ANALISI FUNZIONALE

Attesta

La piattaforma che prova che cosa è stato mostrato a una persona, che cosa ha accettato, negato o revocato, e quando.

Consensi · Evidenze · Verifica · Registro cookie

Versione 1.0 · 5 novembre 2026

Indice

1	Sintesi	3
2	Il problema e a chi si rivolge	4
3	Concetti chiave	6
4	Il ciclo di funzionamento	8
5	Installazione, utenti e accessi	9
6	Soggetti e identità	10
7	Import dell'anagrafica e dello storico	12
8	Documenti, ambiti, finalità e requisiti	13
9	Motore di verifica	15
10	Richieste e percorso del destinatario	16
11	Self-service e revoca	18
12	Evidence vault: il registro delle prove	19
13	Notifiche e OTP	20
14	Controllo massivo e distribuzione massiva	21
15	Dashboard e report	22
16	Accettazioni raccolte da siti web	23
17	Banner cookie e registro dei consensi del sito web	25
18	Ruoli e permessi	29
19	Integrazioni e API	30
20	Sicurezza, privacy e conformità	31
21	Modello di erogazione e parametri	32
22	Glossario	34

1 Sintesi

Attesta è la piattaforma che prova quale testo è stato mostrato a una persona, che cosa ha scelto, con quale comando, in quale sessione e con quale livello di autenticazione. Ogni fatto entra in un registro che non si può riscrivere senza che il sistema se ne accorga.

01

Raccogliere

Consensi, autorizzazioni, accettazioni, prese visione, dichiarazioni e consegne di documenti, sul canale più comodo: QR allo sportello, link via SMS o email, portale aziendale, modulo di un sito web, banner cookie.

02

Provare

Ogni scelta diventa un'evidenza nello stesso istante. La catena di impronte crittografiche è unica per installazione, ogni artefatto è cifrato e il pacchetto probatorio è firmato e verificabile fuori dalla piattaforma.

03

Rispondere

Un operatore o un sistema esterno chiede «posso procedere?» e ottiene due esiti distinti, completezza e decisione, motivati requisito per requisito, anche riferiti a una data passata.

Esigenza	Come risponde Attesta
Raccogliere i consensi in modo ordinato	Requisiti configurati una volta per categoria di persone. A ciascuno si propone solo ciò che manca, nell'ordine giusto, senza chiedere due volte ciò che è già stato dato o negato
Dimostrare che cosa è successo	Per ogni fatto: testo esatto del comando, copia del contenuto mostrato e suo hash, sessione e livello di autenticazione
Sapere se si può usare un dato	La Verification API risponde, per esempio, «per marketing.email questo cliente è allowed / denied», con il motivo. Il controllo massivo risponde per 50.000 righe in una volta
Ricostruire il passato	«Com'era il 1° marzo» con regole e testi in vigore allora; per l'audit anche «che cosa sapevamo il 1° marzo»
Rispettare i diritti della persona	Area personale senza password: consultazione, download della versione esatta su cui ha agito, revoca con effetto immediato anche per i sistemi esterni
Non perdere lo storico	I consensi raccolti prima di Attesta si importano con la loro data. Il livello di prova è quello dichiarato dalla fonte e non viene mai innalzato
Provare i consensi cookie del sito	Ogni scelta fatta sul banner cookie è registrata lato server, consultabile ed esportabile, con il grafico dell'andamento di consensi e rifiuti
Proteggere i dati	Installazione dedicata per cliente, cifratura applicativa di ogni dato personale e di ogni contenuto, chiavi in un gestore di segreti separato

Che cosa distingue Attesta

1. **Due risposte, non un semaforo.** Chi ha negato il marketing ha la posizione completa, ma per marketing.email la decisione è non procedere. I prodotti che riducono tutto a «conforme / non conforme» confondono le due cose.
2. **Lo stato si calcola, non si scrive.** Deriva dagli eventi e dalla configurazione vigente a un istante, quindi si ricostruisce a ogni data.
3. **Niente si sovrascrive.** Una correzione aggiunge una versione. Una revoca è un nuovo evento che cita quello revocato. Il database stesso impedisce all'applicazione di modificare o cancellare le prove.
4. **Un guasto non diventa mai un «no».** Un problema tecnico è dichiarato come tale, alla persona e ai sistemi. «Non verificabile» non è «alterata».
5. **Onestà probatoria.** Uno storico importato o una spunta raccolta da un sito portano un livello di prova esplicito e più basso, che il sistema non innalza mai. È il cliente a decidere, requisito per requisito, se quegli eventi contano.
6. **Prova verificabile fuori dalla piattaforma.** Il pacchetto ZIP firmato con Ed25519 si verifica con `sha256sum` e una libreria standard, senza strumenti forniti da Attesta.

