# INFORMATIVA SUL TRATTAMENTO DEI DATI PERSONALI

*Segnalazioni di vulnerabilità e sicurezza - artt. 13 e, ove applicabile, 14 del Regolamento (UE) 2016/679*

## 1. Titolare del trattamento

Il Titolare del trattamento è Nice s.p.a, con sede legale in Via Callalta n. 1 Oderzo (TV) Italia, CF/P.IVA 03099360269 / 02717060277, PEC accounting@pec.niceforyou.com (il "Titolare"). Il Titolare appartiene al gruppo Nice. In relazione allo specifico prodotto o componente interessato, al trattamento possono partecipare anche altre società del gruppo o soggetti giuridici terzi, secondo quanto indicato nella presente informativa.

## 2. Responsabile della protezione dei dati e contatti

Il Responsabile della protezione dei dati ("DPO"), può essere contattato all'indirizzo niceprivacy@niceforyou.com o all'indirizzo postale Nice spa in Via Callalta n. 1 Oderzo (TV). Le segnalazioni di vulnerabilità possono essere inviate a security@niceforyou.com. La mailbox è gestita da personale autorizzato e le segnalazioni sono inoltrate soltanto ai soggetti che devono partecipare alla loro valutazione e gestione.

## 3. Soggetti interessati

- la persona che effettua una segnalazione di vulnerabilità, incidente o altro problema di sicurezza;
- i referenti, dipendenti o collaboratori dell'organizzazione per conto della quale viene effettuata la segnalazione;
- gli utenti, clienti o terzi i cui dati siano contenuti nella segnalazione, negli allegati, nei log o nelle informazioni trasmesse;
- le persone coinvolte nella gestione tecnica, organizzativa o legale dell'evento.

Se la segnalazione contiene dati riferiti a terzi, il segnalante è invitato a comunicare soltanto le informazioni strettamente necessarie e, quando possibile, a rimuovere o anonimizzare i dati non pertinenti.

## 4. Categorie di dati trattati

- dati identificativi e di contatto del segnalante e dell'organizzazione di appartenenza;
- dati relativi al prodotto, dispositivo, software, firmware, versione o componente interessato;
- contenuto della segnalazione e delle successive comunicazioni;

- informazioni tecniche, quali indirizzi IP, identificativi di dispositivi, log, timestamp, configurazioni, risultati di test, diagnostica, screenshot, video, file ed evidenze tecniche;
- informazioni contenute nei ticket e nei sistemi di vulnerability o incident management;
- dati relativi all'impatto e all'eventuale sfruttamento della vulnerabilità;
- informazioni incluse nelle comunicazioni a ENISA, CSIRT e autorità;
- dati relativi a verifica, mitigazione, correzione, rilascio degli aggiornamenti e chiusura;
- informazioni necessarie a documentare le decisioni, gli adempimenti e la tutela dei diritti.

Il Titolare non richiede categorie particolari di dati ai sensi dell'art. 9 GDPR né dati relativi a condanne penali o reati. Tali dati non devono essere inseriti, salvo siano strettamente indispensabili. Se comunque ricevuti, saranno trattati nei soli limiti necessari e in presenza di una condizione prevista dagli artt. 9 o 10 GDPR e dalla normativa nazionale, inclusa, ove pertinente, la necessità di accertare, esercitare o difendere un diritto.

# 5. Finalità e basi giuridiche

## 5.1 Ricezione, analisi e gestione della segnalazione

I dati sono trattati per ricevere, registrare e verificare la segnalazione; identificare prodotto, componente e owner competente; classificare l'evento; comunicare con il segnalante; coordinare analisi, mitigazione, correzione e divulgazione responsabile; prevenire abusi del canale. La base giuridica è il legittimo interesse del Titolare e di terzi alla sicurezza di prodotti, reti, sistemi e utenti, ai sensi dell'art. 6, par. 1, lett. f), GDPR. Se necessario all'esecuzione di un contratto o di misure precontrattuali richieste dall'interessato, può applicarsi anche l'art. 6, par. 1, lett. b), GDPR.

## 5.2 Adempimenti in materia di cybersicurezza

I dati possono essere trattati per valutare l'esistenza di una vulnerabilità attivamente sfruttata o di un incidente grave; trasmettere early warning, notifiche, aggiornamenti e relazioni finali; adempiere al Regolamento (UE) 2024/2847 (Cyber Resilience Act, "CRA") e ad altre norme nazionali o dell'Unione; rispondere a ENISA, CSIRT, autorità di vigilanza, autorità privacy o altre autorità competenti. La base giuridica è l'adempimento di un obbligo legale, ai sensi dell'art. 6, par. 1, lett. c), GDPR.

