emanuel
celano
23.11.2026
15:56:28
GMT+01:00

# EVIDE: Service Conditions and Privacy Policy

Copy of the texts published on app.certifywebcontent.com, for qualified electronic signature

| | |
|---|---|
| **Service Conditions** | version 2026-16, https://app.certifywebcontent.com/service-conditions |
| **Privacy Policy** | version 2026-16, https://app.certifywebcontent.com/privacy |
| **Effective from** | 24 November 2026 |
| **Languages** | English (Part A) and Italian (Part B) |
| **Issued by** | Informatica in Azienda, Dott. Emanuel Celano, Via Vaccaro 5, 40132 Bologna, Italy, VAT IT02137271207 |
| **Document prepared** | 23 November 2026 |
| **File name after signature** | EVIDE_Terms_2026-16_Privacy_2026-16_signed.pdf |

## About this document

This document reproduces, without changes, the texts of the EVIDE Service Conditions (16 sections) and Privacy Policy (15 sections) in the versions indicated above, as prepared for publication on the canonical pages, in English and in Italian. The German, French and Spanish versions are published on the same pages and are not reproduced here.

This document is prepared for the subsequent application, on behalf of Informatica in Azienda, of a qualified electronic signature (eIDAS) in PAdES format and of a qualified electronic timestamp. Once signed, the document will not be modified. After signature, the SHA-256 fingerprint of the signed file will be published on the canonical pages, so that anyone can check that a copy is identical to the published one.

The signed copy will not be a contract signed by a user and will not record any acceptance. Acceptance of the Service Conditions takes place as described in Section 16.1; for API plans the accepted version is recorded with its own SHA-256 digest. For the API service acceptance the reference text is the English version.

A later version is published with a new version number and a new signed copy. Once published, the signed copy of these versions will not be replaced, and it will continue to document the texts that applied from their effective date until the effective date of the next version. The signed copies of earlier versions remain available and unchanged.

Dates. The effective date of these versions and the date on which this document was prepared are stated above. The date of the signature and of the qualified timestamp will be the one recorded in the signature itself, and is not yet known when this document is prepared. The signature and the timestamp will document the content of this document at the time of signing; they do not by themselves prove that the texts were published on, or applied from, the effective date.

# Contents

1. Part A, English: Service Conditions (version 2026-16); Privacy Policy & Cookie Policy (version 2026-16)
2. Parte B, Italiano: Condizioni di Servizio (versione 2026-16); Privacy Policy & Cookie Policy (versione 2026-16)
3. Signature / Firma

PART A: ENGLISH

# Service Conditions

Version 2026-16 - effective from 24 November 2026 · https://app.certifywebcontent.com/service-conditions

## 1. Purpose and Scope

These conditions govern the use of the EVIDE platform operated by Informatica in Azienda, directed by Dott. Emanuel Celano. These conditions, together with the Privacy Policy, apply to the use of the platform. The way in which they are accepted is described in Section 16.

The platform may be used both by professional users, acting for purposes relating to their trade, business, craft or profession, and by consumers, meaning natural persons acting for purposes outside those activities. Where these conditions contain specific rules for consumers, those rules apply to consumer users. Nothing in these conditions limits the rights that consumers have under mandatory consumer-protection law, including the Italian Consumer Code (Legislative Decree 206/2005) and, for consumers resident in another country, the mandatory provisions of the law of that country. Services specifically intended for household or personal use, if offered in the future, may be subject to supplementary conditions. Users must be at least 18 years old.

## 2. Service Availability

EVIDE is provided as-is. We strive for maximum availability but do not guarantee uninterrupted service. Temporary interruptions may occur due to maintenance, technical issues, or circumstances beyond our control. Service interruptions do not invalidate evidentiary records already created: intake hashes remain verifiable with standard SHA-256 tools, applied to the original material or, for structured intakes, to its canonical form as documented by EVIDE, and the UTC timestamp remains the reference recorded by EVIDE at deposit time. For consumers, this section does not affect the legal guarantee of conformity of digital content and digital services provided by the Consumer Code.

## 3. Force Majeure and Third-Party Dependencies

EVIDE depends on third-party infrastructure including hosting providers, SSL authorities, email delivery services, and, for the FEDIS service only, qualified trust service providers for signatures and time stamps. The base EVIDE deposit does not use qualified time stamps: its UTC timestamp is generated by the EVIDE server. We cannot be held liable for service degradations caused by maintenance, updates, or failures of these providers. In such cases, service will be restored as quickly as technically possible, except where mandatory law requires otherwise.

## 4. Volume Limits and Infrastructure Compatibility

EVIDE is a shared-infrastructure platform designed for professional use at the volumes indicated in each plan. Users requiring more than 500 intakes/month must contact us before activating such volumes to arrange a dedicated infrastructure solution. Standard service plans are not designed to guarantee enterprise-level SLAs at high-volume or continuous-throughput workloads. Performance degradations caused by volumes exceeding the plan threshold do not constitute breach of contract. We reserve the right to suspend accounts generating disproportionate load without prior agreement, with 24 hours notice and proportional refund of the unused period, except where mandatory law requires otherwise. Content sent to the platform, including the structured content of API deposits, is subject to a maximum size set by Informatica in Azienda and stated in the technical documentation; content over the limit is refused, never truncated.

## 5. Price Changes

We reserve the right to modify service prices at any time. Price changes will be communicated with at least 30 days notice via email to the registered address. Users with active paid plans retain their current price until the end of the paid period. Renewal after the effective date of the new pricing will be at the updated rates. Continued use of the service after the effective date constitutes acceptance of the new pricing. Consumers are notified of price changes in the same way and may terminate the contract, without penalty, before the new prices take effect.

## 6. Service Modifications

We reserve the right to modify, improve, or discontinue features of the platform with 30 days notice. In case of discontinuation of the platform, intake hashes already computed remain independently verifiable with standard SHA-256 verification tools, provided that the holder keeps the original material (or, for structured intakes, its canonical form) and the reference hash. The UTC timestamp remains the reference recorded by EVIDE at deposit time: it is not verified with hash tools. Where a modification negatively affects a consumer's access to or use of a paid digital service more than marginally, the consumer is informed in advance and may terminate the contract free of charge, as provided by the Consumer Code.

## 7. User Content: Responsibility, Ownership and Confidentiality

**7.1 Responsibility.** The user is solely responsible for the content deposited. It is prohibited to use the platform to deposit illegal, fraudulent, or rights-infringing content. EVIDE does not moderate deposited content but reserves the right to deactivate accounts in case of documented violations, as described in Section 13.5. The user is responsible for having a lawful basis for any personal data of third parties included in deposited content.

**7.2 Ownership.** Depositing content does not transfer its ownership to Informatica in Azienda. Materials submitted by the user (uploaded content, payloads, declarations and other inputs) remain the property of the user or of the relevant rights holders. The user grants Informatica in Azienda only the rights needed to provide the service, namely to store, hash, process and reproduce those materials in the platform's records, in FEDIS documents and, where the user has requested publication, in the public registry. The EVIDE platform, its software, schemas, APIs and documentation, and the formats of the records it generates (such as EAR versions, evidentiary profiles and FEDIS documents) belong to Informatica in Azienda; this gives Informatica in Azienda no right over the user's content contained in those records, and the user may use the records and FEDIS documents relating to their own deposits for their own purposes.

**7.3 No sale of data.** Informatica in Azienda does not sell, trade, rent or license deposit contents (uploaded content, intake payloads, declarations and the contents of EAR and ESB records) to third parties for those third parties' own purposes. Deposit contents are used only to provide and document the service requested by the user, to comply with legal obligations and to protect the security of the platform; they are not reused for advertising, other commercial purposes, unrelated research or third-party purposes without an appropriate legal basis and the user's authorization. Informatica in Azienda may use aggregated statistics that contain neither deposit contents nor personal data, such as the number of intakes processed. This commitment does not prevent processing by the technical providers that Informatica in Azienda uses to provide the service, such as hosting and qualified trust service providers, as described in the Privacy Policy, nor disclosures required by law or by an order of a competent authority.

**7.4 Artificial intelligence.** Informatica in Azienda does not use deposit contents to train, fine-tune or evaluate its own AI models or those of third parties. The platform does not transmit deposit contents to external AI services. Informatica in Azienda does not provide deposit contents to external AI services that it uses manually, for

example to support the development or maintenance of the platform, unless the contents have been anonymised or the user has authorized it in writing for a specific purpose, under arrangements that prevent the provider from using them for its own purposes. Integrations operated by the user, such as AI agents or MCP clients that send data to EVIDE, are under the user's control.

**7.5 Confidentiality.** Informatica in Azienda treats deposit contents as confidential and limits access to them to the persons who need it to provide the service, such as the certifier when a FEDIS is requested. Deposit contents are never published: the public registry shows only the information described in Section 13.9.

**7.6 Organizations and former members.** A user who belongs to an organization on the platform may deposit intakes for that organization. Intakes deposited for an organization are records of that organization: they are accessible to its current members and are billed to the organization. Any new operation on an organization's intake, such as requesting a FEDIS, accepting or declining a quote, sending messages, adding linked intakes to an evidentiary chain, closing an evidentiary chain or starting a continuation chain from it, updating or closing an ESB, or using an API key issued for the organization, requires current membership of the organization at the time of the operation, in addition to the other conditions that apply to that operation. When a user stops being a member, the user's authority to act for the organization ends immediately; API keys issued for the organization in that user's name stop operating for the organization, without being revoked, until the user is readmitted or the key is reassigned. A former member keeps read-only access to the intakes that he or she personally deposited for the organization, limited to the intake itself, its EAR versions, the evidence still stored on the platform and the current status of the request. The former member does not see the messages, the status history, quotes, prices or other economic details of the request, or the other intakes of the organization's evidentiary chain, and cannot perform any operation on those intakes. Former members who did not make a deposit have no access to it. By depositing intakes through its members, an organization acknowledges that the member who made a deposit keeps this limited access after leaving. An organization that needs a different arrangement for specific intakes should contact Informatica in Azienda before depositing them, or may request their deletion in accordance with Section 13.7.

**7.7 Linked Responses.** Where the Linked Responses function is available on the platform, the user who deposited an intake may invite a named person, identified by DAPI number, first name and last name, to declare his or her own position on a representation of that intake. For an organization's intake, the depositor must be a current member of the organization (Section 7.6). On creating the invitation, the depositor declares that he or she is authorized to share the content with the recipient and that the sharing is permitted by the applicable rules and, for an organization's intake, by the organization's authorizations; these remain declarations of the depositor and are not verified by EVIDE. The invitation is personal: it can be used only through the EVIDE account whose DAPI number, first name and last name match those indicated, and it expires 30 days after its creation.

What the recipient receives is not the record: it is a FAST REVIEW representation generated by the platform from the record indicated by the depositor, according to the applicable template, and frozen with its identifier and fingerprint. In this version the fixed phrases of the representation are in Italian; the highlighted parts in quotation marks reproduce texts present in the record as entered through the depositor's account, and the representation does not establish who their original author is. The recipient does not receive the full record or the external documents that the record cites. The recipient may declare one of four positions on that representation (agree, acknowledge without expressing agreement, dispute, not in a position to assess), adding a motivation, which is required in order to dispute, and a reservation; a later response may replace or supplement an earlier one, which remains preserved. Each response is a record of the recipient and is documented in an EAR-LINKED record; the depositor cannot modify or delete it. EVIDE records the requests to

open the link that its server receives and the declarations made by the recipient; these do not prove that a page was displayed, read or understood, and a declaration of having taken note of a notice is not consent.

A response is visible to the recipient, to the depositor while he or she has access to the record under these conditions (for an organization's intake, while he or she is a current member) and, where the depositor has chosen this visibility, to the current members of the organization; former members do not see it. The depositor may revoke an invitation directly. For an organization's intake, revocation follows the rules recorded for the invitation when it was created: these may instead require a revocation request, submitted by the depositor and decided by a current owner or admin of the organization other than the requester and the depositor, or by a review authority designated by the organization whose designation has been verified with the outcome «confirmed»; urgent requests suspend the invitation until the decision. Informatica in Azienda may suspend an invitation for security reasons. If the depositor stops being a member of the organization, the invitations he or she created on its intakes are closed definitively, unless they were created under the rules that keep them usable until their original expiry; in that case the current owners and admins of the organization may suspend, resume or revoke them, stating a reason. Revocations and suspensions prevent new responses and do not modify or delete responses already deposited.

For the review authority, EVIDE records the title document received (its metadata and a reference, not the document itself), the designation and the verification documented by a verifier appointed by Informatica in Azienda, with the method, the source examined and the outcome declared by the verifier. Neither the declarations of the depositor or of the organization nor the recorded verification are an attestation by EVIDE of the legal validity of the power to share or to decide. A response does not modify, confirm or verify the record, does not certify that the record or any declaration is true, and is not assessed by EVIDE; Sections 8 and 9 apply. Responses may be documented in a FEDIS-LINKED under the conditions of Section 7.8. Linked Responses records are retained as evidentiary records (Section 13.3), and the processing of the related personal data is described in the Privacy Policy.

**7.8 FEDIS-LINKED.** When the FEDIS-LINKED function is available on the platform, the depositor of a structured intake deposited through the web interface or the EVIDE Mobile app (Human Structured Intake) may request a FEDIS that documents, in addition to the intake, the includable linked responses (FEDIS-LINKED). The request follows the same procedure and the same economic conditions as any FEDIS: a quote from the certifier, express acceptance by the requester, use of any FEDIS packages and invoicing. A FEDIS-LINKED may be requested only by the depositor of the intake and, for an organization's intake, only while the depositor is a current member of the organization (Section 7.6). Where an intake has includable responses, the other members of the organization cannot request a FEDIS on that intake.

Only responses that were deposited after the recipient was shown the notice describing FEDIS-LINKED, in a version recorded by the platform as eligible, and whose EAR-LINKED record passes the integrity check, are includable. Revocation or suspension of the invitation after the deposit does not exclude the response; the document states the date of any revocation. If a response or an EAR-LINKED fails the integrity check, the request is not accepted.

Each request gives rise to a separate technical record, placed in the same scope as the intake (personal or organization), and to a snapshot of the relevant records. The snapshot is formed by the platform from its own archive at the time of the request and is identified by its SHA-256 fingerprint. For each included response, the FEDIS-LINKED reports: the respondent's name and DAPI number, any declared role, the positions, motivations and reservations, the deposit date, the visibility indicated in the invitation, and the identifiers and fingerprints of the response and of its EAR-LINKED. It also reports descriptive counts of invitations and responses. For non-

includable responses and for invitations without a deposit, it reports counts only, without names or content. When the document is generated, the platform recomputes the fingerprints of the reported records that are still available and compares them with the recorded ones; if there is a discrepancy, the document is not generated, and records no longer available are indicated as not re-verified. Successive requests form a series: each FEDIS-LINKED is an autonomous document, linked to the previous ones, which it neither modifies nor replaces. A new request is possible only after the previous FEDIS request on the same intake has been concluded, and only if there are includable responses not yet documented in an issued FEDIS-LINKED.

The FEDIS-LINKED is delivered to the requester, who may use it and hand it to third parties regardless of the visibility of the response on the platform. The recipient of a FEDIS-LINKED is responsible, within the limits provided by law, for the uses made of it and for any communication to third parties of the personal data it contains, which must comply with applicable law and serve legitimate purposes. The document is not made available through the platform to the other members of the organization, and the technical record is not published in the public registry. When a FEDIS-LINKED is issued, each depositor of an included response receives an essential notice at the address of their account, without data from other responses.

Where a respondent objects to the processing of their data in FEDIS-LINKED documents, Informatica in Azienda may suspend, during the assessment, new requests and issuances that would include that response. The suspension does not modify or delete any record and does not affect documents already issued.

A FEDIS-LINKED documents the existence, integrity and content of the records at the snapshot time. It does not certify that the intake or the responses are true, that any agreement or consensus exists among the participants, or any declared role or power; the counts are counts of individual declarations, not a vote. Sections 8, 9 and 13.8 apply.

**7.9 Closing an evidentiary chain.** A chain of linked intakes that contains at least two intakes may be closed explicitly on the web platform: a personal chain by its holder; an organization's chain by the depositor of the first intake while still a member, or by a current owner or administrator of the organization. Informatica in Azienda does not close or reopen chains on behalf of users, and a chain cannot be closed through API keys or MCP. The closure freezes a manifest of the chain, which lists the included intakes and the SHA-256 fingerprints of their EAR versions, of the deposited files and, for structured intakes, of the canonical intake records, and records who closed the chain, in what capacity and when; that time is recorded by the EVIDE database and is not a qualified time stamp. A closed chain is never reopened. The platform refuses new deposits linked to a closed chain, from the web, the app and the API; material added later may be deposited in a new continuation chain, which refers to the closed chain without becoming part of it. The closure delimits the included intakes: it does not attest that every relevant event was deposited, that the declarations are true or that no unlinked deposits exist. It does not extend the retention of uploaded content (Section 13.2): the package of a closed chain includes only the files that the requester can still download, so a package obtained later may be incomplete with respect to the manifest. A FEDIS may be requested on the manifest of a closed chain under the ordinary FEDIS procedure; its rejection or cancellation does not affect the closure. After issuance, the administration may upload the signed FEDIS document on the manifest. The platform keeps it with its SHA-256 fingerprint, computed on the stored file; a later upload is recorded as a new version, and the previous versions are kept and marked as superseded. The current version is included in the packages of the chain generated afterwards, for users with full access to the technical record of that FEDIS; superseded versions are only listed. Uploading the document and detecting a signature structure in it are not a cryptographic validation of the signature, of the time stamp or of the certificate. The signed document is not a deposited file of an intake and is not removed by the automatic retention of uploaded content (Section 13.2); its retention is governed by Section 13.3. Deletions after the closure are governed by Section 13.7.

## 8. Evidentiary Value and Jurisdictional Responsibility

EVIDE produces independently verifiable evidentiary records anchored to a SHA-256 cryptographic intake hash, a server-generated UTC timestamp, and an identity reference linked to the user's DAPI-verified account. Roles, authority and other statements contained in a deposit remain declarations of the depositor unless the service description states that they are independently verified. The timestamp of the base deposit is generated by the EVIDE server and is not a qualified time stamp. FEDIS is a separate document, generated by the platform and signed by the certifier, that, under the current certification workflow, states the SHA-256 fingerprints of the intake record and of a specific EAR version (see Section 13.8) and adds a qualified electronic signature and a qualified electronic time stamp (eIDAS Art. 41) issued by a third-party qualified trust service provider; the time stamp attests the moment at which it is applied to the FEDIS document and does not make the timestamp of the base deposit qualified. Combined with FEDIS forensic certification, these records are prepared with reference to ISO/IEC 27037:2012 international standards, eIDAS (EU Regulation 910/2014), and Federal Rules of Evidence 901-902 (USA), providing structured forensic documentation usable in judicial, regulatory, and investigative contexts across the EU, United States, United Kingdom, Canada, Australia, and equivalent jurisdictions.

The essential distinction: EVIDE and FEDIS operate as a **probatory crystallization layer** -- not as a guarantee of automatic admissibility. They do not replace the evaluation of the competent authority, the procedural rules of the jurisdiction, or the role of the court. Their function is to reduce uncertainty by documenting the technical conditions that support evidentiary reliability, making integrity verification objective and independent of trust in the certifying platform.