2 Il problema e a chi si rivolge

Consensi, informative e accettazioni sono di solito sparsi fra moduli cartacei, CRM, email e PDF firmati. Quando un'autorità, un auditor o un giudice chiede «che cosa aveva accettato questa persona, il 3 marzo, su quale testo?», la risposta richiede giorni ed è difficile da provare. Il CRM sa che c'è un flag «consenso = sì»; non sa quale testo era stato mostrato, con quale gesto, se il testo è cambiato o se la persona ha revocato da un altro canale.

Attesta riunisce tre bisogni che di solito stanno in strumenti diversi: raccogliere in modo ordinato le scelte delle persone sul canale più comodo, provarle con evidenze non alterabili, rispondere subito alla domanda «posso procedere?».

Profilo	Che cosa ne ricava
Privacy officer, compliance manager	Definisce una volta che cosa serve a ciascuna categoria di persone, vede chi è in regola e chi no, avvia le raccolte mancanti, risponde a un'ispezione con un pacchetto firmato
Operatore di sportello	Cerca la persona, vede che cosa manca, mostra un QR o invia un link e segue il completamento in diretta

Profilo	Che cosa ne ricava
Auditor, DPO, controllo interno	Consulta tutto in sola lettura, ricostruisce lo stato a una data passata, verifica la catena ed esporta le prove
IT, amministratore di sistema	Gestisce installazione, utenti, integrazioni e canali di invio senza vedere dati personali né prove
Sistemi aziendali (CRM, marketing automation, HR, gestionali, siti web)	Alimentano l'anagrafica, chiedono se un contatto è utilizzabile, creano richieste e ottengono il link da mostrare
La persona (cliente, dipendente, fornitore, paziente, studente...)	Capisce chi le chiede che cosa e perché, sceglie dal telefono senza caselle preselezionate, rivede e revoca in seguito senza creare un account
Il visitatore del sito web	Sceglie dal banner cookie; la sua scelta è registrata come prova e ritrovabile con il proprio ID consenso

Scenari d'uso

Clienti allo sportello

Banca, assicurazione, energia, telefonia, retail. Il cliente inquadra un QR e dà i consensi dal proprio telefono, con un codice via SMS. Il CRM e la marketing automation interrogano Attesta prima di ogni campagna.

Dipendenti e collaboratori

Informativa privacy, regolamento IT, policy di sicurezza, NDA, con presa visione o accettazione e una scadenza. Alla nuova versione di un regolamento, l'accettazione si richiede solo a chi la deve rinnovare.

Fornitori e partner

Codici etici, condizioni e dichiarazioni, con i valori confermati conservati nella prova.

Siti web e portali

Moduli di contatto e di iscrizione, e banner cookie: ogni spunta e ogni scelta sono registrate con un livello di prova esplicito.

Minori e persone rappresentate

Genitore, tutore o amministratore di sostegno agiscono per conto della persona; la prova registra entrambi.

Verifiche retrospettive

A un reclamo o a un'ispezione si risponde riga per riga, con la data dell'invio contestato.

3 Concetti chiave

Il prodotto poggia su otto distinzioni che il sistema non confonde mai.

Soggetto e actor

Il soggetto è la persona a cui si riferiscono gli obblighi; l'actor è chi ha compiuto materialmente l'azione. Di solito coincidono, ma un genitore può agire per il figlio: la prova registra sempre entrambi. La categoria del soggetto (cliente, dipendente, fornitore…) si chiama tipologia ed è configurabile, con campi, identificativi e requisiti propri.

Requisito, azione, evento, evidenza

Entità	Domanda a cui risponde	Esempio
Requisito	Che cosa serve, a chi, con quali regole?	«Ai clienti serve il consenso a comunicazioni promozionali via email; facoltativo; revocabile; prova rafforzata con OTP»
Azione	Che cosa deve fare la persona?	Dare o negare il consenso sul testo della versione 3
Evento	Che cosa è successo, e quando?	`consent_granted`, accaduto il 3/3 alle 10:42:05, registrato il 3/3 alle 10:42:05
Evidenza	Come lo dimostro?	Manifest con comando, sessione, OTP e hash, copia del testo, anello della catena

