Privacy notice on the processing of personal data

Vulnerability and security reports - Articles 13 and, where applicable, 14 of Regulation (EU) 2016/679

1. Data Controller

The data controller is Nice s.p.a, with registered office at Via Callalta n. 1 Oderzo (TV) Italia, tax/VAT number 03099360269 / 02717060277, pec accounting@pec.niceforyou.com (the "Controller"). The Controller is part of the Nice Group. Depending on the product or component concerned, other Group companies or third-party legal entities may participate in the processing as described in this Privacy Notice.

2. Data Protection Officer and contacts

The Data Protection Officer ("DPO"), where appointed, may be contacted at niceprivacy@niceforyou.com or at postal address Nice spa in Via Callalta n. 1 Oderzo (TV). Vulnerability reports may be sent to security@niceforyou.com. The mailbox is managed by authorized personnel and reports are forwarded only to persons and organizations that need to participate in their assessment and handling.

3. Data subjects

- individuals submitting vulnerability, incident or other security reports;
- contact persons, employees or contractors of the organization on whose behalf a report is submitted;
- users, customers or third parties whose data appear in the report, attachments, logs or information provided;
- persons involved in the technical, organizational or legal management of the event.

Where a report contains data relating to other persons, the reporter should disclose only strictly necessary information and, where possible, remove or anonymize irrelevant data.

4. Categories of personal data

- identification and contact details of the reporter and their organisation;
- information concerning the product, device, software, firmware, version or component;
- the report and subsequent communications;
- technical data such as IP addresses, device identifiers, logs, timestamps, configurations, test results, diagnostics, screenshots, videos, files and evidence;
- information held in ticketing and vulnerability or incident-management systems;
- information concerning impact and possible exploitation;
- information included in communications to ENISA, CSIRTs and authorities;
- verification, mitigation, remediation, update-deployment and closure information;
- information necessary to document decisions, compliance and legal protection.

The Controller does not request special categories of personal data under Article 9 GDPR or data relating to criminal convictions and offences. Such data should not be included unless

strictly indispensable. If received, they will be processed only where necessary and where a condition under Articles 9 or 10 GDPR and applicable national law is met, including, where relevant, the establishment, exercise or defence of legal claims.

5. Purposes and legal bases

5.1 Receipt, assessment and handling of reports

Data are processed to receive, register and verify reports; identify the relevant product, component and owner; classify the event; communicate with the reporter; coordinate assessment, mitigation, remediation and responsible disclosure; and prevent misuse of the channel. The legal basis is the legitimate interest pursued by the Controller and third parties in protecting products, networks, systems and users under Article 6(1)(f) GDPR. Article 6(1)(b) GDPR may also apply where processing is necessary for a contract or requested pre-contractual measures.

5.2 Compliance with cybersecurity obligations

Data may be processed to assess an actively exploited vulnerability or severe incident; submit early warnings, notifications, updates and final reports; comply with Regulation (EU) 2024/2847 (Cyber Resilience Act, “CRA”) and other national or Union law; and respond to ENISA, CSIRTs, market surveillance, data protection or other competent authorities. The legal basis is compliance with a legal obligation under Article 6(1)(c) GDPR.

5.3 Security and prevention of further events

Data may be used to identify similar vulnerabilities, correlate events and technical indicators, prevent attacks or unauthorized access, verify corrective measures, improve product security and retain a technical record. The legal basis is legitimate interest under Article 6(1)(f) GDPR.

5.4 Establishment, exercise and defence of legal claims

Data may be processed and retained to document activities and decisions; manage complaints, inspections and proceedings; establish responsibilities; and exercise or defend the rights of the Controller, other entities or third parties. The legal bases are Article 6(1)(f) GDPR and, where applicable, Article 6(1)(c) GDPR. Processing is not based on consent unless expressly stated for a specific additional activity.

6. Nature of provision

Providing identification details is generally voluntary unless identification is required by law, the platform or the circumstances. Anonymous reporting is possible to the extent allowed by the channel; lack of contact details may prevent clarifications, verification, acknowledgements and updates. Essential technical information must be sufficiently complete, otherwise the report may not be verifiable.

7. Processing and security

Data are processed electronically and, where necessary, in documentary form by authorized personnel, in accordance with lawfulness, fairness, transparency, minimization, accuracy, integrity and confidentiality. Risk-appropriate safeguards include access controls, segregation of duties, logging, protected communications, secure attachment handling, protected evidence storage and need-to-know access.