Admissibility, legal weight, or procedural acceptance of evidentiary records may still vary depending on jurisdiction, court, or regulator. The user is responsible for assessing the legal context of their specific proceeding, before subscribing to the service, and for obtaining independent legal advice where required. **Learn more about FEDIS forensic certification →**

## 9. No Warranty on User-Declared Data

EVIDE verifies structural integrity, identity attribution, and intake timing of deposited records. It does not independently verify the factual accuracy, authenticity, completeness, or truthfulness of user-submitted content, declarations, metadata, or any fields declared by the user unless explicitly stated in the service description. The evidentiary value of an EVIDE record derives from its anchoring and integrity properties, not from any guarantee of the accuracy of the declared content.

## 10. UTC Temporal Reference

All timestamps generated by EVIDE are expressed in Coordinated Universal Time (UTC) and represent the platform's independently generated intake time at the moment of deposit processing. EVIDE timestamps are generated server-side and are independent of the user's local clock, device timezone, or client-side time references. They do not represent the time of content creation, signing, or transmission by the user. Discrepancies between user-side timestamps and EVIDE intake timestamps do not constitute a platform error.

## 11. Account Security and API Key Responsibility

Users are responsible for maintaining the confidentiality of API keys, credentials, access tokens, and DAPI codes associated with their account. Actions performed through authenticated credentials -- including API calls, MCP-mediated deposits, and agent-initiated intakes -- are considered attributable to the account holder unless proven otherwise under applicable law. In case of suspected compromise of credentials, the user must notify us immediately at info@informaticainazienda.it. Informatica in Azienda cannot be held liable for deposits, records,

or actions performed through credentials that the user failed to protect. When an account is deactivated, the credentials associated with it are suspended as described in Section 13.5. Informatica in Azienda may also revoke individual credentials, for example in case of suspected compromise; revoked credentials do not become valid again.

## 12. Export Controls and Prohibited Use

The platform may not be used in violation of applicable export controls, sanctions regulations, or laws governing digital evidence and restricted technologies. Use of EVIDE is prohibited where such use would violate the laws of the user's jurisdiction or applicable international regulations. Informatica in Azienda reserves the right to restrict access to users or organizations subject to applicable sanctions or operating in jurisdictions where the service cannot be legally provided.

## 13. Records, Retention, Account Status and Deletion Requests

**13.1 Categories of records.** In providing the service, EVIDE processes different categories of records, which are subject to different rules: (a) account data, such as name, email address, DAPI number and organization; (b) canonical intake records, including the intake hash, the server-generated UTC timestamp, the evide_id, the submitted payload and the evidentiary profile computed by the platform; (c) Evidentiary Artifact Record (EAR) versions and their hashes; (d) Epistemic Stabilization Buffer (ESB) observations, declarations and closure records; (e) content uploaded by the user; (f) FEDIS documents and the records they reference; (g) entries in the EVIDE public registry; (h) operational, security and access logs and billing records; (i) Linked Responses records, such as invitations, declarations, FAST REVIEW representations, responses, EAR-LINKED records, revocation requests, suspensions, revocations and decisions and review-authority data, FEDIS-LINKED snapshots, technical records, notices and suspensions, and the register of changes to organization memberships and to the status of accounts, DAPI identities on EVIDE and organizations; (j) technical records of API requests sent with an idempotency key (Section 13.11); (k) chain closure records, such as the frozen manifest of a closed chain and its SHA-256 fingerprint, the identifier, DAPI number and capacity of the person who closed it, the events recorded after the closure, the references of continuation chains and the records of a FEDIS requested on the manifest and its signed document (Section 7.9). Some of these records may contain personal data of the user or of third parties. A record is not excluded from data protection law merely because it is a hash, an identifier or a technical record.

**13.2 Uploaded content.** For intakes submitted with uploaded content (files, ZIP archives, or a URL or text that the platform stores as a file), the uploaded content is stored on the platform's servers for a limited period and is then deleted, as published in the service description. While it is stored, the user can download it from the account. When a FEDIS is issued for such an intake, its uploaded content is deleted from the platform's storage at the time of issuance; the user should keep an independent copy, or download the content, before issuance. Structured intakes do not include uploaded content: the data submitted with them forms part of the canonical intake record and is handled under Section 13.3. Deletion of uploaded content does not delete the canonical intake record, including the intake hash, nor EAR versions, ESB records or the related metadata, such as the name, size and hash of the uploaded file. The user is solely responsible for keeping an independent copy of any content deposited.

**13.3 Retention of evidentiary records.** Canonical intake records, EAR versions, ESB records and related integrity metadata are not deleted automatically when uploaded content is deleted, when a plan expires, when an account is deactivated or when the contract is terminated. They are retained for as long as necessary to document the deposit and to allow its later verification, in accordance with the retention criteria set out in the Privacy Policy and with applicable law, unless they are deleted earlier through an authorized deletion under Section 13.7. EVIDE does not guarantee that any record will remain available indefinitely. The records of a chain

closure are retained while at least one intake included in the closed chain, or a FEDIS request on its manifest, remains on the platform; when the last of them is deleted, the closure records are deleted with it. The signed documents of a FEDIS on the manifest, including superseded versions, are kept with the closure records: the platform provides no ordinary function to delete them, and while they exist the technical record of that FEDIS and the closure records are not deleted. Any deletion, for example where required by law, is decided separately; this does not amount to a guarantee of indefinite retention.

**13.4 Versioning and integrity.** In the ordinary operation of the platform, an EAR version, once generated, is not edited: when the canonical evidentiary state changes, a new version is added, and each version has a recorded SHA-256 hash. Recomputing the SHA-256 hash of a copy and comparing it with a reference hash shows whether that copy is consistent with the reference. The comparison does not, by itself, prove that both the stored record and the reference hash have remained unchanged; that depends on where and how the reference hash was preserved, for example in a FEDIS or in a copy kept by the user. Hash consistency does not establish that the content of a record, or any declaration in it, is true. This section describes how records are handled by the platform; it is not a promise that records can never be removed in the circumstances described in Sections 13.7 to 13.10.

**13.5 Account deactivation.** Deactivation is an administrative measure. Informatica in Azienda may deactivate an account, in particular in the cases described in Sections 4, 7, 11 and 12, at the user's request, or for security reasons. While an account is deactivated, all authenticated access is suspended: web sessions, mobile access tokens and API keys associated with the account are rejected, and no new deposits, ESB updates or closures can be made. Deactivation does not delete account data, intake records, EAR versions, ESB records, FEDIS documents or other records, and it is neither a termination of the contractual relationship nor an erasure of personal data. If the account is reactivated, credentials that have not expired and have not been explicitly revoked may be used again.

**13.6 Termination, account closure and permanent deletion.** The user may request termination of the contract, closure of the account or permanent deletion of the account by writing to app@certifywebcontent.com or, alternatively, to info@informaticainazienda.it. Informatica in Azienda may terminate the service in the cases provided for in these conditions or by law. Termination ends access to the platform and does not affect payment obligations that have already accrued; on its own, it does not delete account data or records, which are handled in accordance with Section 13.3. Where the user requests closure of the account, Informatica in Azienda, after verifying the identity and documented authority of the requester, deletes the user's personal intakes that can be deleted under Section 13.7, together with their dependent records, permanently revokes the user's sessions and API keys and removes the user's organization memberships. If no record linked to the account has to be retained, the account and the enrolment of the user's DAPI identity on EVIDE are deleted. If records linked to the account have to be retained, such as intakes deposited for an organization, intakes that cannot be deleted under Section 13.7 or records that must be kept by law, the account is kept in a closed state, linked only to those records: it cannot be used to sign in and is not used for any other purpose, and the user is informed of the records retained and of the reasons. Closing an EVIDE account does not revoke or alter the user's DAPI certification, which is governed by its own terms. A closed account is never reopened automatically: access may be restored only on request, after verification of the requester's identity, and a user whose account has been deleted may be enrolled again as a new account; in both cases, deleted records, revoked credentials and former organization memberships are not restored. Deletion removes the deleted data from the platform's active systems; it does not reach documents already delivered to the user or to third parties, copies outside the control of Informatica in Azienda, records that must be retained by law, or backup copies until they are overwritten, as described in the Privacy Policy. Deactivation (Section 13.5) is neither closure nor deletion.

**13.7 Requests to delete intakes and accounts.** The platform does not currently offer users a self-service function to delete intakes, EAR versions, ESB records or the account. Requests are made in writing to app@certifywebcontent.com or, alternatively, to info@informaticainazienda.it and may concern one intake, several intakes, all intakes associated with an account, or the account itself. A request received through another channel is not disregarded for that reason alone; in no case is the address from which a request is sent, in itself, sufficient proof of the requester's identity or authority. Informatica in Azienda verifies the identity and documented authority of the requester and assesses each request in accordance with applicable law, taking into account, in particular, whether a FEDIS has been issued, whether the intake is referenced by other intakes in an evidentiary chain, the rights and interests of third parties and any retention required by law. The existence of a FEDIS or of EAR versions does not in itself prevent deletion; equally, not every request will necessarily be granted. Where deletion is authorized, its scope may include the canonical intake record, EAR versions, ESB buffers and events, public-registry entries, FEDIS-related platform records and other associated technical records. Records are deleted in an order that preserves the integrity of evidentiary chains: an intake on which other intakes depend in a chain is not deleted while those intakes remain, and the chain of the remaining intakes is never altered. Where an authorized deletion cannot be carried out for technical reasons, for example because an issued FEDIS is linked to package or billing records that the platform keeps unaltered, the request is assessed separately; where erasure is due but cannot be carried out at that time, processing is restricted. A technical constraint is not in itself a legal ground for refusing erasure. Intakes deposited for an organization are assessed also in the light of the organization's rights (Section 7.6). Intakes to which Linked Responses invitations or responses are linked are not deleted through the ordinary procedure: the request is assessed separately, also taking into account the rights of the recipients over their own responses and the related revocation records (Section 7.7). A request to delete all intakes is not automatically treated as a request to close the account, and vice versa. The requester is informed of the deletion actually carried out and, where a request is not granted in full, of the reasons. Where a request is made under data protection law, Section 13.10 also applies. If an intake included in a closed chain is deleted, the deletion is recorded as an event after the closure, and the frozen manifest of the chain is not changed (Section 7.9).

**13.8 Certified records (FEDIS).** A FEDIS is a separate document, signed by the certifier and delivered to the user. A FEDIS issued under the current certification workflow states two SHA-256 fingerprints: the intake hash (for intakes with uploaded content, the fingerprint of the received content; for structured intakes, the fingerprint of the canonical intake record) and the hash of the specific EAR version that was current when the FEDIS was issued. That EAR version remains the reference for the FEDIS even if later EAR versions are generated. A FEDIS-LINKED also states the SHA-256 fingerprint of the snapshot of the linked responses and, for each included response, the fingerprints of the response and of its EAR-LINKED, with the outcome of the checks performed when it was generated (Section 7.8). A FEDIS issued before EAR references were introduced into the certification workflow may not reference an EAR version. An authorized deletion under Section 13.7 may include the platform records referenced by a FEDIS. Deletion of platform records does not alter or revoke a FEDIS document already delivered, and that document cannot be removed from the possession of the user or of third parties to whom it has been delivered; once the relevant platform records have been deleted, however, it may no longer be possible to verify that FEDIS against EVIDE's records. Accounting and tax records relating to a FEDIS, such as invoices, are separate from the evidentiary records and are retained as required by law.

**13.9 Public registry.** An entry is published in the EVIDE public registry only at the depositor's request, made when submitting the intake, where the form offers this option, or in writing, and only for intakes for which a FEDIS has been issued; publication is carried out by the certifier. A published entry shows the reference ID, the FEDIS code, the status, the intake hash, the intake timestamp and the publication date; the registry may also show other published entries with the same hash and, for intakes that belong to an evidentiary chain, the position of the entry in the chain. The technical records of FEDIS-LINKED documents and of FEDIS on the

manifest of a closed chain are not published in the public registry. Published entries are publicly accessible and may be indexed by search engines. The user may request removal of an entry at any time by writing to app@certifywebcontent.com or, alternatively, to info@informaticainazienda.it. Removal from the public registry removes the public listing only: it does not delete the underlying intake records, EAR versions or FEDIS documents, and it does not revoke, invalidate or alter an issued FEDIS. Informatica in Azienda cannot control copies of public listings made by third parties, including search engines, before removal.

**13.10 Data protection rights.** Nothing in these conditions limits the rights that data subjects have under Regulation (EU) 2016/679 (GDPR) or other mandatory law, including the rights of access, rectification, erasure, restriction and objection. Requests to exercise these rights are handled as described in the Privacy Policy and within the time limits set by law. Where the erasure of personal data is requested, Informatica in Azienda will assess whether one of the exceptions provided for in Article 17(3) GDPR applies in the specific case, for example where retention is necessary for the establishment, exercise or defence of legal claims. Any such exception is applied only to the extent that it is necessary in the specific case; where it applies, processing may be restricted instead of the data being erased. Administrative deactivation (Section 13.5) and termination (Section 13.6) are distinct from erasure and do not replace the assessment of an erasure request. The user is responsible for having a lawful basis for any personal data of third parties included in deposited content and declarations.

**13.11 Repeated API requests (idempotency keys).** For the API requests for which the technical documentation provides it, the user's system may send an idempotency key that it chooses. Its use is optional: without it, each request is processed as a new request. For 7 days from the first request sent with a given key, a request repeated with the same key, through the same API key, to the same endpoint and with the same content is not executed a second time: the platform returns the outcome already recorded for that key or, if the first request is still in progress or was interrupted, processes it so that it takes effect only once. A request repeated with the same key but with different content, or to a different endpoint, is refused. After 7 days the key is no longer recognised, and a request sent with it is processed as a new request, which may create a new deposit. The user is responsible for generating the keys, for using a different key for each distinct request and for not including personal data or confidential information in them. Where an intake is deleted under Section 13.7, the outcome recorded for the keys that refer to it is replaced by a notice that the record no longer exists, which contains no data of the record; until the end of the 7-day period, a request repeated with such a key receives that notice and does not create a new deposit. This mechanism reduces the duplicates that may arise from repeating the same request within the limits described above; it does not guarantee that the platform will never hold more than one deposit relating to the same event, for example where the same event is sent with different keys, with different content, without a key or after the 7-day period, and it does not establish whether two deposits relate to the same event. A repeated request that returns the outcome already recorded does not create a deposit and is not counted as an additional intake; a deposit completed through a repeated request is counted once, when it is completed. Repeated requests remain subject to authentication, authorization and the request-rate limits of the plan. The technical records used for this purpose are not part of the evidentiary record and are described in the Privacy Policy.

## 14. Limitation of Liability

Informatica in Azienda cannot be held liable for: indirect or consequential damages; loss of data caused by user actions; incorrect interpretations of evidentiary records by third parties; decisions made on the basis of EVIDE records by courts, regulators, or other parties; failure of evidentiary records to be admitted in any legal or administrative proceeding. Nothing in this section excludes or limits liability for wilful misconduct or gross negligence, or any liability that cannot be excluded or limited under applicable law. For consumers, the limitations of liability in this section and in Sections 2, 3, 4 and 9 apply only to the extent permitted by the Consumer Code and do not affect the consumer's statutory rights, including the legal guarantee of conformity.

## 15. Governing Law and Jurisdiction

These conditions are governed by Italian law. For any dispute with professional users, the Court of Bologna, Italy, has exclusive jurisdiction, except where mandatory law provides otherwise. For disputes with consumers, the competent court is that of the consumer's place of residence or domicile, where located in Italy. Consumers resident in another country retain the protection afforded to them by the mandatory provisions of the law of that country and by the applicable rules on jurisdiction.

## 16. Acceptance, Changes and Right of Withdrawal

**16.1 Acceptance.** These conditions apply from the moment the platform is first used. For API plans, they are expressly accepted when the API service is activated, and the accepted version is recorded. Other paid services are provided on the basis of a written request or order, for example by email, indicating the service and its price. For consumers, a contract for a paid service is concluded only with the consumer's express acceptance; before it is concluded, Informatica in Azienda provides the information required by the Consumer Code, and after it is concluded it sends confirmation of the contract on a durable medium.

**16.2 Changes.** Informatica in Azienda may update these conditions by giving at least 30 days' notice by email to the registered address; the notice indicates the new version and the date from which it applies. Where required by law or by the nature of the change, Informatica in Azienda will request renewed acceptance. A consumer who does not accept a change may terminate the contract free of charge before the change takes effect. Earlier versions of these conditions remain available on request. Each version of these conditions, together with the Privacy Policy in force from the same date, is also published as a PDF document bearing a qualified electronic signature, which can be downloaded from the page of these conditions with its SHA-256 fingerprint; once published, a signed copy is never replaced. The signed copy documents the content and the date of the version; acceptance is recorded as described in Section 16.1. A new version applies from its effective date and does not change acts already completed under an earlier version, such as deposits made, FEDIS documents issued or acceptances recorded; recorded acceptances of earlier versions remain unchanged. For users already registered on the publication date, a new version applies from the effective date stated in the notice. A contract concluded after the publication of a new version may expressly refer to it: in that case, that version applies to that contract from its conclusion. A function described in a new version can be used only from when it is available on the platform.

**16.3 Right of withdrawal (consumers).** A consumer who concludes a contract for a paid service at a distance may withdraw from it within 14 days of its conclusion, without giving any reason, by sending an unequivocal statement to info@informaticainazienda.it; the model withdrawal form provided by the Consumer Code may be used but is not mandatory. If the consumer has expressly requested that the service begin during the withdrawal period and then withdraws, the consumer pays an amount proportionate to the service provided until the withdrawal was communicated. The right of withdrawal is lost only if the service has been fully performed and performance began with the consumer's express prior consent and acknowledgement that the right would be lost once the contract had been fully performed. Amounts due to the consumer are refunded within 14 days of receipt of the withdrawal, using the same means of payment unless otherwise agreed.

**16.4 Specific approval and unfair terms.** Clauses that under applicable law require specific approval are effective only if approved in the form required by law. Clauses that are unfair under the Consumer Code do not bind consumers.

PART A: ENGLISH

# Privacy Policy & Cookie Policy

Version 2026-16 - effective from 24 November 2026 · https://app.certifywebcontent.com/privacy

Information on the processing of personal data pursuant to Regulation (EU) 2016/679 (GDPR) for the EVIDE platform at app.certifywebcontent.com, the EVIDE API and the EVIDE Mobile app.

## 1. Data Controller

The data controller is **Informatica in Azienda**, represented by Dott. Emanuel Celano, registered address Via Vaccaro 5, 40132 Bologna, Italy, VAT IT02137271207.

Email: info@informaticainazienda.it - Phone: +393771151946

## 2. Scope of This Policy

This policy applies to the EVIDE platform at app.certifywebcontent.com, to the EVIDE API, to the EVIDE Mobile app and to the EVIDE public registry. It applies to users of the platform, to other persons whose personal data are contained in deposited content and to persons whose data are recorded for the Linked Responses function (for example persons designated to decide on revocations, verifiers and holders of the organization's contact addresses). The EVIDE Governance Lab (lab.certifywebcontent.com) has its own privacy notice. The terms of the service are set out in the Service Conditions.