## 5.3 Sicurezza e prevenzione di ulteriori eventi

I dati possono essere utilizzati per individuare vulnerabilità analoghe, correlare eventi e indicatori tecnici, prevenire attacchi o accessi non autorizzati, verificare le misure correttive, migliorare la sicurezza dei prodotti e conservare una memoria tecnica dell'evento. La base giuridica è il legittimo interesse ai sensi dell'art. 6, par. 1, lett. f), GDPR.

### 5.4 Accertamento, esercizio e difesa dei diritti

I dati possono essere trattati e conservati per documentare attività e decisioni; gestire contestazioni, reclami, ispezioni e procedimenti; accertare responsabilità; esercitare o difendere i diritti del Titolare, delle altre società coinvolte o di terzi. Le basi giuridiche sono l'art. 6, par. 1, lett. f), GDPR e, quando applicabile, l'art. 6, par. 1, lett. c), GDPR. Il trattamento non è basato sul consenso, salvo espressa indicazione per specifiche attività ulteriori.

## 6. Natura del conferimento

Il conferimento dei dati identificativi è di regola facoltativo, salvo che la legge, la piattaforma o le circostanze richiedano l'identificazione. È possibile segnalare senza fornire dati personali nei limiti consentiti dal canale; l'assenza di un recapito può impedire richieste di chiarimento, verifiche, riscontri e aggiornamenti. Le informazioni tecniche indispensabili devono essere sufficientemente complete; in mancanza, la segnalazione potrebbe non essere verificabile.

## 7. Modalità e sicurezza

I dati sono trattati con strumenti informatici e, ove necessario, in forma documentale da personale autorizzato, nel rispetto dei principi di liceità, correttezza, trasparenza, minimizzazione, esattezza, integrità e riservatezza. Sono adottate misure adeguate al rischio, tra cui controllo degli accessi, segregazione dei ruoli, tracciamento, protezione delle comunicazioni, gestione sicura degli allegati, conservazione protetta delle evidenze e accesso secondo necessità.

## 8. Comunicazione e condivisione dei dati

### 8.1 Società del gruppo e altri soggetti giuridici

I dati possono essere condivisi con società del gruppo Nice o altri soggetti giuridici distinti che agiscano quali produttori, importatori, distributori o mandatari; siano responsabili del prodotto, della business unit o del componente; svolgano attività R&D, product management, cybersecurity, assistenza, qualità, compliance, privacy o legali; debbano partecipare alla valutazione, correzione, comunicazione o gestione; oppure siano esposti agli effetti della vulnerabilità. In funzione del ruolo, tali soggetti operano quali titolari autonomi, contitolari o responsabili del trattamento, sulla base degli accordi richiesti dal GDPR.

### 8.2 Fornitori e consulenti

I dati possono essere comunicati a fornitori IT, cloud, posta elettronica, ticketing e cybersecurity; laboratori, consulenti tecnici e società specializzate; consulenti legali, assicuratori, revisori e professionisti; produttori, sviluppatori, manutentori e fornitori del componente. Essi operano quali responsabili o titolari autonomi secondo il ruolo svolto.

### 8.3 ENISA, CSIRT e autorità pubbliche

Quando previsto dalla legge o necessario, i dati possono essere comunicati a ENISA, anche tramite la Single Reporting Platform CRA; al CSIRT designato come coordinatore e ad altri CSIRT; alle autorità nazionali di vigilanza del mercato e di cybersicurezza; alle autorità di protezione dei dati; alle autorità giudiziarie, di polizia e ad altre amministrazioni; alle istituzioni e agli organismi dell'Unione europea; alle autorità pubbliche dello Stato del segnalante, dello Stato di commercializzazione o utilizzo del prodotto e di altri Stati membri interessati. Le informazioni possono essere ulteriormente trasmesse tra autorità quando previsto dal CRA, dal diritto dell'Unione o dalla normativa nazionale. I dati personali comunicati sono limitati a quanto necessario.

## 9. Trasferimenti internazionali

La condivisione tra soggetti stabiliti nello Spazio economico europeo non costituisce trasferimento verso un Paese terzo ai sensi del Capo V GDPR. I trasferimenti fuori dal SEE saranno effettuati, secondo il caso, sulla base di una decisione di adeguatezza, delle clausole contrattuali tipo con eventuali misure supplementari, di norme vincolanti d'impresa, di altra garanzia riconosciuta o, soltanto in casi eccezionali, di una deroga dell'art. 49 GDPR. Informazioni sulle garanzie possono essere richieste al Titolare o al DPO.