8. Disclosure and sharing

8.1 Group companies and other legal entities

Data may be shared with Nice Group companies or other separate legal entities acting as manufacturers, importers, distributors or authorized representatives; responsible for the product, business unit or component; performing R&D, product management, cybersecurity, support, quality, compliance, privacy or legal functions; participating in assessment, remediation, notification or management; or exposed to the vulnerability. Depending on their role, they act as independent controllers, joint controllers or processors under the agreements required by the GDPR.

8.2 Providers and advisers

Recipients may include IT, cloud, email, ticketing and cybersecurity providers; laboratories and technical specialists; legal advisers, insurers, auditors and other professionals; manufacturers, developers, maintainers and component suppliers. They act as processors or independent controllers according to their role.

8.3 ENISA, CSIRTs and public authorities

Where required by law or necessary, data may be disclosed to ENISA, including through the CRA Single Reporting Platform; the CSIRT designated as coordinator and other CSIRTs; national market-surveillance and cybersecurity authorities; data protection authorities; judicial, law-enforcement and other public bodies; Union institutions and bodies; and public authorities in the reporter's country, the country where the product is marketed or used, and other Member States concerned. Information may be further shared among authorities under the CRA, Union law or national law. Personal data disclosed are limited to what is necessary.

9. International transfers

Sharing among entities established in the European Economic Area is not a third-country transfer under Chapter V GDPR. Transfers outside the EEA will rely, as appropriate, on an adequacy decision, Standard Contractual Clauses with supplementary measures, Binding Corporate Rules, another recognised safeguard or, only exceptionally, an Article 49 derogation. Information on safeguards may be requested from the Controller or DPO.

10. Retention periods

Data are not retained only for the time required to provide an initial response. A vulnerability or incident may require technical, regulatory, evidentiary and legal-defence activities after the initial communication is closed.

Category	Ordinary period
Clearly unfounded reports, spam, duplicates with no additional content or irrelevant communications	Up to 12 months from classification or closure, unless needed to prevent repeated misuse.
Technical reports assessed but not confirmed	Up to 5 years from closure were needed to correlate later reports, document assessments and prevent recurrence.
Confirmed reports, tickets, correspondence, assessments, decisions, corrective measures and closure evidence	10 years from final closure or the last substantive activity, if later.
Cases communicated to ENISA, CSIRTs or other authorities	10 years from final closure of the proceeding or the last communication with the authority, if later.
Data connected with disputes, inspections, investigations or proceedings	For the proceeding and until expiry of the applicable periods for exercising or defending rights.
Mailbox, platform or ticketing logs	Normally 24 months, unless linked to an event or needed for an investigation.
Backup data	For the ordinary backup cycle, indicatively no longer than 6 months, followed by overwriting.

For products still supported or capable of producing effects, technical and accountability information may be retained until the end of the support period and thereafter as necessary for legal obligations and protection of rights. Periods may be extended where required by law or an authority, during investigations or disputes, for legal claims or until final resolution. At expiry, data are erased, anonymized or aggregated. Technical information no longer relating to individuals may be retained for statistics, research and security. The Controller periodically reviews necessity and proportionality.

11. Data subjects' rights

Subject to the GDPR, data subjects may request access, rectification, erasure, restriction and portability, object to legitimate-interest processing and withdraw any consent. Requests may be sent to niceprivacy@niceforyou.com. Rights may be restricted or deferred where retention is necessary for legal obligations, security, third-party rights or legal claims. The Controller may verify the requester's identity.

12. Right to object

For processing under Article 6(1)(f) GDPR, the data subject may object on grounds relating to their particular situation. The Controller will cease processing unless compelling overriding grounds exist or processing is necessary for legal claims.

13. Complaint

A complaint may be lodged with the supervisory authority in the Member State of habitual residence, place of work or alleged infringement. For a Controller established in Italy: Garante per la protezione dei dati personali, Piazza Venezia 11, 00187 Rome, Italy, www.garanteprivacy.it. Judicial remedies remain available.

14. Automated decisions

No decisions are made solely by automated processing that produce legal or similarly significant effects. Automated tools may support classification, correlation or prioritisation, while material decisions remain subject to authorised human review.

15. Data obtained from other sources

Data may be obtained from Group companies; customers, distributors, installers and partners; manufacturers and suppliers; security researchers; public sources; vulnerability-disclosure platforms; ENISA, CSIRTs and authorities; and affected systems, products and infrastructure. Where Article 14 GDPR applies, this notice will be provided within the applicable time limits unless an exemption applies.

16. Updates

This Privacy Notice may be updated for legal, organisational or technical developments. The current version will be published at https://www.niceforyou.com/en/cra-policy with the date of the latest update.