## 3. Personal Data We Process

**Account and identity data:** first name, last name, email address, DAPI number and DAPI certificate reference, preferred language, organization and role within it, account status (active, deactivated or closed), dates of registration, verification and last sign-in. DAPI data come from the DAPI identity certification, which is also operated by Informatica in Azienda.

**Authentication data:** one-time sign-in codes (stored only in hashed form), the session cookie, mobile access tokens (stored only in hashed form) with device name, platform, app version, last IP address and revocation status, API keys (stored only in hashed form) with their plan, usage and the record of acceptance of the Service Conditions (date, IP address, version and digest of the accepted text).

**Intake data:** the canonical intake record (submitted payload or structured data, declarations, names and roles entered by the user, the evidentiary profile computed by the platform, the intake hash, the UTC timestamp and the evide_id), uploaded content (files, ZIP archives, URLs or texts stored as files) and its metadata (name, size, type and hash).

**EAR and ESB records:** Evidentiary Artifact Record versions and their hashes; Epistemic Stabilization Buffer observations, declarations, events and closure records.

**Certification data:** FEDIS requests, quotes and decisions, the status history of the request, messages exchanged with the certifier and the platform records referenced by an issued FEDIS (FEDIS code, certified hash, EAR reference). For FEDIS-LINKED documents: the technical emission record, its number in the series, the link to the intake, the fingerprint of the snapshot and the outcome of the checks performed when the document was generated.

**Chain closure records:** when a chain of linked intakes is closed, the platform records the frozen manifest of the

chain and its SHA-256 fingerprint, the identifier, DAPI number and capacity of the person who closed it and, for an organization, his or her role, and the time of the closure. The manifest contains the identifiers, times and fingerprints of the included intakes, EAR versions and files; it does not contain the names of the depositors or the original names of the files. The platform also records the events that occur after the closure, such as the deletion of an included intake, with the person who carried out the operation, the references of continuation chains with the user who started them, and requests for a FEDIS on the manifest with the user who made them. When a FEDIS on the manifest has been issued, the administration may upload the signed PDF: the platform records the file, its original name, size and SHA-256 fingerprint, the administrator who uploaded it, the time of the upload, whether a signature structure was detected and, for later uploads, the superseded versions. The PDF contains the data stated in the FEDIS, such as the DAPI number of the requester, the DAPI number and capacity of the person who closed the chain and the data of the certifier, and the data embedded with the signature and the time stamp, such as the name of the signatory, the certificate data and the time of signing. These data are processed to document the issued FEDIS and to include it in the packages of the chain, for the purposes and on the legal bases of the FEDIS service (Section 4). The platform does not validate the signature, the time stamp or the certificate.

**Linked Responses data:** the data in this block and in the register of access changes are processed when the related functions are active on the platform.

- **invitations:** the inviting user; the record the invitation refers to and the organization that holds it; first name, last name and DAPI number of the recipient as entered by the inviting user; the visibility chosen; dates of creation, expiry and revocation. The invitation link is stored only in hashed form;
- **declarations of the inviting user** (sharing and authorization) and the FAST REVIEW representation of the record made available to the recipient, with their digests. The recipient does not receive the full record or the external documents the record cites;
- **responses:** the position declared by the recipient on the representation of the record, not on the whole record; any motivation and reservation written by the recipient (a motivation is required in order to dispute) and the relation to an earlier response of the recipient, which remains preserved; name and DAPI number at the time of the deposit; any declared role; declaration of having taken note of the summary; date and digests. EAR-LINKED is the EAR document that documents the response;
- **invitation events observed by the server:** requests to open the link that the server receives, including with an account other than the recipient's or on a suspended invitation; representations produced by the server; declarations of having taken note of the notices. These events do not prove that a page was displayed on the device, read or understood;
- **revocation of invitations:** direct revocations by the inviting user or by an owner or admin of the organization, with the reason given; revocation requests (requester, observed role, reason, description, urgency); suspensions; decisions, with the decider and the elements on which they are based; notifications sent and their delivery attempts;
- **review authority:** metadata of title documents received (type, declared sender and role, channel, date of receipt, digest and reference to the place where the document is kept, not the document itself); name and DAPI number of the designated person, with the period of the designation; who recorded these data; verifications (verifier, method, source examined, declared outcome, digest and reference of the evidence); the organization's email or PEC contact addresses used for alerts;
- **FEDIS-LINKED** (when the function is active):
    - the immutable **snapshot** of the relevant records, formed when the depositor of an intake requests a FEDIS-LINKED. For includable responses it contains the response data listed above: name and DAPI number at the time of deposit, any declared role, positions, motivations, reservations, visibility, dates and fingerprints, and the date of any later revocation of the invitation. For non-includable responses and for

invitations it contains only identifiers, the recipient's DAPI number, dates, status and fingerprints, without names or content. It also contains the descriptive counts reported in the document;
    - the **notices** sent to respondents when a document including their response is issued: recipient, response, emission, delivery outcome;
    - **suspensions** of new emissions while an objection is assessed: response concerned, case reference, opening and closing dates, no content of the objection.

  Before the free-text fields (motivation, reservation, role), respondents are warned not to enter health data or other special categories of data, unnecessary data about other people, or confidential information that is not relevant. The platform is not designed to process special categories of data; the warning is not a legal basis for processing them.
- **technical registers:** technical observations of requests (user, mobile session, function called, channel, result, declared app version; no IP address and no free text); registers that prevent the same action from being recorded twice; deposit preparations that were not used.

**Register of access changes:** every request to add or remove an organization membership, to close or reactivate an account, to deactivate or reactivate a DAPI identity on EVIDE or to suspend or reactivate an organization is recorded with its time, outcome (executed, refused or without effect), the person concerned (identifier and DAPI number), organization, role before and after, who acted and under which authorization, and the originating function. The resulting alerts to the EVIDE administrator contain only counts and internal identifiers.

**Public registry data:** for published entries only, the data described in Section 8.

**Logs and security data:** API request logs (API key, endpoint, IP address, request hash, result, error and processing time), application logs, web server logs, counters used to limit sign-in attempts and API requests.

**API idempotency records:** when an API request is sent with an idempotency key, the platform records the API key used, the key chosen by the client system, the endpoint, a SHA-256 fingerprint of the request, the status and times of processing, the internal reference to the intake or buffer concerned and a copy of the response returned. For a deposit, that copy contains the data returned by the API, which may include declarations and other intake data described above. These records are used only to recognise a repeated request and return the same outcome; they are not part of the evidentiary record and are not included in hashes, EAR versions or FEDIS documents.

**Billing data:** billing details provided by the user or the organization (for example name, company, address and tax identifiers), plans and packages purchased, usage, billing events and invoices.

**Communications:** emails and requests sent to Informatica in Azienda, including support requests and requests to exercise rights or to delete data.

**Personal data of third parties:** deposited content may contain personal data of persons other than the user (for example persons named in a document, a screenshot or a declaration). Informatica in Azienda does not select these data: they are chosen by the user who makes the deposit.

Account and authentication data are necessary to use the platform; without them the service cannot be provided. The platform is not designed to process special categories of personal data: users should not deposit them unless they have a specific legal basis to do so.

## 4. Purposes and Legal Bases

**Providing the service** (account, sign-in, intakes, EAR, ESB, chain closures, FEDIS, API, mobile app, support and, where the user requests it, publication in the public registry): performance of a contract or of pre-contractual steps requested by the user (Article 6(1)(b) GDPR). This includes recognising API requests repeated with an idempotency key, so that the same request takes effect only once.

**Linked Responses:**

- creating invitations, making available the FAST REVIEW representation generated from the record indicated by the inviting user, according to the applicable template, recording responses and EAR-LINKED, revocation requests, suspensions and decisions: performance of the contract with the inviting user, with the responding user and with the users who request or decide a revocation (Article 6(1)(b) GDPR);
- forming the snapshot, documenting responses in a FEDIS-LINKED requested by the depositor of the intake, and notifying respondents:
  - for the data of the requester: performance of the contract (Article 6(1)(b) GDPR);
  - for the data of respondents and of the other invitation recipients: the legitimate interest of the depositor in documenting the responses received in a verifiable way and of Informatica in Azienda in providing that documentation (Article 6(1)(f) GDPR).

  Only responses deposited after the recipient was shown a notice describing FEDIS-LINKED are documented with their content; for the other responses and for invitations without a deposit, only counts are reported. Acknowledging the notice is not consent;
- processing the recipient data entered by the inviting user and the data of designated persons, verifiers and the organization's contact addresses, and documenting who was admitted to decide on revocations and on which elements: legitimate interest of Informatica in Azienda, of the organizations and of the users involved in controlled sharing and documented revocation decisions (Article 6(1)(f) GDPR);
- register of access changes and technical registers: legitimate interest in a secure service and in documenting who could act for an organization at a given time (Article 6(1)(f) GDPR); the technical registers also prevent duplicate deposits (Article 6(1)(b) GDPR).

**Accounting, tax and other legal obligations**, including responses to orders of competent authorities: compliance with a legal obligation (Article 6(1)(c) GDPR).

**Security of the platform and prevention of abuse** (authentication, logs, request limits): legitimate interest of Informatica in Azienda and of users in a secure service (Article 6(1)(f) GDPR).

**Retention of evidentiary records after the service has ended**, so that deposits, FEDIS documents and linked responses can still be verified, and the establishment, exercise or defence of legal claims: legitimate interest of Informatica in Azienda and of users (Article 6(1)(f) GDPR), within the limits and periods described in Section 9 and without prejudice to the right to object and to request erasure.

**Service communications**, including notices of changes to the Service Conditions and to this policy: performance of the contract and legitimate interest (Article 6(1)(b) and (f) GDPR).

Personal data are not used for marketing or profiling. The evidentiary profile computed by the platform describes a deposited record; it is not a decision about a person producing legal effects within the meaning of Article 22 GDPR. Users who deposit personal data of third parties are responsible for having a legal basis to do so.

## 5. No Sale of Data, Artificial Intelligence and Confidentiality

Informatica in Azienda does not sell, trade, rent or license deposit contents to third parties for their own purposes, and does not reuse them for advertising, other commercial purposes, unrelated research or third-party purposes. Deposit contents are not used to train, fine-tune or evaluate AI models, either its own or those of third parties. The platform does not transmit deposit contents to external AI services; Informatica in Azienda does not provide them to external AI services that it uses manually unless they have been anonymised or the user has authorized it in writing for a specific purpose. Access to deposit contents is limited to the persons who need it to provide the service. These commitments are set out in Section 7 of the Service Conditions and do not prevent processing by the providers listed in Section 7 below or disclosures required by law.

## 6. Role of Informatica in Azienda

Informatica in Azienda acts as **controller** for account, authentication, security, log, billing and communication data, for the public registry and for the evidentiary records it keeps, including Linked Responses records and FEDIS-LINKED snapshots, in order to provide the service and to allow the later verification of deposits and FEDIS documents.

For personal data of third parties contained in content deposited by a customer, the role of Informatica in Azienda depends on the relationship with that customer. Where a customer, such as an organization, deposits content for its own purposes and Informatica in Azienda processes it only on that customer's behalf, Informatica in Azienda acts as **processor** (Article 28 GDPR) and the processing must be governed by a data processing agreement. Customers who need such an agreement should contact info@informaticainazienda.it before depositing personal data of third parties.

**Organizations and former members.** Intakes deposited for an organization are accessible to its current members. A member who leaves the organization keeps read-only access to the intakes he or she personally deposited for it, limited to the intake, its EAR versions, the evidence still stored and the current status of the request; that member has no access to messages, status history, quotes or other economic details, nor to other intakes of the organization. Former members who did not make the deposit have no access to it. This limited access is based on the legitimate interest of the depositor, who is identified in those records, and of Informatica in Azienda in allowing the depositor to verify the deposits attributed to him or her (Article 6(1)(f) GDPR); it does not allow any new operation on behalf of the organization (Service Conditions, Section 7.6).

## 7. Recipients and Transfers

Personal data may be processed by:

- **Hosting provider:** Aruba S.p.A., on servers located in Italy, acting as processor for hosting and backup.
- **Email:** emails are sent through the mail server of Informatica in Azienda, which runs on the same hosting infrastructure.
- **Qualified trust service providers:** when a FEDIS is issued, the certifier applies a qualified electronic signature and a qualified electronic time stamp through a qualified trust service provider, which processes the document or its digest in accordance with its own role under Regulation (EU) 910/2014 (eIDAS).
- **Recipients chosen by the user:** persons to whom the user delivers a FEDIS or other records. A FEDIS-LINKED is delivered to the requester, who may hand it to third parties and is responsible for the uses and communications made of it (Service Conditions, Section 7.8). The document reports the data of the included responses regardless of the visibility chosen for the response on the platform.
- **Linked Responses participants:** the recipient of an invitation sees the FAST REVIEW representation generated from the record indicated by the inviting user, according to the applicable template, and the invitation information. The response, with the name, DAPI number and any declared role of the responding

user, is visible to the inviting user only while that user has access to the record under the applicable rules (for an organization record, while he or she is a current member) and, where the inviting user has chosen this visibility, to the current members of the organization that holds the record; former members do not see it. The other members of the organization do not receive the FEDIS-LINKED or the snapshot through the platform, and do not see the summary of responses, which is shown only to the depositor of the record. Current owners and admins of the organization also see the invitations still usable that were created on its records by persons who are no longer members. Revocation requests are visible to the current owners and admins of the organization, to persons designated to decide and to the EVIDE administrator. Review-authority data are visible to the EVIDE administrator and to the verifiers appointed by Informatica in Azienda; when a designated person decides, the basis of the decision (designation, title date, verification and declared outcome) is shown together with the decision. If no one can decide within the review period, an alert containing only the identifiers of the request may be sent to the organization's verified contact addresses.

- **The public:** for entries published in the public registry, the data described in Section 8.
- **Professional advisers** bound by confidentiality, and **authorities** where required by law.

The EVIDE Mobile app is distributed through app stores, which process data in accordance with their own policies. One page of the site, Evidentiary Questions, includes a translation widget provided by a third party (see Section 14).

Informatica in Azienda does not transfer personal data outside the European Economic Area, except where required by law. The translation widget described in Section 14 is loaded from a third-party provider: that provider and the translation services it uses may process visitors' technical data, such as the IP address, outside the European Economic Area, under their own terms.

## 8. Public Registry

An entry is published in the EVIDE public registry only at the depositor's request and only for intakes for which a FEDIS has been issued; publication is carried out by the certifier. A published entry shows the reference ID, the FEDIS code, the status, the intake hash, the intake timestamp and the publication date. The registry may also show other published entries with the same hash and, for intakes that belong to an evidentiary chain, the position of the entry in the chain and the existence of other unpublished intakes in the same chain, without their content or identifiers. Published entries are publicly accessible and may be indexed by search engines.

Identifiers and hashes can be personal data where they can be linked to a person. The user may request removal of an entry at any time by writing to app@certifywebcontent.com or, alternatively, to info@informaticainazienda.it. Removal deletes the public listing; it does not delete the underlying records, which are handled as described in Sections 9 and 11. Copies of public listings made by third parties before removal are outside the control of Informatica in Azienda.

## 9. Retention

Personal data are kept only for as long as necessary for the purposes for which they are processed. Retention periods and criteria:

- **Account data:** for as long as the account exists. After the account is closed or deleted, they are removed from active systems, except the data needed to document the contractual relationship, the acceptance of the Service Conditions and the related communications, which are kept for the establishment, exercise or defence of legal claims for no longer than the ordinary limitation period of 10 years (Article 2946 of the Italian Civil Code), and the data that must be kept for accounting and tax purposes. Where an account is closed but records linked to it are retained, for example intakes deposited for an organization or records that

cannot yet be deleted, the account record is kept in a closed state, together with the name and DAPI number attributed to those records, only for as long as those records are retained, and it is not used for any other purpose.

- **Uploaded content:** deleted automatically from the server at the end of the period shown on the pricing page for the status of the intake, or when a FEDIS is issued, whichever comes first.
- **Canonical intake records, EAR and ESB records, certification history and messages, FEDIS-related records:** for as long as the account exists; after it is closed, for the period necessary to allow the verification of the deposits and of any FEDIS issued and the establishment, exercise or defence of legal claims relating to them, which as a rule does not exceed 10 years from the end of the contractual relationship, unless a longer period is necessary because of a pending dispute or a request from a competent authority. These records are not deleted automatically: at the end of the period, Informatica in Azienda deletes or anonymises them. They may be deleted earlier as described in Section 11.
- **Chain closure records:** within the periods of the previous item, for as long as at least one intake included in the closed chain, or a FEDIS request on its manifest, remains on the platform; when the last of them is deleted, the closure records and their events are deleted with it. The reference kept by a continuation chain follows the records of that chain. The signed documents of a FEDIS on the manifest, including superseded versions, are kept with the closure records and are not removed by the automatic retention of uploaded content; the platform provides no ordinary function to delete them and, while they exist, the technical record of that FEDIS and the closure records are kept. Any deletion, for example where required by law or following a request under Section 12, is assessed separately.
- **Linked Responses records, the register of access changes and related administrative alerts** (invitations and their events; declarations of the inviting user; representations; responses; acknowledgements; EAR-LINKED; revocation requests, suspensions, revocations and decisions, with their notifications; review-authority data; FEDIS-LINKED snapshots, technical records, notices and suspensions): for as long as the accounts concerned and the record they refer to exist; after that, for the period necessary to allow the verification of the responses and decisions and the establishment, exercise or defence of legal claims relating to them, which as a rule does not exceed 10 years from the end of the last contractual relationship concerned, unless a longer period is necessary because of a pending dispute or a request from a competent authority. These records are not deleted automatically: at the end of the period, Informatica in Azienda deletes or anonymises them.
- **Title documents and verification evidence of the review authority:** only the metadata and references described in Section 3 are kept on the platform, for the period of the previous item. The original documents are not uploaded to the platform and remain in the channel or archive named in the reference; those received by Informatica in Azienda are kept under the "Communications and requests" item.
- **Linked Responses technical registers:** technical observations of requests: 90 days from recording. Registers against recording the same action twice, and deposit preparations that were not used: 30 days (720 hours) from the definitive closure of the invitation they refer to, that is, from its revocation or, if earlier, from its original expiry; suspensions and other reversible states of the invitation do not start the period. Every month Informatica in Azienda checks which registers have reached the end of the period and, where needed, deletes them through a manual, recorded retention run. Web server logs ("Web server logs" item), backup copies (Section 10) and temporary exports made during maintenance remain separate; such exports are kept with restricted access and deleted when no longer needed.
- **Public registry entries:** until removal is requested or the underlying records are deleted.
- **Sign-in codes:** valid for 15 minutes; deleted within 24 hours after expiry. Counters of sign-in attempts are deleted once the 15-minute lock period has ended.
- **Web sessions:** a web session ends one hour after sign-in; the session cookie is deleted when the browser is closed.