## 10. Periodi di conservazione

I dati non sono conservati soltanto per il tempo necessario al primo riscontro. Una vulnerabilità o un incidente può richiedere attività tecniche, regolamentari, probatorie e difensive successive alla chiusura della comunicazione iniziale.

| Tipologia | Periodo ordinario |
|---|---|
| Segnalazioni infondate, spam, duplicati privi di contenuto aggiuntivo o comunicazioni non pertinenti | Fino a 12 mesi dalla classificazione o chiusura, salvo necessità di contrastare abusi reiterati. |
| Segnalazioni tecniche analizzate ma non confermate | Fino a 5 anni dalla chiusura, ove necessario per correlare segnalazioni successive, documentare le verifiche e prevenire la reiterazione del rischio. |
| Segnalazioni confermate, ticket, corrispondenza, valutazioni, decisioni, misure correttive ed evidenze di chiusura | 10 anni dalla chiusura definitiva o dall'ultima attività sostanziale, se successiva. |
| Casi comunicati a ENISA, CSIRT o altre autorità | 10 anni dalla chiusura definitiva del procedimento o dall'ultima comunicazione con l'autorità, se successiva. |
| Dati collegati a contestazioni, ispezioni, indagini o procedimenti | Per la durata del procedimento e fino alla scadenza dei termini applicabili per l'esercizio o la difesa dei diritti. |

| Tipologia | Periodo ordinario |
|---|---|
| Log della mailbox, della piattaforma o del ticketing | Di regola 24 mesi, salvo collegamento con un evento o necessità di indagine. |
| Dati nei backup | Per il normale ciclo di backup, indicativamente non oltre 6 mesi, con successiva sovrascrittura. |

Per prodotti ancora supportati o suscettibili di produrre effetti, le informazioni tecniche e di accountability possono essere conservate fino alla fine del support period e successivamente per il periodo necessario agli obblighi normativi e alla tutela dei diritti. I termini possono essere estesi se richiesto dalla legge o da un'autorità, in presenza di indagini o controversie, per la difesa di diritti o finché l'evento non sia definitivamente risolto. Alla scadenza i dati sono cancellati, anonimizzati o aggregati. Le informazioni tecniche non più riferibili a persone fisiche possono essere conservate per finalità statistiche, di ricerca e di sicurezza. Il Titolare verifica periodicamente necessità e proporzionalità della conservazione.

## 11. Diritti degli interessati

Nei casi previsti dal GDPR, l'interessato può chiedere accesso, rettifica, cancellazione, limitazione e portabilità, opporsi ai trattamenti fondati sul legittimo interesse e revocare l'eventuale consenso. Le richieste possono essere inviate a niceprivacy@niceforyou.com. Alcuni diritti possono essere limitati o differiti quando la conservazione sia necessaria per obblighi normativi, sicurezza, diritti di terzi o difesa di un diritto. Il Titolare può verificare l'identità del richiedente.

## 12. Diritto di opposizione

Per i trattamenti fondati sull'art. 6, par. 1, lett. f), GDPR, l'interessato può opporsi per motivi connessi alla propria situazione particolare. Il Titolare cesserà il trattamento salvo motivi legittimi cogenti prevalenti o necessità di accertare, esercitare o difendere un diritto.

## 13. Reclamo

L'interessato può proporre reclamo all'autorità di controllo dello Stato membro di residenza abituale, lavoro o presunta violazione. Per un Titolare stabilito in Italia: Garante per la protezione dei dati personali, Piazza Venezia 11, 00187 Roma, www.garanteprivacy.it. Resta fermo il diritto di ricorrere all'autorità giudiziaria.

## 14. Decisioni automatizzate

Non sono adottate decisioni basate unicamente su trattamenti automatizzati che producano effetti giuridici o analogamente significativi. Strumenti automatici possono supportare classificazione, correlazione o priorità, fermo l'intervento di personale autorizzato nelle decisioni rilevanti.

## 15. Dati ottenuti da altre fonti

Il Titolare può ottenere dati da società del gruppo; clienti, distributori, installatori e partner; produttori e fornitori; ricercatori di sicurezza; fonti pubbliche; piattaforme di vulnerability disclosure; ENISA, CSIRT e autorità; sistemi, prodotti e infrastrutture interessati. Quando si applica l'art. 14 GDPR, l'informativa è resa nei termini previsti, salvo un'eccezione applicabile.

## 16. Aggiornamenti

La presente informativa può essere aggiornata per modifiche normative, organizzative o tecniche. La versione aggiornata è pubblicata alla pagina https://www.ableautomation.com/it/CRA-policy/, con la data dell'ultimo aggiornamento.