Le sei azioni

Azione	Che cosa fa la persona	Esiti
Sola consegna	Nulla: il documento è reso disponibile o consegnato e ne resta traccia	Messa a disposizione, consegna confermata o visualizzazione, secondo la regola del requisito
Presa visione	Conferma esplicitamente di aver preso visione	`acknowledged`
Consenso	Acconsente o non acconsente a una finalità	`consent_granted` / `consent_denied`; revocabile
Autorizzazione	Autorizza o non autorizza, eventualmente per un periodo	`authorization_granted` / `authorization_denied`; revocabile
Accettazione	Accetta un regolamento o un accordo, o lo rifiuta se ammesso	`accepted` / `refused`
Dichiarazione	Conferma un testo e i dati mostrati	`declaration_confirmed`, con i valori confermati nella prova

Regole comuni: il comando è sempre esplicito e mai preselezionato; il testo esatto del pulsante confermato entra nella prova; un «no» è un esito valido, registrato come un «sì»; aprire un documento produce solo un evento di consultazione, che non vale mai come presa visione.

Completezza e decisione: due esiti distinti

Esito	Domanda	Valori
`completion_status`	La posizione è completa rispetto ai requisiti?	`complete`, `incomplete`, `attention` (conflitto dopo l'unificazione di due anagrafiche), `unknown`, `not_applicable`
`decision`	Un processo può procedere, in questo ambito?	`allowed`, `denied`, `action_required`, `not_applicable`, `unknown`

> Un cliente che ha negato il consenso marketing facoltativo ha posizione `complete` e decisione su `marketing.email = denied`. Un dipendente che ha rifiutato un regolamento obbligatorio è `incomplete` e `denied`. Una persona non trovata è `unknown` / `unknown`: mai «negato» per un errore di battitura, mai «consentito» per un ambito inesistente.

Ambiti (scope)

Un ambito è una classificazione gerarchica dei trattamenti con un codice stabile, per esempio `marketing`, `marketing.email`, `marketing.sms`. È la dimensione lungo cui si chiede la verifica. Ogni ambito dichiara come si valuta: `completion` («la posizione è in regola?»), `permission` («posso usare questo canale?») o `mixed`.

Stato derivato del requisito

Lo stato di ogni coppia persona/requisito si ricalcola a ogni domanda: mai espresso, attivo, negato, revocato, scaduto (passata la validità in giorni), superato (una nuova versione del testo chiede una nuova azione), non applicabile. Nessuno è memorizzato come verità: è sempre ricostruibile dagli eventi.

Livelli di prova

Livello	Significato
`base`	Link o QR personale aperto in una sessione valida, con azione esplicita
`reinforced`	Come base, più un codice OTP verificato nella stessa sessione su un recapito già noto
`none` / `declared` / `documented`	Eventi importati: livello dichiarato dalla fonte, `documented` solo con un artefatto allegato, mai innalzato
`integration_declared`	Scelta dichiarata da un sito web. Inferiore a `base`, mai innalzata, non può soddisfare un requisito che chiede l'OTP

Il tempo: due orologi

Attesta è bitemporale: distingue quando un fatto è accaduto (`occurred_at`; per una configurazione, il periodo di efficacia) da quando Attesta lo ha saputo (`recorded_at`).

- `as_of`: «com'era la posizione il 1° marzo, con tutto ciò che sappiamo oggi?». Disponibile anche nell'API pubblica.
- `knowledge_as_of`: «che cosa sapevamo il 1° marzo?». Esclude ciò che è stato registrato dopo, per esempio uno storico importato ieri. È lo strumento di audit interno, tracciato.

Nessuna configurazione si sovrascrive: una modifica chiude la versione precedente e ne apre una nuova, sigillata nella catena. Una verifica a una data passata usa requisiti, testi, ambiti, tipologia della persona e rappresentanze di quella data.

4 Il ciclo di funzionamento

Il ciclo è sempre lo stesso, per un cliente allo sportello, per un dipendente via email o per migliaia di persone in una distribuzione massiva.

1 — Censire
Dal CRM o dall'HR via API o file, compreso lo storico dei consensi già raccolti.

2 — Dire che cosa serve
Per ogni tipologia: documenti, scelte, livello di prova e validità.

3 — Chiedere
Dalla scheda, da un'integrazione o in massa, con QR, SMS o email.

4 — La persona agisce
Dal proprio telefono: legge, sceglie, conferma, eventualmente con OTP.

5 — Ogni scelta è una prova
Nello stesso istante, in un registro che non si riscrive.

6 — Chiunque verifica
Operatore, sistema esterno o auditor, anche a una data passata.

7 — Cambiare idea
Revoca dal self-service, già visibile alla verifica successiva.

Tre principi rendono la prova credibile: lo stato non si scrive, si calcola; niente si sovrascrive; un guasto tecnico non diventa mai un «no».