- **Mobile sessions:** a mobile access token remains valid until the user signs out or the session is revoked. Records of revoked sessions are deleted 12 months after revocation; records of active sessions are deleted together with the account.
- **API request logs and application logs:** 12 months. Monthly usage totals derived from API logs are kept as billing records.
- **API idempotency records:** 7 days from the first request sent with the key; they are then deleted by a daily automatic procedure. When an intake is deleted, the copies of the responses that refer to it are immediately replaced by a notice that contains no data of the record, and the remaining technical record is deleted at the end of the same period. A record of a request interrupted after its deposit had been recorded is not deleted automatically, because deleting it could cause the same deposit to be recorded twice: it is kept until the request is completed by a retry with the same key or until Informatica in Azienda, having checked the case, deletes it.
- **API request-rate counters:** deleted after 15 minutes.
- **Web server logs:** kept according to the log rotation configured on the hosting server.
- **Billing data and accounting records:** billing details for as long as the account exists; invoices and accounting records for 10 years, as required by Article 2220 of the Italian Civil Code.
- **Communications and requests**, including requests to exercise rights or to delete data and the related authorizations: for as long as necessary to document the request and its outcome, as a rule no longer than 10 years.

## 10. Backups and Copies Outside Our Control

The hosting environment keeps backup copies for disaster recovery. Data deleted from active systems may remain in backup copies until those copies are overwritten in accordance with the backup rotation. Backup copies are not used for any other purpose; if a backup has to be restored, data deleted in the meantime are deleted again. Occasional exports made for maintenance or testing are kept only for the time needed for that activity and are then deleted.

Deletion from EVIDE's systems cannot reach copies outside the control of Informatica in Azienda, such as FEDIS documents and other records already delivered to the user or to third parties, files downloaded by the user and copies of public listings made by third parties.

## 11. Deactivation, Account Closure and Deletion

**Deactivation** suspends access to the account; it does not delete account data or evidentiary records.

**Account closure and deletion** can be requested in writing to app@certifywebcontent.com or, alternatively, to info@informaticainazienda.it. The platform does not currently offer users a self-service function to delete intakes or the account: each request is assessed individually, on the basis of the identity and documented authority of the requester and of applicable law. Where deletion is authorized, it may include the account, the canonical intake records, EAR versions, ESB records, public-registry entries and the FEDIS-related records kept on the platform, which are removed from active systems. Deletion of an intake to which Linked Responses invitations or responses are linked is not carried out through the ordinary procedure: it is assessed separately, also taking into account the rights of the other users over their own declarations and the related revocation records.

When an account is closed, the user's personal intakes that can be deleted are deleted together with their dependent records, sessions and API keys are permanently revoked and organization memberships are removed. If nothing has to be retained, the account and the enrolment of the user's DAPI identity on EVIDE are

deleted; otherwise the account is kept in a closed state, linked only to the records that must be retained (see Section 9), and the user is informed of what has been retained and why. Closing an EVIDE account does not revoke the DAPI certification, which is governed by its own terms. A closed account is not reopened automatically: access can be restored only on request, after verification of the requester's identity, and deleted records, revoked credentials and former organization memberships are not restored.

Some data may be kept after an authorized deletion only where a documented legal basis justifies it, for example accounting records that must be kept by law or data needed for a pending dispute. Where a deletion cannot be carried out for technical reasons, processing is restricted until it can be carried out; a technical constraint is not in itself a legal ground for refusing erasure. Deleted data may remain in backup copies as described in Section 10. Once the relevant platform records have been deleted, a FEDIS already delivered may no longer be verifiable against EVIDE's records.

## 12. Your Rights

Under Articles 15 to 22 GDPR you have the right to:

- access your personal data;
- request their rectification;
- request their erasure, which is assessed case by case and may be limited where an exception under Article 17(3) GDPR applies in the specific case, for example where the data are necessary for the establishment, exercise or defence of legal claims;
- request the restriction of processing, which may also apply instead of erasure;
- receive the data you have provided in a structured, commonly used and machine-readable format, where processing is based on the contract and carried out by automated means;
- object to processing based on legitimate interest;
- lodge a complaint with the Italian supervisory authority (Garante per la protezione dei dati personali, www.garanteprivacy.it) or with the supervisory authority of the country where you live or work.

A respondent may object to the documentation of their response in new FEDIS-LINKED documents. While the objection is assessed, Informatica in Azienda may suspend new requests and issuances that would include it; the suspension does not modify or delete any record and does not reach documents already delivered (Section 10).

Requests should be sent to app@certifywebcontent.com or, alternatively, to info@informaticainazienda.it. Informatica in Azienda may ask for information needed to verify the identity of the requester. A request received through another channel is not disregarded for that reason alone; the address from which a request is sent is not, in itself, sufficient proof of identity. A reply is given without undue delay and in any case within one month of receipt; this period may be extended by two further months where necessary, taking into account the complexity and number of requests, and the requester is informed of any extension within the first month. Requests are free of charge, unless they are manifestly unfounded or excessive. Informatica in Azienda informs the recipients to whom data have been disclosed of any rectification, erasure or restriction, unless this proves impossible or involves disproportionate effort.

Persons whose data are contained in content deposited by a user may also exercise these rights. Where Informatica in Azienda acts as processor for a customer, it forwards the request to that customer and assists it in responding.

## 13. Security

The platform is accessible only over encrypted connections (HTTPS). Session cookies are protected (Secure, HttpOnly, SameSite=Strict); sign-in codes, mobile access tokens and API keys are stored only in hashed form. Access to accounts can be suspended immediately, and sign-in attempts and API requests are rate-limited. Integrity hashes allow any alteration of deposited records to be detected against a reference hash.

## 14. Cookie Policy

**Technical cookies (no consent required):**
The platform uses only cookies that are strictly necessary for it to work:

- `cwc_session`: session cookie used to manage authentication; it is deleted when the browser is closed;
- `lang`: stores the language selected by the user; duration 12 months.

These cookies do not require consent and are installed automatically.

**Third-party translation widget:**
The Evidentiary Questions page loads a translation widget provided by GTranslate (cdn.gtranslate.net). When the page is opened, the browser connects to that provider's servers; if a translation is selected, the widget may store a cookie to remember the chosen language, and the translation is provided by third-party translation services. No other page of the platform loads this widget.

**No tracking cookies:**
The platform does not use Google Analytics, Facebook Pixel or other analytics, advertising or profiling cookies.

**EVIDE Mobile app:**
The app does not use cookies. It keeps the access token on the device so that the user remains signed in until signing out.

**Cookie management:**
You can manage or delete cookies from your browser settings. Disabling technical cookies may prevent the platform from working correctly.

## 15. Changes to This Policy

This policy may be updated. Material changes are communicated by email to registered users at least 30 days before they take effect; the notice indicates the new version and the date from which it applies. The current version is always available at this address, and earlier versions are available on request. Each version of this policy, together with the Service Conditions in force from the same date, is also published as a PDF document bearing a qualified electronic signature, which can be downloaded from this page with its SHA-256 fingerprint; once published, a signed copy is never replaced.

PARTE B: ITALIANO

# Condizioni di Servizio

Versione 2026-16 - in vigore dal 24 novembre 2026 · https://app.certifywebcontent.com/service-conditions

Il testo di riferimento ai fini dell'accettazione del servizio API e' la versione inglese; le altre lingue sono fornite per comodita'.

## 1. Oggetto e ambito

Le presenti condizioni disciplinano l'utilizzo della piattaforma EVIDE gestita da Informatica in Azienda, diretta dal Dott. Emanuel Celano. Le presenti condizioni, unitamente alla Privacy Policy, si applicano all'utilizzo della piattaforma. Le modalità con cui sono accettate sono descritte nella Sezione 16.

La piattaforma può essere utilizzata sia da utenti professionali, che agiscono per scopi relativi alla propria attività imprenditoriale, commerciale, artigianale o professionale, sia da consumatori, intesi come persone fisiche che agiscono per scopi estranei a tali attività. Quando le presenti condizioni prevedono regole specifiche per i consumatori, tali regole si applicano agli utenti consumatori. Nessuna disposizione delle presenti condizioni limita i diritti che i consumatori hanno in base alle norme inderogabili a tutela dei consumatori, incluso il Codice del consumo (D.Lgs. 206/2005) e, per i consumatori residenti in un altro Paese, le disposizioni inderogabili della legge di tale Paese. Servizi specificamente destinati all'uso domestico o personale, se offerti in futuro, potranno essere soggetti a condizioni integrative. Per utilizzare la piattaforma occorre avere almeno 18 anni.

## 2. Disponibilità del servizio

EVIDE è fornito nello stato in cui si trova. Ci impegniamo a garantire la massima disponibilità ma non garantiamo un servizio privo di interruzioni. Interruzioni temporanee possono verificarsi per manutenzione, problemi tecnici o circostanze fuori dal nostro controllo. Le interruzioni del servizio non invalidano i record probatori già creati: gli hash di intake restano verificabili con strumenti SHA-256 standard, applicati al materiale originale o, per gli intake strutturati, alla sua forma canonica come documentata da EVIDE, e il timestamp UTC resta il riferimento registrato da EVIDE al momento del deposito. Per i consumatori, la presente sezione non pregiudica la garanzia legale di conformità dei contenuti digitali e dei servizi digitali prevista dal Codice del consumo.

## 3. Forza maggiore e dipendenze da terzi

EVIDE dipende da infrastrutture di terze parti tra cui provider di hosting, autorità SSL, servizi di consegna email e, per il solo servizio FEDIS, prestatori di servizi fiduciari qualificati per la firma e la marca temporale. Il deposito base EVIDE non utilizza marche temporali qualificate: il suo timestamp UTC è generato dal server EVIDE. Non possiamo essere ritenuti responsabili per degradazioni del servizio causate da manutenzione, aggiornamenti o guasti di tali provider. In questi casi il servizio sarà ripristinato nel minor tempo tecnicamente possibile, salvo diversa previsione di legge inderogabile.

## 4. Limiti di volume e compatibilità infrastrutturale

EVIDE è una piattaforma su infrastruttura condivisa progettata per utilizzo professionale ai volumi indicati per ciascun piano. Gli utenti che necessitano di più di 500 intake/mese devono contattarci prima di attivare tali volumi per concordare una soluzione su infrastruttura dedicata. I piani standard non sono progettati per garantire SLA di livello enterprise a volumi elevati o con throughput continuo. Le degradazioni di performance causate da volumi superiori alla soglia del piano non costituiscono inadempimento contrattuale. Ci riserviamo il diritto di sospendere account che generano un carico sproporzionato senza accordo preventivo, con preavviso di 24 ore e rimborso proporzionale del periodo non goduto, salvo diversa previsione di legge inderogabile. I contenuti inviati alla piattaforma, compresi i contenuti strutturati dei depositi via API, sono soggetti a una

dimensione massima stabilita da Informatica in Azienda e indicata nella documentazione tecnica; i contenuti oltre il limite sono rifiutati, mai troncati.

## 5. Modifiche ai prezzi

Ci riserviamo il diritto di modificare i prezzi del servizio in qualsiasi momento. Le variazioni di prezzo saranno comunicate con almeno 30 giorni di preavviso via email all'indirizzo di registrazione. Gli utenti con piani a pagamento attivi mantengono il prezzo corrente fino alla scadenza del periodo pagato. Il rinnovo successivo alla data di entrata in vigore dei nuovi prezzi avverrà alle nuove tariffe. Il proseguimento nell'utilizzo del servizio dopo la data di entrata in vigore costituisce accettazione dei nuovi prezzi. I consumatori ricevono la comunicazione delle variazioni di prezzo con le stesse modalità e possono recedere dal contratto, senza penali, prima dell'entrata in vigore dei nuovi prezzi.

## 6. Modifiche al servizio

Ci riserviamo il diritto di modificare, migliorare o dismettere funzionalità della piattaforma con 30 giorni di preavviso. In caso di dismissione della piattaforma, gli hash di intake già calcolati restano verificabili in modo indipendente con strumenti standard di verifica SHA-256, a condizione che il titolare conservi il materiale originale (o, per gli intake strutturati, la sua forma canonica) e l'hash di riferimento. Il timestamp UTC resta il riferimento registrato da EVIDE al momento del deposito: non si verifica con strumenti di hash. Se una modifica incide negativamente, in modo non trascurabile, sull'accesso di un consumatore a un servizio digitale a pagamento o sul suo utilizzo, il consumatore ne è informato in anticipo e può recedere dal contratto gratuitamente, come previsto dal Codice del consumo.

## 7. Contenuti dell'utente: responsabilità, titolarità e riservatezza

**7.1 Responsabilità.** L'utente è il solo responsabile dei contenuti depositati. È vietato utilizzare la piattaforma per depositare contenuti illegali, fraudolenti o che violino diritti di terzi. EVIDE non modera i contenuti depositati ma si riserva il diritto di disattivare account in caso di violazioni documentate, come descritto nella Sezione 13.5. L'utente è responsabile di disporre di una base giuridica per qualsiasi dato personale di terzi incluso nei contenuti depositati.

**7.2 Titolarità.** Il deposito di un contenuto non ne trasferisce la titolarità a Informatica in Azienda. I materiali inviati dall'utente (contenuti caricati, payload, dichiarazioni e altri input) restano di proprietà dell'utente o dei relativi titolari dei diritti. L'utente concede a Informatica in Azienda solo i diritti necessari a fornire il servizio, cioè conservare, sottoporre a hash, trattare e riprodurre tali materiali nei record della piattaforma, nei documenti FEDIS e, se l'utente ne ha chiesto la pubblicazione, nel registro pubblico. La piattaforma EVIDE, il suo software, gli schemi, le API e la documentazione, nonché i formati dei record che genera (come versioni EAR, profili evidenziari e documenti FEDIS) appartengono a Informatica in Azienda; ciò non attribuisce a Informatica in Azienda alcun diritto sui contenuti dell'utente presenti in tali record, e l'utente può utilizzare per i propri scopi i record e i documenti FEDIS relativi ai propri depositi.

**7.3 Nessuna vendita dei dati.** Informatica in Azienda non vende, non scambia, non cede in locazione e non concede in licenza i contenuti dei depositi (contenuti caricati, payload di intake, dichiarazioni e contenuti dei record EAR ed ESB) a terzi per le finalità proprie di tali terzi. I contenuti dei depositi sono utilizzati solo per fornire e documentare il servizio richiesto dall'utente, per adempiere a obblighi di legge e per proteggere la sicurezza della piattaforma; non sono riutilizzati per pubblicità, altre finalità commerciali, ricerche estranee al servizio o finalità di terzi senza un'adeguata base giuridica e l'autorizzazione dell'utente. Informatica in Azienda può utilizzare statistiche aggregate che non contengono né contenuti dei depositi né dati personali, come il numero di intake elaborati. Questo impegno non impedisce il trattamento da parte dei fornitori tecnici di cui

Informatica in Azienda si avvale per fornire il servizio, come i fornitori di hosting e i prestatori di servizi fiduciari qualificati, come descritto nella Privacy Policy, né le comunicazioni imposte dalla legge o da un ordine di un'autorità competente.

**7.4 Intelligenza artificiale.** Informatica in Azienda non utilizza i contenuti dei depositi per addestrare, perfezionare o valutare modelli di intelligenza artificiale propri o di terzi. La piattaforma non trasmette i contenuti dei depositi a servizi di intelligenza artificiale esterni. Informatica in Azienda non fornisce i contenuti dei depositi a servizi di intelligenza artificiale esterni che utilizza manualmente, ad esempio a supporto dello sviluppo o della manutenzione della piattaforma, salvo che i contenuti siano stati anonimizzati o che l'utente lo abbia autorizzato per iscritto per una finalità specifica, con accordi che impediscano al fornitore di utilizzarli per proprie finalità. Le integrazioni gestite dall'utente, come agenti di intelligenza artificiale o client MCP che inviano dati a EVIDE, restano sotto il controllo dell'utente.

**7.5 Riservatezza.** Informatica in Azienda tratta i contenuti dei depositi come riservati e ne limita l'accesso alle persone che ne hanno bisogno per fornire il servizio, come il certificatore quando è richiesto un FEDIS. I contenuti dei depositi non sono mai pubblicati: il registro pubblico mostra soltanto le informazioni descritte nella Sezione 13.9.

**7.6 Organizzazioni ed ex membri.** L'utente che appartiene a un'organizzazione sulla piattaforma può depositare intake per quell'organizzazione. Gli intake depositati per un'organizzazione sono record di quell'organizzazione: sono accessibili ai suoi membri attuali e sono fatturati all'organizzazione. Qualsiasi nuova operazione su un intake dell'organizzazione, come la richiesta di un FEDIS, l'accettazione o il rifiuto di un preventivo, l'invio di messaggi, l'aggiunta di intake collegati a una catena evidenziaria, la chiusura di una catena evidenziaria o l'avvio di una catena di integrazione a partire da essa, l'aggiornamento o la chiusura di un ESB o l'uso di una chiave API emessa per l'organizzazione, richiede l'appartenenza attuale all'organizzazione nel momento dell'operazione, oltre alle altre condizioni che si applicano a quell'operazione. Quando un utente cessa di essere membro, il suo potere di agire per l'organizzazione cessa immediatamente; le chiavi API emesse per l'organizzazione a nome di quell'utente smettono di operare per l'organizzazione, senza essere revocate, finché l'utente non viene reinserito o la chiave non viene riassegnata. L'ex membro conserva l'accesso in sola lettura agli intake che ha depositato personalmente per l'organizzazione, limitato all'intake stesso, alle sue versioni EAR, alle evidenze ancora conservate sulla piattaforma e allo stato corrente della richiesta. L'ex membro non vede i messaggi, la cronologia degli stati, i preventivi, i prezzi o altri dettagli economici della richiesta, né gli altri intake della catena evidenziaria dell'organizzazione, e non può compiere alcuna operazione su quegli intake. Gli ex membri che non hanno effettuato un deposito non vi hanno accesso. Depositando intake tramite i propri membri, l'organizzazione prende atto che il membro che ha effettuato un deposito conserva questo accesso limitato dopo la sua uscita. L'organizzazione che necessita di una disciplina diversa per determinati intake deve contattare Informatica in Azienda prima di depositarli, oppure può chiederne la cancellazione ai sensi della Sezione 13.7.

**7.7 Linked Responses.** Quando la funzione Linked Responses è disponibile sulla piattaforma, l'utente che ha depositato un intake può invitare una persona indicata nominativamente, identificata da numero DAPI, nome e cognome, a dichiarare la propria posizione su una rappresentazione di quell'intake. Per un intake di un'organizzazione, chi ha depositato deve esserne membro attuale (Sezione 7.6). Creando l'invito, chi ha depositato dichiara di essere autorizzato a condividere il contenuto con il destinatario e che la condivisione è consentita dalle regole applicabili e, per un intake di organizzazione, dalle autorizzazioni dell'organizzazione; queste restano dichiarazioni di chi ha depositato e non sono verificate da EVIDE. L'invito è personale: può essere usato solo tramite l'account EVIDE il cui numero DAPI, nome e cognome corrispondono a quelli indicati, e scade 30 giorni dopo la creazione.

