal information may be transferred to, stored in, and processed in the United States or in other jurisdictions in which we or our service providers operate. These jurisdictions may have data protection laws different from those of your country of residence.

For transfers of personal information from the European Economic Area, the United Kingdom, or Switzerland to the United States or to third countries that have not received an adequacy decision, we rely on appropriate safeguards, including the European Commission’s Standard Contractual Clauses (2021/914) and, where applicable, the UK International Data Transfer Addendum and the Swiss Addendum. Further information about these safeguards is available on request.

As we expand to serve customers in the Netherlands, Belgium, and other European Economic Area jurisdictions, we will extend these safeguards to those customers and will designate representatives and take other steps required under Applicable Law as our footprint in these markets develops.

Information Security

We maintain an information security program consistent with the commitments in our Master Subscription Agreement with our customers (MSA §16). Our program includes encryption of personal information in transit (TLS 1.2 or higher) and at rest, access controls and authentication, vulnerability management, secure software development practices, security training for personnel, and a documented incident response plan. No security program can guarantee that information will never be accessed without authorization; we work continuously to reduce that risk.

Additional information about our security practices is available on our website or on request. Customer-specific security commitments are set out in the Security Practices Exhibit to the Master Subscription Agreement.

Changes to this Policy

We may update this Policy from time to time. When we do, we will update the “Last Updated” date above and, where changes are material, provide reasonable additional notice (for example, a prominent

notice on our website or, for active customer contacts, email notification). Your continued use of our services after a change becomes effective constitutes acceptance of the updated Policy.

Contact Us

Questions, concerns, or privacy rights requests can be directed to:

Flux Tailor LLC

Attn: Privacy Contact

Email: utilipub-privacy@utilipub.com

Postal: Flux Tailor LLC, Brooklyn, New York (full postal address available on request).

Privacy contact and Data Protection Officer

Until Flux Tailor formally designates a Data Protection Officer, Klaar De Schepper, our Chief Executive Officer, serves as our initial privacy contact and discharges Data Protection Officer functions to the extent applicable. Klaar may be reached at utilipub-privacy@utilipub.com. If and when a formal Data Protection Officer is designated, we will update this Policy to reflect the designation and contact details.

EU, UK, and Swiss representatives

We do not currently offer services to individuals in the European Economic Area, the United Kingdom, or Switzerland in a manner that requires designation of a local representative under GDPR Article 27 or equivalent laws. We will designate representatives and update this Policy if and when we serve customers in those jurisdictions in a manner that triggers the designation requirement.

— END OF PRIVACY POLICY —