BUGSENG product-security privacy notice

ECLAIR security reporting and response

Document status	Reviewed and Approved – RSGQ, DPO
Version	Rev. 1
Effective date	September 3rd, 2026

Scope

This notice explains how BUGSENG processes personal data when it receives or investigates an ECLAIR security or vulnerability report, maintains a product-security case, coordinates remediation or disclosure, fulfils cybersecurity reporting duties, or sends security information to affected users.

The relevant transparency duties arise under European Union (EU) law: Regulation (EU) 2016/679, the General Data Protection Regulation (GDPR) and Regulation (EU) 2024/2847, the Cyber Resilience Act (CRA).

Controller and contacts

Controller	BUGSENG srl, an Italian limited liability company
Address	Via Fiorentina 214/C, 56121 Pisa, Italy
Tax identifiers	Italian tax code and value added tax registration number IT02592690347
Privacy contact	privacy@bugseng.com

Product-security reports and replies concerning a security case: security@bugseng.com

Data Protection Officer (DPO): Valentina Loggini, valentina.loggini@bugseng.com

Personal data and sources

Depending on the report or case, BUGSENG may process:

- a reporter's name, contact details, organisation and role, if supplied;
- report correspondence, attachments, acknowledgement preferences and any requested public credit;
- ECLAIR and component versions, timestamps, network or system identifiers, logs, diagnostic details and other technical evidence;
- business contact details, product applicability, distributor routes and delivery status used to inform affected users;
- case decisions, approvals and communications with affected users, distributors, suppliers, advisers and authorities; and
- limited personal data about other people if they appear in submitted evidence.

Data may come directly from the reporter or affected person. It may also come from BUGSENG's customer, licence, delivery, maintenance or support records; from a user's organisation, distributor, supplier or component maintainer; from public vulnerability sources; or from a competent authority.

BUGSENG does not ask reporters to submit passwords, private keys, personal datasets, special-category personal data or unrelated third-party information. If such data are received, BUGSENG restricts access and deletes or redacts them when they are not necessary. BUGSENG processes special-category personal data only if a specific GDPR Article 9 condition applies.

Purposes and legal bases

BUGSENG processes the minimum personal data necessary:

- to receive, validate, investigate, remediate and coordinate vulnerability reports, and to protect ECLAIR, its users and third parties. The legal basis is BUGSENG's legitimate interest in product security and Coordinated Vulnerability Disclosure (CVD), under GDPR Article 6(1)(f);
- to make mandatory notifications, cooperate with competent authorities and inform affected users where required by the CRA or another applicable law. The legal basis is compliance with a legal obligation under GDPR Article 6(1)(c);
- to contact users or their organisations about a security risk and maintain evidence that an actionable notice was delivered. The legal bases are GDPR Article 6(1)(c), where legally required, and BUGSENG's legitimate interest in protecting users and products under Article 6(1)(f); and
- to establish, exercise or defend legal claims, prevent misuse and respond to binding requests. The legal basis is GDPR Article 6(1)(f), or Article 6(1)(c) where disclosure is legally required.

BUGSENG's legitimate interests are to receive security information, determine whether ECLAIR users are at risk, coordinate safe correction and disclosure, protect its systems and users, and retain proportionate evidence of its response. BUGSENG balances those interests against the rights and interests of the individuals concerned, limits access and removes identifiers when they are no longer necessary.

A reporter's name or identifying credit is made public only with the person's separate, explicit consent under GDPR Article 6(1)(a). Consent may be withdrawn at any time for future use without affecting earlier lawful processing.

Whether personal data must be provided

A reporter's name or personal contact details are not a statutory or contractual requirement. Anonymous reports are accepted. A usable contact route is needed for security coordination; without one, BUGSENG may be unable to ask questions, acknowledge the report or provide case-specific feedback.

Business contact data already held for an affected user or organisation may be used where necessary to deliver security information.

Recipients

Access within BUGSENG is limited to people who need the information for product-security response, technical remediation, controlled records, legal or privacy review, authority reporting or affected-user communication.

Where necessary and limited to the relevant purpose, information may be disclosed to:

- providers acting for BUGSENG in the categories of email, secure file transfer, information-technology support, website hosting, controlled record storage and backup;
- affected users or their organisations and documented distributors;
- suppliers and component maintainers involved in analysis or remediation;
- legal, security and privacy advisers; and
- the coordinating Computer Security Incident Response Team (CSIRT), the European Union Agency for Cybersecurity (ENISA), other competent CSIRTs, market-surveillance authorities, data-protection authorities, courts or other authorities where applicable.

Reporter identity is removed before a disclosure when it is not necessary. It is not disclosed to affected users or published without the reporter's permission unless disclosure is required by law.

International transfers

The systems and providers used for this processing store and process personal data only in the European Economic Area (EEA).

Retention

BUGSENG applies the following retention schedule:

- Obvious spam and submissions unrelated to product security are deleted within 30 days.
- Personal contact data and correspondence for a report that does not result in a confirmed security case are deleted or anonymised within 12 months after closure.
- Personal contact data and correspondence for a confirmed security case are deleted or anonymised within 24 months after closure.
- Technical and compliance evidence is reviewed at closure and at least annually thereafter. Personal identifiers are removed when no longer necessary. Any remaining personal data follow the 12- or 24-month rule above.

Data may be retained longer when necessary for continuing coordination, a binding legal obligation, an authority request, a documented legal hold, or the establishment, exercise or defence of legal claims. Delivery evidence is reduced where possible to the organisation, route, time and delivery result.

Security

BUGSENG applies access control, data minimisation, backup and appropriate technical and organisational measures. Do not send passwords, private keys, personal datasets or exploit material by ordinary email. Ask security@bugseng.com for the approved protected-transfer method before sending sensitive evidence.

Information obtained indirectly

When BUGSENG obtains personal data from another source, it provides this notice within the period required by GDPR Article 14: generally no later than one month, or earlier at the first communication with the person or first disclosure to another recipient. A lawful exception in GDPR Article 14(5) may apply. The data categories and sources are described above.

Individual rights

Subject to the conditions and exceptions in data-protection law, individuals may request access to and correction or deletion of their personal data, restriction of processing and data portability. They may object at any time to processing based on legitimate interests, including by explaining their particular situation. They may withdraw consent for future public credit at any time. Requests may be sent to privacy@bugseng.com

Individuals may lodge a complaint with the *Garante per la Protezione dei Dati Personali*, the Italian data-protection authority. The complaint procedure is available at www.garanteprivacy.it — complaint procedure. Individuals may also complain to another competent supervisory authority.

Automated decision-making

BUGSENG does not use personal data covered by this notice for marketing, profiling or decisions based solely on automated processing that produce legal or similarly significant effects.

Personal-data breaches

If a product-security incident is also a personal-data breach, BUGSENG applies the separate documentation, supervisory-authority notification and affected-individual communication rules in GDPR Articles 33 and 34.

Changes to this notice

BUGSENG may update this notice when its processing or legal obligations change. The current version and effective date are shown at the top. The latest version is publicly available on https://bugseng.com/.