Il destinatario non riceve il record: riceve una rappresentazione FAST REVIEW generata dalla piattaforma dal record indicato da chi ha depositato, secondo il modello applicabile, e congelata con il suo identificativo e la sua impronta. In questa versione le frasi fisse della rappresentazione sono in italiano; le parti evidenziate tra virgolette riportano testi presenti nel record così come vi sono stati inseriti tramite l'account di chi ha depositato, e la rappresentazione non stabilisce chi ne sia l'autore originario. Il destinatario non riceve il record completo né i documenti esterni che il record cita. Può dichiarare su quella rappresentazione una di quattro posizioni (concordo, prendo atto senza esprimere accordo, contesto, non sono in condizione di valutare), aggiungendo una motivazione, obbligatoria per contestare, e una riserva; un riscontro successivo può sostituire o integrare il precedente, che resta conservato. Ogni riscontro è un record del destinatario ed è documentato in un record EAR-LINKED; chi ha depositato non può modificarlo né cancellarlo. EVIDE registra le richieste di apertura del link ricevute dal proprio server e le dichiarazioni rese dal destinatario; queste non provano che una pagina sia stata mostrata, letta o compresa, e la dichiarazione di presa visione di un'informativa non è un consenso.

Il riscontro è visibile al destinatario, a chi ha depositato finché ha accesso al record secondo queste condizioni (per un intake di organizzazione, finché ne è membro attuale) e, se chi ha depositato ha scelto questa visibilità, ai membri attuali dell'organizzazione; gli ex membri non lo vedono. Chi ha depositato può revocare direttamente l'invito. Per un intake di organizzazione la revoca segue le regole registrate per l'invito al momento della creazione: queste possono invece prevedere una richiesta di revoca, presentata da chi ha depositato e decisa da un owner o admin attuale dell'organizzazione diverso dal richiedente e da chi ha depositato, oppure da un'autorità di riesame designata dall'organizzazione la cui designazione è stata verificata con esito «confermato»; le richieste urgenti sospendono l'invito fino alla decisione. Informatica in Azienda può sospendere un invito per ragioni di sicurezza. Se chi ha depositato cessa di essere membro dell'organizzazione, gli inviti che ha creato sui suoi intake sono chiusi definitivamente, salvo quelli creati con le regole che li mantengono utilizzabili fino alla scadenza originaria; in questo caso gli owner e admin attuali dell'organizzazione possono sospenderli, riprenderli o revocarli indicando un motivo. Revoche e sospensioni impediscono nuovi riscontri e non modificano né cancellano i riscontri già depositati.

Per l'autorità di riesame EVIDE registra il documento di titolo ricevuto (metadati e riferimento, non il documento stesso), la designazione e la verifica documentata da un verificatore incaricato da Informatica in Azienda, con il metodo, la fonte esaminata e l'esito dichiarato dal verificatore. Né le dichiarazioni di chi ha depositato o dell'organizzazione né la verifica registrata costituiscono un'attestazione di EVIDE sulla validità giuridica del potere di condividere o di decidere. Un riscontro non modifica, non conferma e non verifica il record, non certifica la verità del record né di alcuna dichiarazione e non è valutato da EVIDE; si applicano le Sezioni 8 e 9. I riscontri possono essere documentati in un FEDIS-LINKED alle condizioni della Sezione 7.8. I record di Linked Responses sono conservati come record probatori (Sezione 13.3) e il trattamento dei relativi dati personali è descritto nella Privacy Policy.

**7.8 FEDIS-LINKED.** Quando la funzione FEDIS-LINKED è disponibile sulla piattaforma, chi ha depositato un intake strutturato tramite l'interfaccia web o l'app EVIDE Mobile (Human Structured Intake) può richiedere un FEDIS che documenti, oltre all'intake, i riscontri collegati includibili (FEDIS-LINKED). La richiesta segue la stessa procedura e le stesse condizioni economiche di ogni FEDIS: preventivo del certificatore, accettazione espressa del richiedente, utilizzo degli eventuali pacchetti FEDIS e fatturazione. Il FEDIS-LINKED può essere richiesto solo da chi ha depositato l'intake e, per un intake di un'organizzazione, solo finché ne è membro attuale (Sezione 7.6). Quando un intake ha riscontri includibili, gli altri membri dell'organizzazione non possono richiedere un FEDIS su quell'intake.

Sono includibili soltanto i riscontri che sono stati depositati dopo che al destinatario è stata mostrata l'informativa che descrive il FEDIS-LINKED, in una versione che la piattaforma registra come idonea, e il cui record EAR-LINKED supera il controllo di integrità. La revoca o la sospensione dell'invito successive al deposito non escludono il riscontro; il documento riporta la data dell'eventuale revoca. Se un riscontro o un EAR-LINKED non supera il controllo di integrità, la richiesta non è accolta.

Ogni richiesta dà origine a una pratica tecnica distinta, collocata nello stesso ambito dell'intake (personale o dell'organizzazione), e a un'istantanea dei record pertinenti. L'istantanea è formata dalla piattaforma dal proprio archivio al momento della richiesta ed è identificata dalla sua impronta SHA-256. Per ogni riscontro incluso il FEDIS-LINKED riporta: nome e numero DAPI di chi ha risposto, l'eventuale ruolo dichiarato, le posizioni, le motivazioni e le riserve, la data di deposito, la visibilità indicata nell'invito, gli identificativi e le impronte del riscontro e del relativo EAR-LINKED. Riporta inoltre conteggi descrittivi degli inviti e dei riscontri. Dei riscontri non includibili e degli inviti senza deposito riporta solo conteggi, senza nomi né contenuti. Alla generazione del documento la piattaforma ricalcola le impronte dei record riportati ancora disponibili e le confronta con quelle registrate; in caso di discrepanza il documento non è generato, e i record non più disponibili sono indicati come non riverificati. Le richieste successive formano una serie: ogni FEDIS-LINKED è un documento autonomo, collegato ai precedenti, che non li modifica né li sostituisce. Una nuova richiesta è possibile solo dopo la conclusione della richiesta FEDIS precedente sullo stesso intake e solo se ci sono riscontri includibili non ancora documentati in un FEDIS-LINKED emesso.

Il FEDIS-LINKED è consegnato a chi lo ha richiesto, che può utilizzarlo e consegnarlo a terzi indipendentemente dalla visibilità del riscontro sulla piattaforma. Chi riceve il FEDIS-LINKED è responsabile, nei limiti previsti dalla legge, degli usi che ne fa e delle comunicazioni a terzi dei dati personali in esso contenuti, che devono avvenire nel rispetto della normativa applicabile e per finalità legittime. Il documento non è reso disponibile tramite la piattaforma agli altri membri dell'organizzazione e la pratica tecnica non è pubblicata nel registro pubblico. Quando un FEDIS-LINKED è rilasciato, chi ha depositato un riscontro incluso riceve una comunicazione essenziale all'indirizzo del proprio account, senza dati di altri riscontri.

Quando chi ha risposto si oppone al trattamento dei propri dati nei FEDIS-LINKED, Informatica in Azienda può sospendere, durante la valutazione, le nuove richieste e i rilasci che includerebbero quel riscontro. La sospensione non modifica né cancella alcun record e non riguarda i documenti già rilasciati.

Il FEDIS-LINKED documenta l'esistenza, l'integrità e il contenuto dei record alla data dell'istantanea. Non certifica la verità dell'intake o dei riscontri, l'esistenza di un accordo o di un consenso tra i partecipanti, né i ruoli o i poteri dichiarati; i conteggi sono conteggi di dichiarazioni individuali e non un voto. Si applicano le Sezioni 8, 9 e 13.8.

**7.9 Chiusura di una catena evidenziaria.** Una catena di intake collegati che contiene almeno due intake può essere chiusa in modo esplicito sulla piattaforma web: una catena personale dal suo titolare; una catena di un'organizzazione da chi ha depositato il primo intake finché è ancora membro, oppure da un owner o da un amministratore attuale dell'organizzazione. Informatica in Azienda non chiude né riapre catene per conto degli utenti, e una catena non può essere chiusa tramite chiavi API o MCP. La chiusura congela un manifest della catena, che elenca gli intake inclusi e le impronte SHA-256 delle loro versioni EAR, dei file depositati e, per gli intake strutturati, dei record canonici di intake, e registra chi ha chiuso la catena, in quale veste e quando; quell'ora è registrata dal database di EVIDE e non è una marca temporale qualificata. Una catena chiusa non viene mai riaperta. La piattaforma rifiuta i nuovi depositi collegati a una catena chiusa, dal web, dall'app e dall'API; il materiale aggiunto in seguito può essere depositato in una nuova catena di integrazione, che fa riferimento alla catena chiusa senza farne parte. La chiusura delimita gli intake inclusi: non attesta che ogni

evento rilevante sia stato depositato, che le dichiarazioni siano vere o che non esistano depositi non collegati. Non estende la conservazione dei contenuti caricati (Sezione 13.2): il pacchetto di una catena chiusa comprende solo i file che chi lo richiede può ancora scaricare, quindi un pacchetto ottenuto più tardi può essere incompleto rispetto al manifest. Sul manifest di una catena chiusa può essere richiesto un FEDIS secondo la procedura ordinaria del FEDIS; il suo rifiuto o il suo annullamento non incidono sulla chiusura. Dopo l'emissione, l'amministrazione può caricare il documento FEDIS firmato sul manifest. La piattaforma lo conserva con la sua impronta SHA-256, calcolata sul file salvato; un caricamento successivo è registrato come nuova versione, e le versioni precedenti sono conservate e segnate come sostituite. La versione corrente è inclusa nei pacchetti della catena generati successivamente, per gli utenti con accesso completo alla pratica tecnica di quel FEDIS; le versioni sostituite sono soltanto elencate. Il caricamento del documento e il rilevamento in esso di una struttura di firma non costituiscono una validazione crittografica della firma, della marca temporale o del certificato. Il documento firmato non è un file depositato di un intake e non è rimosso dalla conservazione automatica dei contenuti caricati (Sezione 13.2); la sua conservazione è disciplinata dalla Sezione 13.3. Le cancellazioni successive alla chiusura sono disciplinate dalla Sezione 13.7.

## 8. Valore Evidenziario e Responsabilità Giurisdizionale

EVIDE produce record probatori indipendentemente verificabili, ancorati a un hash SHA-256 calcolato all'intake, a un timestamp UTC generato lato server e a un riferimento di identità collegato all'account dell'utente verificato tramite DAPI. Ruoli, poteri e altre affermazioni contenute in un deposito restano dichiarazioni del depositante, salvo che la descrizione del servizio indichi che sono verificati in modo indipendente. Il timestamp del deposito base è generato dal server EVIDE e non è una marca temporale qualificata. FEDIS è un documento distinto, generato dalla piattaforma e sottoscritto dal certificatore, che, secondo l'attuale procedura di certificazione, riporta le impronte SHA-256 del record di intake e di una specifica versione EAR (vedi Sezione 13.8) e aggiunge una firma elettronica qualificata e una marca temporale elettronica qualificata (art. 41 eIDAS) rilasciata da un prestatore di servizi fiduciari qualificato terzo; la marca attesta il momento in cui è apposta al documento FEDIS e non rende qualificato il timestamp del deposito base. Combinati con la certificazione forense FEDIS, questi record sono predisposti con riferimento agli standard internazionali ISO/IEC 27037:2012, al regolamento eIDAS (UE 910/2014) e alle Federal Rules of Evidence 901-902 (USA), fornendo documentazione forense strutturata utilizzabile in contesti giudiziari, regolatori e investigativi nell'UE, negli Stati Uniti, nel Regno Unito, in Canada, in Australia e nelle giurisdizioni equivalenti.

La distinzione essenziale: EVIDE e FEDIS operano come un **layer di cristallizzazione probatoria** -- non come garanzia di ammissibilità automatica. Non sostituiscono la valutazione dell'autorità competente, le regole procedurali della giurisdizione o il ruolo del tribunale. La loro funzione è ridurre l'incertezza documentando le condizioni tecniche che supportano l'affidabilità probatoria, rendendo la verifica dell'integrità oggettiva e indipendente dalla fiducia nella piattaforma certificante.

L'ammissibilità, il peso legale o l'accettazione procedurale dei record probatori possono variare in base alla giurisdizione, al tribunale o all'autorità di regolamentazione. L'utente è responsabile della valutazione del contesto legale del proprio procedimento, prima di aderire al servizio, e dell'ottenimento di consulenza legale indipendente ove necessario. **Scopri la certificazione forense FEDIS →**

## 9. Nessuna garanzia sui dati dichiarati dall'utente

EVIDE verifica l'integrità strutturale, l'attribuzione dell'identità e la tempistica di intake dei record depositati. Non verifica in modo indipendente l'accuratezza fattuale, l'autenticità, la completezza o la veridicità dei contenuti, delle dichiarazioni, dei metadati o di qualsiasi campo dichiarato dall'utente, salvo diversamente indicato nella descrizione del servizio. Il valore probatorio di un record EVIDE deriva dalle sue proprietà di ancoraggio e integrità, non da alcuna garanzia sull'accuratezza del contenuto dichiarato.

## 10. Riferimento temporale UTC

Tutti i timestamp generati da EVIDE sono espressi in Coordinated Universal Time (UTC) e rappresentano il tempo di intake generato autonomamente dalla piattaforma nel momento dell'elaborazione del deposito. I timestamp EVIDE sono generati lato server e sono indipendenti dall'orologio locale dell'utente, dal fuso orario del dispositivo o da riferimenti temporali lato client. Non rappresentano il momento di creazione, firma o trasmissione del contenuto da parte dell'utente. Le discrepanze tra i timestamp lato utente e i timestamp di intake EVIDE non costituiscono un errore della piattaforma.

## 11. Sicurezza dell'account e responsabilità delle API key

Gli utenti sono responsabili del mantenimento della riservatezza delle API key, delle credenziali, dei token di accesso e dei codici DAPI associati al proprio account. Le azioni eseguite tramite credenziali autenticate -- incluse le chiamate API, i depositi mediati da MCP e gli intake avviati da agenti AI -- sono considerate attribuibili al titolare dell'account, salvo prova contraria ai sensi della legge applicabile. In caso di sospetto di compromissione delle credenziali, l'utente deve notificarcelo immediatamente a info@informaticainazienda.it. Informatica in Azienda non può essere ritenuta responsabile per depositi, record o azioni eseguiti tramite credenziali che l'utente ha omesso di proteggere. Quando un account è disattivato, le credenziali associate sono sospese come descritto nella Sezione 13.5. Informatica in Azienda può inoltre revocare singole credenziali, ad esempio in caso di sospetta compromissione; le credenziali revocate non tornano valide.

## 12. Controlli all'esportazione e uso vietato

La piattaforma non può essere utilizzata in violazione dei controlli all'esportazione applicabili, delle normative sulle sanzioni o delle leggi che disciplinano le prove digitali e le tecnologie soggette a restrizioni. L'utilizzo di EVIDE è vietato laddove tale utilizzo violerebbe le leggi della giurisdizione dell'utente o le normative internazionali applicabili. Informatica in Azienda si riserva il diritto di limitare l'accesso a utenti o organizzazioni soggetti a sanzioni applicabili o che operano in giurisdizioni in cui il servizio non può essere fornito legalmente.

## 13. Record, conservazione, stato dell'account e richieste di cancellazione

**13.1 Categorie di record.** Nell'erogazione del servizio, EVIDE tratta diverse categorie di record, soggette a regole diverse: (a) dati dell'account, come nome, indirizzo email, numero DAPI e organizzazione; (b) record canonici di intake, inclusi l'hash di intake, il timestamp UTC generato dal server, l'evide_id, il payload inviato e il profilo evidenziario calcolato dalla piattaforma; (c) versioni dell'Evidentiary Artifact Record (EAR) e i relativi hash; (d) osservazioni, dichiarazioni e record di chiusura dell'Epistemic Stabilization Buffer (ESB); (e) contenuti caricati dall'utente; (f) documenti FEDIS e i record a cui fanno riferimento; (g) voci del registro pubblico EVIDE; (h) log operativi, di sicurezza e di accesso e dati di fatturazione; (i) i record di Linked Responses, come inviti, dichiarazioni, rappresentazioni FAST REVIEW, riscontri, record EAR-LINKED, richieste di revoca, sospensioni, revoche e decisioni e dati dell'autorità di riesame, le istantanee, le pratiche tecniche, le notifiche e le sospensioni relative ai FEDIS-LINKED, e il registro delle modifiche delle appartenenze alle organizzazioni e dello stato di account, identità DAPI su EVIDE e organizzazioni; (j) i record tecnici delle richieste API inviate con una chiave di idempotenza (Sezione 13.11); (k) i record della chiusura di una catena, come il manifest congelato di una catena chiusa e la sua impronta SHA-256, l'identificativo, il numero DAPI e la veste di chi l'ha chiusa, gli eventi registrati dopo la chiusura, i riferimenti delle catene di integrazione e i record di un FEDIS richiesto sul manifest e il suo documento firmato (Sezione 7.9). Alcuni di questi record possono contenere dati personali dell'utente o di terzi. Un record non è escluso dall'applicazione della normativa sulla protezione dei dati per il solo fatto di essere un hash, un identificativo o un record tecnico.

**13.2 Contenuti caricati.** Per gli intake inviati con contenuti caricati (file, archivi ZIP, oppure un URL o un testo che la piattaforma memorizza come file), il contenuto caricato è conservato sui server della piattaforma per un

periodo limitato e successivamente cancellato, come indicato nella descrizione del servizio. Finché è conservato, l'utente può scaricarlo dal proprio account. Quando per uno di tali intake viene emesso un FEDIS, il relativo contenuto caricato è cancellato dalla memoria della piattaforma al momento dell'emissione; l'utente deve quindi conservarne una copia indipendente, o scaricarlo, prima dell'emissione. Gli intake strutturati non includono contenuti caricati: i dati inviati con essi fanno parte del record canonico di intake e sono disciplinati dalla Sezione 13.3. La cancellazione del contenuto caricato non comporta la cancellazione del record canonico di intake, incluso l'hash di intake, né delle versioni EAR, dei record ESB o dei relativi metadati, come il nome, la dimensione e l'hash del file caricato. L'utente è il solo responsabile della conservazione di una copia indipendente di qualsiasi contenuto depositato.

**13.3 Conservazione dei record probatori.** I record canonici di intake, le versioni EAR, i record ESB e i relativi metadati di integrità non vengono cancellati automaticamente quando viene cancellato il contenuto caricato, alla scadenza di un piano, alla disattivazione dell'account o alla cessazione del contratto. Sono conservati per il tempo necessario a documentare il deposito e a consentirne la successiva verifica, in conformità ai criteri di conservazione indicati nella Privacy Policy e alla normativa applicabile, salvo che siano cancellati prima mediante una cancellazione autorizzata ai sensi della Sezione 13.7. EVIDE non garantisce che alcun record resti disponibile a tempo indeterminato. I record della chiusura di una catena sono conservati finché resta sulla piattaforma almeno un intake incluso nella catena chiusa o una richiesta di FEDIS sul suo manifest; quando l'ultimo di questi viene cancellato, i record della chiusura vengono cancellati con esso. I documenti firmati di un FEDIS sul manifest, comprese le versioni sostituite, sono conservati con i record della chiusura: la piattaforma non offre una funzione ordinaria per cancellarli e, finché esistono, la pratica tecnica di quel FEDIS e i record della chiusura non vengono cancellati. Un'eventuale cancellazione, per esempio quando è richiesta dalla legge, è decisa separatamente; ciò non costituisce una garanzia di conservazione a tempo indeterminato.

