

NOTA PER UFFICI LEGALI, DPO E UFFICI TECNICI

Dati, privacy e *sicurezza*.

Un microfono installato in un luogo accessibile solleva una domanda legittima prima ancora che venga posta. Questa nota risponde a quella domanda e alle altre che emergono in istruttoria.

La risposta breve

Il sensore **non conserva l'audio**. Registra una finestra di 40 secondi, la analizza a bordo, estrae il nome della specie e cancella il file. Non esiste archivio di registrazioni, né sul dispositivo né nel cloud. Non c'è nulla da cui si possa ricostruire una conversazione.

Cosa viene trattato

Il dato che lascia il sensore è composto da: nome scientifico della specie riconosciuta, istante della rilevazione, grado di confidenza del riconoscimento, identificativo della postazione. A questo si aggiunge lo stato tecnico del dispositivo — temperatura, memoria, spazio su disco, qualità del collegamento.

Nessuno di questi elementi è un dato personale ai sensi dell'art. 4 del GDPR. Non vengono trattate immagini, non viene conservato parlato, non vengono raccolti identificativi di dispositivi di terzi nelle vicinanze.

Dove risiedono i dati

Elaborazione audio	A bordo del sensore. L'audio non viene mai trasmesso
Archiviazione dei riconoscimenti	Infrastruttura cloud con server nell'Unione Europea
Trasferimenti extra-UE	Nessuno per i dati di rilevazione
Titolare	Terra Sense S.r.l., Treviglio (BG)

Accesso ai dati e licenza

Le rilevazioni grezze sono pubblicate in **CC0 1.0**, cioè rilasciate nel pubblico dominio: chiunque può scaricarle, riutilizzarle e verificarle senza chiedere permesso e senza obbligo di citazione. I contenuti editoriali sono in CC BY 4.0.

Questa scelta ha una conseguenza che conviene esplicitare in istruttoria: i dati del vostro sito saranno pubblici. È la condizione che li rende verificabili da un revisore terzo, ed è ciò che distingue una misura da

una dichiarazione. Se un sito richiede riservatezza — per esempio la posizione esatta di una specie sensibile — la posizione può essere pubblicata con granularità ridotta.

Sicurezza del dispositivo

- Il sensore stabilisce solo connessioni in uscita. Non espone servizi raggiungibili da internet.
- Il collegamento avviene su rete cellulare dietro NAT dell'operatore: non ha un indirizzo pubblico raggiungibile dall'esterno.
- Le comunicazioni con il backend avvengono su HTTPS.
- Il dispositivo non è collegato alla rete locale dell'ospitante e non vi accede in alcun modo.

Un punto che semplifica molte istruzioni

Poiché il sensore non si collega alla rete dell'ospitante e non espone servizi, non rientra nel perimetro dei sistemi informativi dell'organizzazione che lo ospita. Non richiede valutazioni di sicurezza sull'infrastruttura interna né aperture sul firewall.

Continuità e trasparenza del servizio

Lo stato di ogni sensore è noto con cadenza semioraria. Se un dispositivo smette di registrare, la condizione è rilevabile da remoto e databile con precisione: il periodo scoperto viene dichiarato, non nascosto. Nei dati pubblici le rilevazioni generate in via simulata — usate solo per mantenere continuità visiva durante un fermo prolungato — sono marcate come tali ed escluse da API, snapshot e dataset citabili.