**13.4 Versioni e integrità.** Nel funzionamento ordinario della piattaforma, una versione EAR, una volta generata, non viene modificata: quando lo stato evidenziario canonico cambia, viene aggiunta una nuova versione, e ogni versione ha un hash SHA-256 registrato. Ricalcolare l'hash SHA-256 di una copia e confrontarlo con un hash di riferimento indica se quella copia è coerente con il riferimento. Il confronto non prova, di per sé, che sia il record conservato sia l'hash di riferimento siano rimasti invariati; ciò dipende da dove e come l'hash di riferimento è stato conservato, ad esempio in un FEDIS o in una copia conservata dall'utente. La coerenza dell'hash non stabilisce che il contenuto di un record, o qualsiasi dichiarazione in esso contenuta, sia vero. La presente sezione descrive il modo in cui la piattaforma tratta i record; non costituisce una promessa che i record non possano mai essere rimossi nei casi descritti dalle Sezioni da 13.7 a 13.10.

**13.5 Disattivazione dell'account.** La disattivazione è una misura amministrativa. Informatica in Azienda può disattivare un account, in particolare nei casi descritti dalle Sezioni 4, 7, 11 e 12, su richiesta dell'utente o per motivi di sicurezza. Mentre un account è disattivato, ogni accesso autenticato è sospeso: le sessioni web, i token di accesso mobile e le API key associati all'account sono rifiutati, e non è possibile effettuare nuovi depositi, aggiornamenti o chiusure ESB. La disattivazione non comporta la cancellazione di dati dell'account, record di intake, versioni EAR, record ESB, documenti FEDIS o altri record, e non costituisce né la cessazione del rapporto contrattuale né la cancellazione di dati personali. Se l'account viene riattivato, le credenziali non scadute e non revocate esplicitamente possono essere nuovamente utilizzate.

**13.6 Cessazione, chiusura dell'account e cancellazione definitiva.** L'utente può chiedere la cessazione del contratto, la chiusura dell'account o la cancellazione definitiva dell'account scrivendo a app@certifywebcontent.com o, in alternativa, a info@informaticainazienda.it. Informatica in Azienda può far cessare il servizio nei casi previsti dalle presenti condizioni o dalla legge. La cessazione pone fine all'accesso alla piattaforma e non incide sugli obblighi di pagamento già maturati; di per sé non comporta la cancellazione dei

dati dell'account o dei record, che sono trattati secondo la Sezione 13.3. Quando l'utente chiede la chiusura dell'account, Informatica in Azienda, dopo aver verificato l'identità e i poteri documentati del richiedente, cancella gli intake personali dell'utente che possono essere cancellati ai sensi della Sezione 13.7, insieme ai record dipendenti, revoca definitivamente le sessioni e le chiavi API dell'utente e rimuove le sue appartenenze a organizzazioni. Se nessun record collegato all'account deve essere conservato, l'account e l'abilitazione dell'identità DAPI dell'utente su EVIDE sono cancellati. Se alcuni record collegati all'account devono essere conservati, come gli intake depositati per un'organizzazione, gli intake che non possono essere cancellati ai sensi della Sezione 13.7 o i record da conservare per legge, l'account è mantenuto in stato chiuso, collegato soltanto a quei record: non può essere usato per accedere e non è usato per nessun altro scopo, e l'utente è informato dei record conservati e delle relative ragioni. La chiusura di un account EVIDE non revoca né modifica la certificazione DAPI dell'utente, che è disciplinata dalle proprie condizioni. Un account chiuso non viene mai riaperto automaticamente: l'accesso può essere ripristinato solo su richiesta, dopo la verifica dell'identità del richiedente, e l'utente il cui account è stato cancellato può essere abilitato di nuovo come nuovo account; in entrambi i casi non sono ripristinati i record cancellati, le credenziali revocate e le precedenti appartenenze a organizzazioni. La cancellazione rimuove i dati cancellati dai sistemi attivi della piattaforma; non raggiunge i documenti già consegnati all'utente o a terzi, le copie che non sono sotto il controllo di Informatica in Azienda, i record che devono essere conservati per legge, né le copie di backup fino alla loro sovrascrittura, come descritto nella Privacy Policy. La disattivazione (Sezione 13.5) non è né una chiusura né una cancellazione.

**13.7 Richieste di cancellazione di intake e account.** La piattaforma non offre attualmente agli utenti una funzione self-service per cancellare intake, versioni EAR, record ESB o l'account. Le richieste si presentano per iscritto a app@certifywebcontent.com o, in alternativa, a info@informaticainazienda.it e possono riguardare un intake, più intake, tutti gli intake associati a un account oppure l'account stesso. Una richiesta ricevuta attraverso un altro canale non viene ignorata per questo solo motivo; in nessun caso l'indirizzo da cui una richiesta è inviata costituisce, di per sé, prova sufficiente dell'identità o dei poteri del richiedente. Informatica in Azienda verifica l'identità e i poteri documentati del richiedente e valuta ogni richiesta in conformità alla normativa applicabile, tenendo conto in particolare dell'eventuale emissione di un FEDIS, dell'eventuale riferimento all'intake da parte di altri intake in una catena evidenziaria, dei diritti e degli interessi di terzi e di qualsiasi conservazione imposta dalla legge. L'esistenza di un FEDIS o di versioni EAR non impedisce di per sé la cancellazione; allo stesso modo, non ogni richiesta sarà necessariamente accolta. Quando la cancellazione è autorizzata, il suo ambito può comprendere il record canonico di intake, le versioni EAR, i buffer e gli eventi ESB, le voci del registro pubblico, i record della piattaforma relativi ai FEDIS e altri record tecnici associati. I record sono cancellati in un ordine che preserva l'integrità delle catene evidenziarie: un intake da cui dipendono altri intake di una catena non è cancellato finché quegli intake esistono, e la catena degli intake che restano non viene mai modificata. Quando una cancellazione autorizzata non può essere eseguita per ragioni tecniche, ad esempio perché un FEDIS emesso è collegato a record di pacchetti o di fatturazione che la piattaforma conserva inalterati, la richiesta è valutata separatamente; se la cancellazione è dovuta ma non può essere eseguita in quel momento, il trattamento è limitato. Un vincolo tecnico non costituisce di per sé un motivo legittimo per rifiutare la cancellazione. Gli intake depositati per un'organizzazione sono valutati tenendo conto anche dei diritti dell'organizzazione (Sezione 7.6). Gli intake a cui sono collegati inviti o riscontri di Linked Responses non sono cancellati con la procedura ordinaria: la richiesta è valutata separatamente, tenendo conto anche dei diritti dei destinatari sui propri riscontri e dei record di revoca collegati (Sezione 7.7). Una richiesta di cancellazione di tutti gli intake non è considerata automaticamente una richiesta di chiusura dell'account, e viceversa. Il richiedente è informato della cancellazione effettivamente eseguita e, qualora la richiesta non sia accolta integralmente, delle relative motivazioni. Se la richiesta è formulata ai sensi della normativa sulla protezione dei dati, si applica anche la Sezione 13.10. Se viene cancellato un intake incluso in una catena chiusa, la cancellazione è registrata come evento successivo alla chiusura e il manifest congelato della catena non cambia (Sezione 7.9).

**13.8 Record certificati (FEDIS).** Il FEDIS è un documento distinto, sottoscritto dal certificatore e consegnato all'utente. Un FEDIS emesso secondo l'attuale procedura di certificazione riporta due impronte SHA-256: l'hash di intake (per gli intake con contenuti caricati, l'impronta del contenuto ricevuto; per gli intake strutturati, l'impronta del record canonico di intake) e l'hash della specifica versione EAR vigente al momento dell'emissione del FEDIS. Tale versione EAR resta il riferimento del FEDIS anche se successivamente vengono generate nuove versioni EAR. Un FEDIS-LINKED riporta inoltre l'impronta SHA-256 dell'istantanea dei riscontri collegati e, per ogni riscontro incluso, le impronte del riscontro e del relativo EAR-LINKED, con l'esito delle verifiche eseguite alla sua generazione (Sezione 7.8). Un FEDIS emesso prima che i riferimenti all'EAR fossero introdotti nella procedura di certificazione può non fare riferimento ad alcuna versione EAR. Una cancellazione autorizzata ai sensi della Sezione 13.7 può comprendere i record della piattaforma a cui fa riferimento un FEDIS. La cancellazione di record della piattaforma non modifica né revoca un documento FEDIS già consegnato, e tale documento non può essere rimosso dal possesso dell'utente o dei terzi a cui è stato consegnato; una volta cancellati i relativi record della piattaforma, tuttavia, potrebbe non essere più possibile verificare quel FEDIS rispetto ai record di EVIDE. Le scritture contabili e fiscali relative a un FEDIS, come le fatture, sono distinte dai record probatori e sono conservate come previsto dalla legge.

**13.9 Registro pubblico.** Una voce è pubblicata nel registro pubblico EVIDE solo su richiesta del depositante, formulata al momento dell'invio dell'intake, se il modulo prevede questa opzione, oppure per iscritto, e solo per intake per i quali è stato emesso un FEDIS; la pubblicazione è eseguita dal certificatore. Una voce pubblicata mostra il reference ID, il codice FEDIS, lo stato, l'hash di intake, il timestamp di intake e la data di pubblicazione; il registro può inoltre mostrare altre voci pubblicate con lo stesso hash e, per gli intake che fanno parte di una catena evidenziaria, la posizione della voce nella catena. Le pratiche tecniche dei FEDIS-LINKED e dei FEDIS sul manifest di una catena chiusa non sono pubblicate nel registro pubblico. Le voci pubblicate sono accessibili a chiunque e possono essere indicizzate dai motori di ricerca. L'utente può chiedere in qualsiasi momento la rimozione di una voce scrivendo a app@certifywebcontent.com o, in alternativa, a info@informaticainazienda.it. La rimozione dal registro pubblico elimina soltanto la voce pubblica: non comporta la cancellazione dei record di intake, delle versioni EAR o dei documenti FEDIS sottostanti, e non revoca, invalida o modifica un FEDIS emesso. Informatica in Azienda non può controllare le copie delle voci pubbliche effettuate da terzi, inclusi i motori di ricerca, prima della rimozione.

**13.10 Diritti in materia di protezione dei dati.** Nessuna disposizione delle presenti condizioni limita i diritti che gli interessati hanno ai sensi del Regolamento (UE) 2016/679 (GDPR) o di altre norme inderogabili, inclusi i diritti di accesso, rettifica, cancellazione, limitazione e opposizione. Le richieste di esercizio di tali diritti sono gestite come descritto nella Privacy Policy ed entro i termini previsti dalla legge. Quando è richiesta la cancellazione di dati personali, Informatica in Azienda valuterà se nel caso specifico si applichi una delle eccezioni previste dall'articolo 17, paragrafo 3, del GDPR, ad esempio quando la conservazione è necessaria per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria. Tali eccezioni sono applicate solo nella misura necessaria nel caso specifico; quando si applicano, il trattamento può essere limitato anziché i dati essere cancellati. La disattivazione amministrativa (Sezione 13.5) e la cessazione (Sezione 13.6) sono distinte dalla cancellazione e non sostituiscono la valutazione di una richiesta di cancellazione. L'utente è responsabile di disporre di una base giuridica per qualsiasi dato personale di terzi incluso nei contenuti e nelle dichiarazioni depositati.

**13.11 Richieste API ripetute (chiavi di idempotenza).** Per le richieste API per le quali la documentazione tecnica lo prevede, il sistema dell'utente può inviare una chiave di idempotenza da esso scelta. L'uso della chiave è facoltativo: senza di essa ogni richiesta è trattata come una richiesta nuova. Per 7 giorni dalla prima richiesta inviata con una determinata chiave, una richiesta ripetuta con la stessa chiave, tramite la stessa API key, allo stesso endpoint e con lo stesso contenuto non viene eseguita una seconda volta: la piattaforma restituisce l'esito già registrato per quella chiave oppure, se la prima richiesta è ancora in corso o si è interrotta, la tratta in

modo che produca effetto una sola volta. Una richiesta ripetuta con la stessa chiave ma con contenuto diverso, o verso un endpoint diverso, viene rifiutata. Trascorsi 7 giorni la chiave non è più riconosciuta e una richiesta inviata con essa è trattata come nuova, e può quindi creare un nuovo deposito. L'utente è responsabile della generazione delle chiavi, dell'uso di una chiave diversa per ogni richiesta distinta e di non inserirvi dati personali o informazioni riservate. Quando un intake è cancellato ai sensi della Sezione 13.7, l'esito registrato per le chiavi che vi si riferiscono è sostituito da un avviso che il record non esiste più, privo di qualsiasi dato del record; fino al termine dei 7 giorni, una richiesta ripetuta con una di tali chiavi riceve quell'avviso e non crea un nuovo deposito. Questo meccanismo riduce i duplicati che possono derivare dalla ripetizione della stessa richiesta, nei limiti descritti; non garantisce che sulla piattaforma non esista mai più di un deposito relativo allo stesso evento, ad esempio quando lo stesso evento è inviato con chiavi diverse, con contenuto diverso, senza chiave o dopo i 7 giorni, e non stabilisce se due depositi si riferiscano allo stesso evento. Una richiesta ripetuta che restituisce l'esito già registrato non crea un deposito e non è conteggiata come intake aggiuntivo; un deposito completato tramite una richiesta ripetuta è conteggiato una sola volta, al momento del completamento. Le richieste ripetute restano soggette ad autenticazione, autorizzazione e ai limiti di frequenza delle richieste previsti dal piano. I record tecnici usati a questo scopo non fanno parte del record probatorio e sono descritti nella Privacy Policy.

## 14. Limitazione di responsabilità

Informatica in Azienda non può essere ritenuta responsabile per: danni indiretti o consequenziali; perdita di dati causata da azioni dell'utente; interpretazioni errate dei record probatori da parte di terzi; decisioni assunte sulla base di record EVIDE da parte di tribunali, autorità di regolamentazione o altre parti; mancata ammissione dei record probatori in qualsiasi procedimento legale o amministrativo. Nessuna disposizione della presente sezione esclude o limita la responsabilità per dolo o colpa grave, né alcuna responsabilità che non possa essere esclusa o limitata ai sensi della legge applicabile. Per i consumatori, le limitazioni di responsabilità previste dalla presente sezione e dalle Sezioni 2, 3, 4 e 9 si applicano solo nei limiti consentiti dal Codice del consumo e non pregiudicano i diritti riconosciuti al consumatore dalla legge, inclusa la garanzia legale di conformità.

## 15. Legge applicabile e foro competente

Le presenti condizioni sono regolate dalla legge italiana. Per qualsiasi controversia con utenti professionali è competente in via esclusiva il Foro di Bologna, Italia, salvo diversa previsione di legge inderogabile. Per le controversie con i consumatori è competente il giudice del luogo di residenza o di domicilio del consumatore, se ubicati in Italia. I consumatori residenti in un altro Paese conservano la tutela loro garantita dalle disposizioni inderogabili della legge di tale Paese e dalle norme applicabili in materia di competenza giurisdizionale.

## 16. Accettazione, modifiche e diritto di recesso

**16.1 Accettazione.** Le presenti condizioni si applicano dal primo utilizzo della piattaforma. Per i piani API, sono accettate espressamente al momento dell'attivazione del servizio API, e la versione accettata viene registrata. Gli altri servizi a pagamento sono forniti sulla base di una richiesta o di un ordine scritto, ad esempio via email, che indica il servizio e il relativo prezzo. Per i consumatori, un contratto per un servizio a pagamento si conclude solo con l'accettazione espressa del consumatore; prima della conclusione, Informatica in Azienda fornisce le informazioni previste dal Codice del consumo e, dopo la conclusione, invia la conferma del contratto su un supporto durevole.

**16.2 Modifiche.** Informatica in Azienda può aggiornare le presenti condizioni dandone almeno 30 giorni di preavviso via email all'indirizzo registrato; la comunicazione indica la nuova versione e la data da cui si applica. Ove richiesto dalla legge o dalla natura della modifica, Informatica in Azienda richiederà una nuova accettazione. Il consumatore che non accetta una modifica può recedere dal contratto gratuitamente prima che

la modifica abbia effetto. Le versioni precedenti delle presenti condizioni restano disponibili su richiesta. Ogni versione delle presenti condizioni, insieme alla Privacy Policy in vigore dalla stessa data, è pubblicata anche come documento PDF con firma elettronica qualificata, scaricabile dalla pagina delle presenti condizioni con la relativa impronta SHA-256; una volta pubblicata, una copia firmata non viene mai sostituita. La copia firmata documenta il contenuto e la data della versione; l'accettazione è registrata come descritto nella Sezione 16.1. Una nuova versione si applica dalla sua data di efficacia e non modifica gli atti già compiuti sotto una versione precedente, come i depositi effettuati, i documenti FEDIS emessi o le accettazioni registrate; le accettazioni registrate delle versioni precedenti restano invariate. Per gli utenti già registrati alla data di pubblicazione, una nuova versione si applica dalla data di efficacia indicata nell'avviso. Un contratto concluso dopo la pubblicazione di una nuova versione può richiamarla espressamente: in questo caso quella versione si applica a quel contratto dalla sua conclusione. Una funzione descritta in una nuova versione è utilizzabile solo da quando è disponibile sulla piattaforma.

**16.3 Diritto di recesso (consumatori).** Il consumatore che conclude a distanza un contratto per un servizio a pagamento può recedere entro 14 giorni dalla sua conclusione, senza dover fornire alcuna motivazione, inviando una dichiarazione esplicita a info@informaticainazienda.it; può essere utilizzato il modulo tipo di recesso previsto dal Codice del consumo, ma non è obbligatorio. Se il consumatore ha chiesto espressamente che il servizio inizi durante il periodo di recesso e poi recede, è tenuto a pagare un importo proporzionale al servizio fornito fino alla comunicazione del recesso. Il diritto di recesso si perde solo se il servizio è stato interamente prestato e l'esecuzione è iniziata con l'accordo espresso del consumatore e con la sua accettazione del fatto che avrebbe perso il diritto di recesso a seguito della piena esecuzione del contratto. Le somme dovute al consumatore sono rimborsate entro 14 giorni dal ricevimento del recesso, utilizzando lo stesso mezzo di pagamento salvo diverso accordo.

**16.4 Approvazione specifica e clausole vessatorie.** Le clausole che, ai sensi della legge applicabile, richiedono una specifica approvazione sono efficaci solo se approvate nella forma prevista dalla legge. Le clausole vessatorie ai sensi del Codice del consumo non vincolano i consumatori.

PARTE B: ITALIANO

# Privacy Policy & Cookie Policy

Versione 2026-16 - in vigore dal 24 novembre 2026 · https://app.certifywebcontent.com/privacy

Informativa sul trattamento dei dati personali ai sensi del Regolamento (UE) 2016/679 (GDPR) per la piattaforma EVIDE su app.certifywebcontent.com, l'API EVIDE e l'app EVIDE Mobile.

## 1. Titolare del trattamento

Il titolare del trattamento è **Informatica in Azienda**, nella persona del Dott. Emanuel Celano, con sede legale in Via Vaccaro 5, 40132 Bologna (Italia), P.IVA IT02137271207.

Email: info@informaticainazienda.it - Telefono: +393771151946

## 2. Ambito della presente informativa

La presente informativa si applica alla piattaforma EVIDE su app.certifywebcontent.com, all'API EVIDE, all'app EVIDE Mobile e al registro pubblico EVIDE. Riguarda gli utenti della piattaforma, le altre persone i cui dati personali sono contenuti nei contenuti depositati e le persone i cui dati sono registrati per la funzione Linked Responses (ad esempio le persone designate a decidere sulle revoche, i verificatori e i titolari dei recapiti dell'organizzazione). L'EVIDE Governance Lab (lab.certifywebcontent.com) ha una propria informativa privacy. Le condizioni del servizio sono indicate nelle Condizioni di Servizio.

## 3. Dati personali trattati

**Dati dell'account e di identità:** nome, cognome, indirizzo email, numero DAPI e riferimento del certificato DAPI, lingua preferita, organizzazione e ruolo al suo interno, stato dell'account (attivo, disattivato o chiuso), date di registrazione, verifica e ultimo accesso. I dati DAPI provengono dalla certificazione di identità DAPI, anch'essa gestita da Informatica in Azienda.

**Dati di autenticazione:** codici di accesso monouso (conservati solo in forma di hash), il cookie di sessione, i token di accesso mobile (conservati solo in forma di hash) con nome del dispositivo, piattaforma, versione dell'app, ultimo indirizzo IP e stato di revoca, le API key (conservate solo in forma di hash) con piano, utilizzo e registrazione dell'accettazione delle Condizioni di Servizio (data, indirizzo IP, versione e digest del testo accettato).

**Dati degli intake:** il record canonico di intake (payload o dati strutturati inviati, dichiarazioni, nomi e ruoli inseriti dall'utente, profilo evidenziario calcolato dalla piattaforma, hash di intake, timestamp UTC ed evide_id), i contenuti caricati (file, archivi ZIP, URL o testi memorizzati come file) e i relativi metadati (nome, dimensione, tipo e hash).

**Record EAR ed ESB:** versioni dell'Evidentiary Artifact Record e relativi hash; osservazioni, dichiarazioni, eventi e record di chiusura dell'Epistemic Stabilization Buffer.

**Dati di certificazione:** richieste, preventivi e decisioni relative ai FEDIS, storico degli stati della richiesta, messaggi scambiati con il certificatore e record della piattaforma a cui fa riferimento un FEDIS emesso (codice FEDIS, hash certificato, riferimento EAR). Per i FEDIS-LINKED: la pratica tecnica di emissione, il numero nella serie, il collegamento all'intake, l'impronta dell'istantanea e l'esito delle verifiche eseguite alla generazione del documento.

**Record delle chiusure di catena:** quando una catena di intake collegati viene chiusa, la piattaforma registra il manifest congelato della catena e la sua impronta SHA-256, l'identificativo, il numero DAPI e la veste di chi l'ha chiusa e, per un'organizzazione, il suo ruolo, e l'ora della chiusura. Il manifest contiene gli identificativi, le ore e le impronte degli intake, delle versioni EAR e dei file inclusi; non contiene i nomi dei depositanti né i nomi originali dei file. La piattaforma registra inoltre gli eventi successivi alla chiusura, come la cancellazione di un intake incluso, con la persona che ha eseguito l'operazione, i riferimenti delle catene di integrazione con l'utente che le ha avviate e le richieste di FEDIS sul manifest con l'utente che le ha presentate. Quando un FEDIS sul manifest è stato emesso, l'amministrazione può caricare il PDF firmato: la piattaforma registra il file, il suo nome originale, la dimensione e l'impronta SHA-256, l'amministratore che lo ha caricato, l'ora del caricamento, se è stata rilevata una struttura di firma e, per i caricamenti successivi, le versioni sostituite. Il PDF contiene i dati riportati nel FEDIS, come il numero DAPI del richiedente, il numero DAPI e la veste di chi ha chiuso la catena e i dati del certificatore, e i dati inseriti con la firma e la marca temporale, come il nome del firmatario, i dati del certificato e l'ora della firma. Questi dati sono trattati per documentare il FEDIS emesso e per includerlo nei pacchetti della catena, per le finalità e sulle basi giuridiche del servizio FEDIS (Sezione 4). La piattaforma non valida la firma, la marca temporale o il certificato.

**Dati di Linked Responses (riscontri collegati):** i dati di questo blocco e del registro delle modifiche di accesso sono trattati quando le relative funzioni sono attive sulla piattaforma.

- **inviti:** chi invita; il record a cui l'invito si riferisce e l'organizzazione titolare; nome, cognome e numero DAPI del destinatario indicati da chi invita; visibilità scelta; date di creazione, scadenza e revoca. Il link d'invito è conservato solo in forma di hash;
- **dichiarazioni di chi invita** (condivisione e autorizzazione) e rappresentazione FAST REVIEW del record messa a disposizione del destinatario, con le relative impronte. Il destinatario non riceve il record completo né i documenti esterni che il record cita;
- **riscontri:** posizione dichiarata dal destinatario sulla rappresentazione del record, non sull'intero record; motivazione e riserva eventualmente scritte dal destinatario (la motivazione è obbligatoria per contestare) e relazione con un suo riscontro precedente, che resta conservato; nome e numero DAPI al momento del deposito; eventuale ruolo dichiarato; dichiarazione di presa visione del riepilogo; data e impronte. L'EAR-LINKED è il documento EAR che documenta il riscontro;
- **eventi dell'invito osservati dal server:** richieste di apertura del link ricevute, anche con un account diverso da quello del destinatario o su un invito sospeso; rappresentazioni prodotte dal server; dichiarazioni di presa visione delle informative. Questi eventi non dimostrano che una pagina sia stata mostrata sul dispositivo, letta o compresa;
- **revoca degli inviti:** revoche dirette di chi invita o di un owner o admin dell'organizzazione, con il motivo indicato; richieste di revoca (richiedente, ruolo osservato, motivo, descrizione, urgenza); sospensioni; decisioni, con il decisore e gli elementi su cui si basano; notifiche inviate e relativi tentativi di consegna;
- **autorità di riesame:** metadati dei documenti di titolo ricevuti (tipo, mittente e ruolo dichiarati, canale, data di ricezione, impronta e riferimento del luogo di conservazione, non il documento stesso); nome e numero DAPI della persona designata, con il periodo della designazione; chi ha registrato questi dati; verifiche (verificatore, metodo, fonte esaminata, esito dichiarato, impronta e riferimento della prova); recapiti email o PEC dell'organizzazione usati per le segnalazioni;
- **FEDIS-LINKED** (quando la funzione è attiva):
  - l'**istantanea** immutabile dei record pertinenti, formata quando chi ha depositato un intake richiede un FEDIS-LINKED. Per i riscontri includibili contiene i dati del riscontro indicati sopra: nome e numero DAPI al momento del deposito, eventuale ruolo dichiarato, posizioni, motivazioni, riserve, visibilità, date e impronte, data dell'eventuale revoca successiva dell'invito. Per i riscontri non includibili e per gli inviti

contiene solo identificativi, numero DAPI del destinatario, date, stato e impronte, senza nomi né contenuti. Contiene inoltre i conteggi descrittivi riportati nel documento;
    - le **notifiche** inviate a chi ha risposto quando un documento che include il suo riscontro è rilasciato: destinatario, riscontro, emissione, esito dell'invio;
    - le **sospensioni** di nuove emissioni durante la valutazione di un'opposizione: riscontro interessato, riferimento della pratica, date di apertura e chiusura, nessun contenuto dell'opposizione.

  Prima dei campi liberi (motivazione, riserva, ruolo) chi risponde riceve un avviso a non inserire dati sulla salute o altre categorie particolari di dati, dati di altre persone non necessari o informazioni riservate non pertinenti. La piattaforma non è progettata per trattare categorie particolari di dati; l'avviso non costituisce una base giuridica per trattarle.
- **registri tecnici:** osservazioni tecniche delle richieste (utente, sessione mobile, funzione richiamata, canale, esito, versione dell'app dichiarata; nessun indirizzo IP e nessun testo libero); registri che impediscono di registrare due volte la stessa azione; preparazioni di deposito non usate.

**Registro delle modifiche di accesso:** ogni richiesta di aggiungere o rimuovere un'appartenenza a un'organizzazione, di chiudere o riattivare un account, di disattivare o riattivare un'identità DAPI su EVIDE o di sospendere o riattivare un'organizzazione è registrata con istante, esito (eseguita, rifiutata o senza effetto), persona interessata (identificativo e numero DAPI), organizzazione, ruolo prima e dopo, chi ha agito e con quale autorizzazione, funzione di origine. Le segnalazioni all'amministratore EVIDE che ne derivano contengono solo conteggi e identificativi interni.

**Dati del registro pubblico:** solo per le voci pubblicate, i dati descritti nella Sezione 8.

**Log e dati di sicurezza:** log delle richieste API (API key, endpoint, indirizzo IP, hash della richiesta, esito, errore e tempo di elaborazione), log applicativi, log del server web, contatori usati per limitare i tentativi di accesso e le richieste API.

**Record di idempotenza delle API:** quando una richiesta API è inviata con una chiave di idempotenza, la piattaforma registra l'API key usata, la chiave scelta dal sistema del cliente, l'endpoint, un'impronta SHA-256 della richiesta, lo stato e i tempi dell'elaborazione, il riferimento interno all'intake o al buffer interessato e una copia della risposta restituita. Per un deposito la copia contiene i dati restituiti dall'API, che possono includere dichiarazioni e altri dati dell'intake descritti sopra. Questi record servono solo a riconoscere una richiesta ripetuta e a restituirne lo stesso esito; non fanno parte del record probatorio e non entrano in hash, versioni EAR o documenti FEDIS.

**Dati di fatturazione:** dati di fatturazione forniti dall'utente o dall'organizzazione (ad esempio nome, ragione sociale, indirizzo e identificativi fiscali), piani e pacchetti acquistati, utilizzo, eventi di fatturazione e fatture.

**Comunicazioni:** email e richieste inviate a Informatica in Azienda, incluse le richieste di assistenza e le richieste di esercizio dei diritti o di cancellazione dei dati.

**Dati personali di terzi:** i contenuti depositati possono contenere dati personali di persone diverse dall'utente (ad esempio persone nominate in un documento, in uno screenshot o in una dichiarazione). Informatica in Azienda non seleziona questi dati: sono scelti dall'utente che effettua il deposito.

I dati dell'account e di autenticazione sono necessari per utilizzare la piattaforma; senza di essi il servizio non può essere fornito. La piattaforma non è progettata per trattare categorie particolari di dati personali: gli utenti non dovrebbero depositarle se non dispongono di una specifica base giuridica per farlo.

## 4. Finalità e basi giuridiche

**Erogazione del servizio** (account, accesso, intake, EAR, ESB, chiusure di catena, FEDIS, API, app mobile, assistenza e, su richiesta dell'utente, pubblicazione nel registro pubblico): esecuzione di un contratto o di misure precontrattuali richieste dall'utente (art. 6(1)(b) GDPR). Comprende il riconoscimento delle richieste API ripetute con una chiave di idempotenza, affinché la stessa richiesta produca effetto una sola volta.

**Linked Responses:**

- creazione degli inviti, messa a disposizione della rappresentazione FAST REVIEW generata dal record indicato da chi invita, secondo il modello applicabile, registrazione dei riscontri e dell'EAR-LINKED, richieste, sospensioni e decisioni di revoca: esecuzione del contratto con l'utente che invita, con l'utente che risponde e con gli utenti che chiedono o decidono una revoca (art. 6(1)(b) GDPR);
- formazione dell'istantanea, documentazione dei riscontri in un FEDIS-LINKED richiesto da chi ha depositato l'intake e notifica a chi ha risposto:
  - per i dati di chi richiede il documento: esecuzione del contratto (art. 6(1)(b) GDPR);
  - per i dati di chi ha risposto e degli altri destinatari degli inviti: legittimo interesse di chi ha depositato l'intake a documentare in modo verificabile i riscontri ricevuti e di Informatica in Azienda a fornire tale documentazione (art. 6(1)(f) GDPR).

  Sono documentati con il loro contenuto solo i riscontri depositati dopo che al destinatario è stata mostrata un'informativa che descrive il FEDIS-LINKED; degli altri riscontri e degli inviti senza deposito sono riportati solo conteggi. La presa visione dell'informativa non è un consenso;
- trattamento dei dati del destinatario indicati da chi invita, dei dati delle persone designate, dei verificatori e dei recapiti dell'organizzazione, e documentazione di chi era ammesso a decidere sulle revoche e su quali elementi: legittimo interesse di Informatica in Azienda, delle organizzazioni e degli utenti coinvolti a una condivisione controllata e a decisioni di revoca documentate (art. 6(1)(f) GDPR);
- registro delle modifiche di accesso e registri tecnici: legittimo interesse a un servizio sicuro e a documentare chi poteva agire per un'organizzazione in un dato momento (art. 6(1)(f) GDPR); i registri tecnici servono anche a evitare depositi doppi (art. 6(1)(b) GDPR).

**Obblighi contabili, fiscali e altri obblighi di legge**, incluse le risposte a ordini di autorità competenti: adempimento di un obbligo legale (art. 6(1)(c) GDPR).

**Sicurezza della piattaforma e prevenzione degli abusi** (autenticazione, log, limiti alle richieste): legittimo interesse di Informatica in Azienda e degli utenti a un servizio sicuro (art. 6(1)(f) GDPR).

**Conservazione dei record probatori dopo la fine del servizio**, affinché depositi, documenti FEDIS e riscontri collegati restino verificabili, e accertamento, esercizio o difesa di diritti in sede giudiziaria: legittimo interesse di Informatica in Azienda e degli utenti (art. 6(1)(f) GDPR), nei limiti e per i periodi descritti nella Sezione 9 e fermi restando il diritto di opposizione e il diritto di chiedere la cancellazione.

**Comunicazioni di servizio**, inclusi gli avvisi di modifica delle Condizioni di Servizio e della presente informativa: esecuzione del contratto e legittimo interesse (art. 6(1)(b) e (f) GDPR).

I dati personali non sono utilizzati per marketing o profilazione. Il profilo evidenziario calcolato dalla piattaforma descrive un record depositato; non è una decisione riguardante una persona che produce effetti giuridici ai sensi dell'art. 22 GDPR. Gli utenti che depositano dati personali di terzi sono responsabili di disporre di una base giuridica per farlo.

## 5. Nessuna vendita dei dati, intelligenza artificiale e riservatezza

Informatica in Azienda non vende, non scambia, non cede in locazione e non concede in licenza i contenuti dei depositi a terzi per le loro finalità, e non li riutilizza per pubblicità, altre finalità commerciali, ricerche estranee al servizio o finalità di terzi. I contenuti dei depositi non sono utilizzati per addestrare, perfezionare o valutare modelli di intelligenza artificiale, propri o di terzi. La piattaforma non trasmette i contenuti dei depositi a servizi di intelligenza artificiale esterni; Informatica in Azienda non li fornisce a servizi di intelligenza artificiale esterni che utilizza manualmente, salvo che siano stati anonimizzati o che l'utente lo abbia autorizzato per iscritto per una finalità specifica. L'accesso ai contenuti dei depositi è limitato alle persone che ne hanno bisogno per fornire il servizio. Questi impegni sono indicati nella Sezione 7 delle Condizioni di Servizio e non impediscono il trattamento da parte dei fornitori indicati nella Sezione 7 che segue né le comunicazioni imposte dalla legge.

## 6. Ruolo di Informatica in Azienda

Informatica in Azienda agisce come **titolare del trattamento** per i dati dell'account, di autenticazione, di sicurezza, dei log, di fatturazione e delle comunicazioni, per il registro pubblico e per i record probatori che conserva, compresi i record di Linked Responses e le istantanee dei FEDIS-LINKED, per fornire il servizio e consentire la successiva verifica dei depositi e dei documenti FEDIS.

Per i dati personali di terzi contenuti nei contenuti depositati da un cliente, il ruolo di Informatica in Azienda dipende dal rapporto con quel cliente. Quando un cliente, ad esempio un'organizzazione, deposita contenuti per proprie finalità e Informatica in Azienda li tratta solo per conto di quel cliente, Informatica in Azienda agisce come **responsabile del trattamento** (art. 28 GDPR) e il trattamento deve essere disciplinato da un accordo sul trattamento dei dati. I clienti che necessitano di tale accordo devono contattare info@informaticainazienda.it prima di depositare dati personali di terzi.

**Organizzazioni ed ex membri.** Gli intake depositati per un'organizzazione sono accessibili ai suoi membri attuali. Il membro che esce dall'organizzazione conserva l'accesso in sola lettura agli intake che ha depositato personalmente per essa, limitato all'intake, alle sue versioni EAR, alle evidenze ancora conservate e allo stato corrente della richiesta; non ha accesso ai messaggi, alla cronologia degli stati, ai preventivi o ad altri dettagli economici, né agli altri intake dell'organizzazione. Gli ex membri che non hanno effettuato il deposito non vi hanno accesso. Questo accesso limitato si fonda sul legittimo interesse del depositante, che è identificato in quei record, e di Informatica in Azienda a consentire al depositante di verificare i depositi a lui attribuiti (art. 6, par. 1, lett. f) GDPR); non consente alcuna nuova operazione per conto dell'organizzazione (Condizioni di Servizio, Sezione 7.6).

## 7. Destinatari e trasferimenti

I dati personali possono essere trattati da:

- **Fornitore di hosting:** Aruba S.p.A., su server situati in Italia, in qualità di responsabile del trattamento per hosting e backup.
- **Email:** le email sono inviate tramite il server di posta di Informatica in Azienda, che opera sulla stessa infrastruttura di hosting.
- **Prestatori di servizi fiduciari qualificati:** quando viene emesso un FEDIS, il certificatore appone una firma elettronica qualificata e una marca temporale elettronica qualificata tramite un prestatore di servizi fiduciari qualificato, che tratta il documento o la sua impronta secondo il proprio ruolo ai sensi del Regolamento (UE) 910/2014 (eIDAS).
- **Destinatari scelti dall'utente:** le persone a cui l'utente consegna un FEDIS o altri record. Un FEDIS-LINKED è consegnato a chi lo ha richiesto, che può consegnarlo a terzi ed è responsabile degli usi e delle

comunicazioni che ne fa (Condizioni di Servizio, Sezione 7.8). Il documento riporta i dati dei riscontri inclusi indipendentemente dalla visibilità scelta per il riscontro sulla piattaforma.

- **Partecipanti a Linked Responses:** il destinatario di un invito vede la rappresentazione FAST REVIEW generata dal record indicato da chi invita, secondo il modello applicabile, e le informazioni dell'invito. Il riscontro, con nome, numero DAPI ed eventuale ruolo dichiarato di chi risponde, è visibile a chi ha invitato solo finché ha accesso al record secondo le regole applicabili (per un record di organizzazione, finché ne è membro attuale) e, se chi invita ha scelto questa visibilità, ai membri attuali dell'organizzazione titolare del record; gli ex membri non lo vedono. Gli altri membri dell'organizzazione non ricevono il FEDIS-LINKED né l'istantanea tramite la piattaforma, e non vedono il riepilogo dei riscontri, che è mostrato solo a chi ha depositato il record. Gli owner e admin attuali dell'organizzazione vedono anche gli inviti ancora utilizzabili creati sui suoi record da chi non ne fa più parte. Le richieste di revoca sono visibili agli owner e admin attuali dell'organizzazione, alle persone designate a decidere e all'amministratore EVIDE. I dati dell'autorità di riesame sono visibili all'amministratore EVIDE e ai verificatori incaricati da Informatica in Azienda; quando decide una persona designata, la base della decisione (designazione, data del titolo, verifica ed esito dichiarato) è mostrata insieme alla decisione. Se nessuno può decidere entro il termine di riesame, una segnalazione con i soli identificativi della richiesta può essere inviata ai recapiti verificati dell'organizzazione.
- **Il pubblico:** per le voci pubblicate nel registro pubblico, i dati descritti nella Sezione 8.
- **Consulenti professionali** tenuti alla riservatezza e **autorità** ove richiesto dalla legge.

L'app EVIDE Mobile è distribuita tramite store di applicazioni, che trattano i dati secondo le proprie informative. Una pagina del sito, Evidentiary Questions, include un widget di traduzione fornito da terzi (vedi Sezione 14).

Informatica in Azienda non trasferisce dati personali al di fuori dello Spazio Economico Europeo, salvo obblighi di legge. Il widget di traduzione descritto nella Sezione 14 è caricato da un fornitore terzo: tale fornitore e i servizi di traduzione di cui si avvale possono trattare dati tecnici dei visitatori, come l'indirizzo IP, al di fuori dello Spazio Economico Europeo, secondo le proprie condizioni.

## 8. Registro pubblico

Una voce è pubblicata nel registro pubblico EVIDE solo su richiesta del depositante e solo per intake per i quali è stato emesso un FEDIS; la pubblicazione è eseguita dal certificatore. Una voce pubblicata mostra il reference ID, il codice FEDIS, lo stato, l'hash di intake, il timestamp di intake e la data di pubblicazione. Il registro può inoltre mostrare altre voci pubblicate con lo stesso hash e, per gli intake che fanno parte di una catena evidenziaria, la posizione della voce nella catena e l'esistenza di altri intake non pubblicati della stessa catena, senza il loro contenuto né i loro identificativi. Le voci pubblicate sono accessibili a chiunque e possono essere indicizzate dai motori di ricerca.

Identificativi e hash possono essere dati personali quando possono essere collegati a una persona. L'utente può chiedere in qualsiasi momento la rimozione di una voce scrivendo a app@certifywebcontent.com o, in alternativa, a info@informaticainazienda.it. La rimozione elimina la voce pubblica; non cancella i record sottostanti, che sono trattati come descritto nelle Sezioni 9 e 11. Le copie delle voci pubbliche effettuate da terzi prima della rimozione sono fuori dal controllo di Informatica in Azienda.

## 9. Conservazione

I dati personali sono conservati solo per il tempo necessario alle finalità per cui sono trattati. Periodi e criteri di conservazione:

- **Dati dell'account:** per tutta la durata dell'account. Dopo la chiusura o la cancellazione dell'account sono rimossi dai sistemi attivi, ad eccezione dei dati necessari a documentare il rapporto contrattuale, l'accettazione delle Condizioni di Servizio e le relative comunicazioni, conservati per l'accertamento,

l'esercizio o la difesa di diritti in sede giudiziaria per non oltre il termine ordinario di prescrizione di 10 anni (art. 2946 del Codice civile), e dei dati da conservare a fini contabili e fiscali. Se un account è chiuso ma i record a esso collegati sono conservati, ad esempio gli intake depositati per un'organizzazione o i record che non possono ancora essere cancellati, il record dell'account è mantenuto in stato chiuso, insieme al nome e al numero DAPI attribuiti a quei record, solo finché quei record sono conservati, e non è usato per nessun altro scopo.

- **Contenuti caricati:** cancellati automaticamente dal server al termine del periodo indicato nella pagina dei prezzi per lo stato dell'intake, oppure all'emissione di un FEDIS, se precedente.
- **Record canonici di intake, record EAR ed ESB, storico e messaggi della certificazione, record relativi ai FEDIS:** per tutta la durata dell'account; dopo la chiusura, per il periodo necessario a consentire la verifica dei depositi e dei FEDIS emessi e l'accertamento, l'esercizio o la difesa di diritti in sede giudiziaria a essi relativi, che di regola non supera 10 anni dalla fine del rapporto contrattuale, salvo che sia necessario un periodo più lungo per una controversia in corso o una richiesta di un'autorità competente. Questi record non sono cancellati automaticamente: al termine del periodo, Informatica in Azienda li cancella o li anonimizza. Possono essere cancellati prima come descritto nella Sezione 11.
- **Record delle chiusure di catena:** nei periodi della voce precedente, finché resta sulla piattaforma almeno un intake incluso nella catena chiusa o una richiesta di FEDIS sul suo manifest; quando l'ultimo di questi viene cancellato, i record della chiusura e i loro eventi vengono cancellati con esso. Il riferimento conservato da una catena di integrazione segue i record di quella catena. I documenti firmati di un FEDIS sul manifest, comprese le versioni sostituite, sono conservati con i record della chiusura e non sono rimossi dalla conservazione automatica dei contenuti caricati; la piattaforma non offre una funzione ordinaria per cancellarli e, finché esistono, la pratica tecnica di quel FEDIS e i record della chiusura sono conservati. Un'eventuale cancellazione, per esempio quando è richiesta dalla legge o a seguito di una richiesta ai sensi della Sezione 12, è valutata separatamente.
- **Record di Linked Responses, registro delle modifiche di accesso e segnalazioni amministrative collegate** (inviti e relativi eventi; dichiarazioni di chi invita; rappresentazioni; riscontri; prese visione; EAR-LINKED; richieste, sospensioni, revoche e decisioni, con le relative notifiche; dati dell'autorità di riesame; istantanee, pratiche tecniche, notifiche e sospensioni dei FEDIS-LINKED): per tutta la durata degli account interessati e del record a cui si riferiscono; dopo, per il periodo necessario a consentire la verifica dei riscontri e delle decisioni e l'accertamento, l'esercizio o la difesa di diritti in sede giudiziaria a essi relativi, che di regola non supera 10 anni dalla fine dell'ultimo rapporto contrattuale interessato, salvo che sia necessario un periodo più lungo per una controversia in corso o una richiesta di un'autorità competente. Questi record non sono cancellati automaticamente: al termine del periodo, Informatica in Azienda li cancella o li anonimizza.
- **Documenti di titolo e prove delle verifiche dell'autorità di riesame:** sulla piattaforma sono conservati solo i metadati e i riferimenti indicati nella Sezione 3, con il periodo della voce precedente. I documenti originali non sono caricati sulla piattaforma e restano nel canale o nell'archivio indicato nel riferimento; quelli ricevuti da Informatica in Azienda sono conservati secondo la voce «Comunicazioni e richieste».
- **Registri tecnici di Linked Responses:** osservazioni tecniche delle richieste: 90 giorni dalla registrazione. Registri contro la doppia registrazione della stessa azione e preparazioni di deposito non usate: 30 giorni (720 ore) dalla chiusura definitiva dell'invito a cui si riferiscono, cioè dalla sua revoca o, se precedente, dalla sua scadenza originaria; le sospensioni e gli altri stati reversibili dell'invito non fanno decorrere il periodo. Ogni mese Informatica in Azienda verifica quali registri hanno raggiunto il termine e, se necessario, li cancella con un'esecuzione di conservazione manuale e registrata. Restano distinti i log del server web (voce «Log del server web»), le copie di backup (Sezione 10) e le esportazioni temporanee create durante interventi di manutenzione, custodite con accesso limitato e cancellate quando non sono più necessarie.
- **Voci del registro pubblico:** fino alla richiesta di rimozione o alla cancellazione dei record sottostanti.

- **Codici di accesso:** validi 15 minuti; cancellati entro 24 ore dalla scadenza. I contatori dei tentativi di accesso sono cancellati al termine del periodo di blocco di 15 minuti.
- **Sessioni web:** una sessione web termina un'ora dopo l'accesso; il cookie di sessione è cancellato alla chiusura del browser.
- **Sessioni mobile:** un token di accesso mobile resta valido finché l'utente non esce o la sessione non viene revocata. I record delle sessioni revocate sono cancellati 12 mesi dopo la revoca; i record delle sessioni attive sono cancellati insieme all'account.
- **Log delle richieste API e log applicativi:** 12 mesi. I totali mensili di utilizzo ricavati dai log API sono conservati come dati di fatturazione.
- **Record di idempotenza delle API:** 7 giorni dalla prima richiesta inviata con la chiave; sono poi cancellati da una procedura automatica giornaliera. Quando un intake è cancellato, le copie delle risposte che vi si riferiscono sono sostituite subito da un avviso privo di qualsiasi dato del record, e il record tecnico residuo è cancellato al termine dello stesso periodo. Il record di una richiesta interrotta dopo che il relativo deposito era stato registrato non è cancellato automaticamente, perché la sua cancellazione potrebbe far registrare due volte lo stesso deposito: è conservato finché la richiesta non è completata da un nuovo tentativo con la stessa chiave o finché Informatica in Azienda, verificato il caso, non lo cancella.
- **Contatori del limite di richieste API:** cancellati dopo 15 minuti.
- **Log del server web:** conservati secondo la rotazione dei log configurata sul server di hosting.
- **Dati di fatturazione e scritture contabili:** i dati di fatturazione per tutta la durata dell'account; fatture e scritture contabili per 10 anni, come previsto dall'art. 2220 del Codice civile.
- **Comunicazioni e richieste**, incluse le richieste di esercizio dei diritti o di cancellazione dei dati e le relative autorizzazioni: per il tempo necessario a documentare la richiesta e il suo esito, di regola non oltre 10 anni.

## 10. Backup e copie fuori dal nostro controllo

L'ambiente di hosting conserva copie di backup per il ripristino in caso di guasto. I dati cancellati dai sistemi attivi possono restare nelle copie di backup finché queste non vengono sovrascritte secondo la rotazione dei backup. Le copie di backup non sono utilizzate per altre finalità; se un backup deve essere ripristinato, i dati cancellati nel frattempo vengono cancellati di nuovo. Le esportazioni occasionali effettuate per manutenzione o test sono conservate solo per il tempo necessario a tale attività e poi cancellate.

La cancellazione dai sistemi di EVIDE non può raggiungere le copie che non sono sotto il controllo di Informatica in Azienda, come i documenti FEDIS e gli altri record già consegnati all'utente o a terzi, i file scaricati dall'utente e le copie delle voci pubbliche effettuate da terzi.

## 11. Disattivazione, chiusura dell'account e cancellazione

La **disattivazione** sospende l'accesso all'account; non cancella i dati dell'account né i record probatori.

La **chiusura e la cancellazione dell'account** possono essere richieste per iscritto a app@certifywebcontent.com o, in alternativa, a info@informaticainazienda.it. La piattaforma non offre attualmente agli utenti una funzione self-service per cancellare gli intake o l'account: ogni richiesta è valutata singolarmente, sulla base dell'identità e dei poteri documentati del richiedente e della normativa applicabile. Quando la cancellazione è autorizzata, può comprendere l'account, i record canonici di intake, le versioni EAR, i record ESB, le voci del registro pubblico e i record relativi ai FEDIS conservati sulla piattaforma, che sono rimossi dai sistemi attivi. La cancellazione di un intake a cui sono collegati inviti o riscontri di Linked Responses non è eseguita con la procedura ordinaria: è valutata separatamente, tenendo conto anche dei diritti degli altri utenti sulle proprie dichiarazioni e dei record di revoca collegati.

Quando un account è chiuso, gli intake personali dell'utente che possono essere cancellati sono cancellati insieme ai record dipendenti, le sessioni e le chiavi API sono revocate definitivamente e le appartenenze a organizzazioni sono rimosse. Se nulla deve essere conservato, l'account e l'abilitazione dell'identità DAPI dell'utente su EVIDE sono cancellati; altrimenti l'account è mantenuto in stato chiuso, collegato soltanto ai record che devono essere conservati (vedi Sezione 9), e l'utente è informato di ciò che è stato conservato e del perché. La chiusura di un account EVIDE non revoca la certificazione DAPI, che è disciplinata dalle proprie condizioni. Un account chiuso non viene riaperto automaticamente: l'accesso può essere ripristinato solo su richiesta, dopo la verifica dell'identità del richiedente, e non sono ripristinati i record cancellati, le credenziali revocate e le precedenti appartenenze a organizzazioni.

Alcuni dati possono essere conservati dopo una cancellazione autorizzata solo se una base giuridica documentata lo giustifica, ad esempio le scritture contabili da conservare per legge o i dati necessari per una controversia in corso. Quando una cancellazione non può essere eseguita per ragioni tecniche, il trattamento è limitato finché la cancellazione non può essere eseguita; un vincolo tecnico non costituisce di per sé un motivo legittimo per rifiutare la cancellazione. I dati cancellati possono restare nelle copie di backup come descritto nella Sezione 10. Una volta cancellati i relativi record della piattaforma, un FEDIS già consegnato potrebbe non essere più verificabile rispetto ai record di EVIDE.

## 12. I tuoi diritti

Ai sensi degli artt. da 15 a 22 GDPR hai il diritto di:

- accedere ai tuoi dati personali;
- chiederne la rettifica;
- chiederne la cancellazione, che è valutata caso per caso e può essere limitata quando nel caso specifico si applica un'eccezione prevista dall'art. 17(3) GDPR, ad esempio quando i dati sono necessari per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria;
- chiedere la limitazione del trattamento, che può applicarsi anche in alternativa alla cancellazione;
- ricevere i dati che hai fornito in un formato strutturato, di uso comune e leggibile da dispositivo automatico, quando il trattamento si basa sul contratto ed è effettuato con mezzi automatizzati;
- opporti al trattamento basato sul legittimo interesse;
- proporre reclamo al Garante per la protezione dei dati personali (www.garanteprivacy.it) o all'autorità di controllo del Paese in cui vivi o lavori.

Chi ha depositato un riscontro può opporsi alla sua documentazione in nuovi FEDIS-LINKED. Durante la valutazione dell'opposizione Informatica in Azienda può sospendere le nuove richieste e i rilasci che lo includerebbero; la sospensione non modifica né cancella i record e non raggiunge i documenti già consegnati (Sezione 10).

Le richieste vanno inviate a app@certifywebcontent.com o, in alternativa, a info@informaticainazienda.it. Informatica in Azienda può chiedere le informazioni necessarie a verificare l'identità del richiedente. Una richiesta ricevuta attraverso un altro canale non viene ignorata per questo solo motivo; l'indirizzo da cui una richiesta è inviata non costituisce, di per sé, prova sufficiente dell'identità. La risposta è fornita senza ingiustificato ritardo e comunque entro un mese dal ricevimento; questo termine può essere prorogato di due mesi, se necessario, tenuto conto della complessità e del numero delle richieste, e il richiedente è informato della proroga entro il primo mese. Le richieste sono gratuite, salvo che siano manifestamente infondate o eccessive. Informatica in Azienda comunica ai destinatari a cui i dati sono stati trasmessi le eventuali rettifiche, cancellazioni o limitazioni, salvo che ciò si riveli impossibile o implichi uno sforzo sproporzionato.

Anche le persone i cui dati sono contenuti nei contenuti depositati da un utente possono esercitare questi

diritti. Quando Informatica in Azienda agisce come responsabile del trattamento per un cliente, inoltra la richiesta a quel cliente e lo assiste nella risposta.

## 13. Sicurezza

La piattaforma è accessibile solo tramite connessioni cifrate (HTTPS). I cookie di sessione sono protetti (Secure, HttpOnly, SameSite=Strict); i codici di accesso, i token di accesso mobile e le API key sono conservati solo in forma di hash. L'accesso agli account può essere sospeso immediatamente, e i tentativi di accesso e le richieste API sono soggetti a limiti. Gli hash di integrità consentono di rilevare qualsiasi alterazione dei record depositati rispetto a un hash di riferimento.

## 14. Cookie Policy

**Cookie tecnici (senza consenso):**
La piattaforma utilizza solo cookie strettamente necessari al suo funzionamento:

- `cwc_session`: cookie di sessione per la gestione dell'autenticazione; viene cancellato alla chiusura del browser;
- `lang`: memorizza la lingua selezionata dall'utente; durata 12 mesi.

Questi cookie non richiedono consenso e vengono installati automaticamente.

**Widget di traduzione di terzi:**
La pagina Evidentiary Questions carica un widget di traduzione fornito da GTranslate (cdn.gtranslate.net). All'apertura della pagina, il browser si collega ai server di tale fornitore; se si seleziona una traduzione, il widget può memorizzare un cookie per ricordare la lingua scelta, e la traduzione è fornita da servizi di traduzione di terzi. Nessun'altra pagina della piattaforma carica questo widget.

**Nessun cookie di tracciamento:**
La piattaforma non utilizza Google Analytics, Facebook Pixel o altri cookie analitici, pubblicitari o di profilazione.

**App EVIDE Mobile:**
L'app non utilizza cookie. Conserva il token di accesso sul dispositivo affinché l'utente resti connesso fino all'uscita.

**Gestione dei cookie:**
Puoi gestire o cancellare i cookie dalle impostazioni del browser. La disabilitazione dei cookie tecnici potrebbe impedire il corretto funzionamento della piattaforma.

## 15. Modifiche alla presente informativa

La presente informativa può essere aggiornata. Le modifiche sostanziali sono comunicate via email agli utenti registrati almeno 30 giorni prima che abbiano effetto; la comunicazione indica la nuova versione e la data da cui si applica. La versione vigente è sempre disponibile a questo indirizzo e le versioni precedenti sono disponibili su richiesta. Ogni versione della presente informativa, insieme alle Condizioni di Servizio in vigore dalla stessa data, è pubblicata anche come documento PDF con firma elettronica qualificata, scaricabile da questa pagina con la relativa impronta SHA-256; una volta pubblicata, una copia firmata non viene mai sostituita.

# Signature / Firma

This document is prepared to be signed by Dott. Emanuel Celano, on behalf of Informatica in Azienda, with a qualified electronic signature (eIDAS) in PAdES format and a qualified electronic timestamp. Once applied, the signature, the timestamp and the certificate data will be contained in this PDF and can be verified with any eIDAS-compliant validation tool, for example Adobe Acrobat or the EU DSS validator. The date of signature will be the one recorded in the signature.

Il presente documento è predisposto per essere firmato dal Dott. Emanuel Celano, per conto di Informatica in Azienda, con firma elettronica qualificata (eIDAS) in formato PAdES e marca temporale qualificata. Una volta apposte, la firma, la marca temporale e i dati del certificato saranno contenuti in questo PDF e potranno essere verificati con qualsiasi strumento di validazione conforme a eIDAS, ad esempio Adobe Acrobat o il validatore DSS dell'UE. La data della firma sarà quella registrata nella firma stessa.