5 Installazione, utenti e accessi

Ogni cliente ha un'installazione dedicata, con istanza, database, object storage e gestore di chiavi propri. Non esiste il concetto di tenant: nessun dato, nessuna chiave e nessun amministratore è condiviso fra clienti. Il provisioning è ripetibile e automatizzabile e produce la configurazione con i valori predefiniti, i feature flag e il primo amministratore tecnico, che riceve un invito. Gli aggiornamenti passano da migrazioni versionate che non modificano né cancellano le prove già registrate.

Marchio e comunicazioni del cliente

La persona vede l'organizzazione che le scrive, non Attesta. L'installazione ha i propri elementi di marchio: nome e dati minimi dell'azienda, logo (PNG o JPEG verificati sui byte, fino a 1 MB e 2000 px), colore primario, nome e indirizzo del mittente email, testo introduttivo delle email. Se il colore primario non garantisce un contrasto sufficiente, le pagine pubbliche usano il colore predefinito.

Feature flag

Le funzioni opzionali si accendono o si spengono al provisioning: canale SMS, distribuzione massiva, import storico, self-service, Distribution API e registro dei consensi cookie. Una funzione spenta non è raggiungibile né dal menu né dalle API. Il prodotto si adatta così al contratto del cliente senza versioni diverse del software.

Parametri di prodotto

Durate, scadenze, limiti e cadenze dei controlli sono parametri dell'installazione, ciascuno con un valore predefinito e un intervallo ammesso. Ogni modifica entra nell'audit con i valori prima e dopo. Alcuni pavimenti non si abbassano: password di almeno 12 caratteri, OTP di almeno 6 cifre, file di contenuto fino a 20 MB.

Accesso al backoffice

Aspetto	Comportamento
Attivazione	Invito via email valido 72 ore. L'utente imposta la password, registra un'app authenticator (TOTP) e riceve 8 codici di recupero monouso
Credenziali	Email, password di almeno 12 caratteri con blocklist di password compromesse, secondo fattore TOTP obbligatorio. Nessuna regola di composizione né scadenza, in linea con NIST SP 800-63B
Tentativi falliti	Dopo 5 tentativi consecutivi l'account si blocca per 15 minuti. Il messaggio è sempre «Credenziali non valide», così non rivela se un account esiste, è bloccato o sospeso
Sessione	8 ore al massimo e 30 minuti di inattività, con avviso 2 minuti prima. Ogni utente vede e chiude le proprie sessioni
Utenti	Quattro ruoli fissi, uno per utente. Gli utenti si sospendono e non si cancellano; resta sempre almeno un amministratore tecnico attivo

Aspetto	Comportamento
Audit	Accessi, fallimenti, blocchi, cambi di ruolo e di configurazione entrano in un registro append-only, con IP e user agent

Pagina «Stato dell'installazione»

Mostra la versione dell'applicazione, i feature flag attivi, l'esito del test che verifica che l'utenza applicativa non possa modificare le tabelle probatorie, lo stato delle chiavi (versione, ultima rotazione, avanzamento della ri-cifratura, controllo di usabilità, mai il valore) e le chiavi pubbliche del sigillo dei pacchetti, comprese quelle ritirate, con il periodo di validità. Una checklist «fatto / da fare» guida la configurazione iniziale.

6 Soggetti e identità

Attesta lavora su persone conosciute. I dati arrivano dai sistemi che li possiedono già (CRM, HR, ERP), senza un secondo inserimento, e ogni valore anagrafico porta la propria provenienza: fonte, autore e data.

Tipologie e campi

Il compliance manager definisce le tipologie di soggetto e, per ciascuna, i campi, scegliendo fra sette tipi con validazione formale: testo, email, telefono, codice fiscale, matricola, ID esterno, data. Per ogni campo si decide se è obbligatorio, ricercabile, univoco, da verificare; chi lo vede (persona, operatore, integrazioni); chi può modificarlo; la fonte autoritativa; se partecipa alle regole, nel qual caso è storicizzato con i due orologi.

Fonti, identificativi e riconciliazione

Ogni sistema esterno è una fonte. La coppia fonte + identificativo esterno è univoca in tutta l'installazione e rende idempotenti API e import.

La riconciliazione è deterministica ed è la stessa per API, import e backoffice: prima l'identificativo esterno, poi i campi univoci. Un'ambiguità o un conflitto non creano mai niente e non aggiornano mai a metà: restituiscono un codice d'errore esplicito. Un campo che appartiene al CRM lo aggiorna solo il CRM; un aggiornamento scartato per precedenza non è un errore e gli altri campi procedono. Il compliance manager può forzare un valore con una motivazione tracciata. Un valore vuoto in ingresso significa «non fornito» e non cancella niente.

Recapiti

Email e telefono sono verificati o non verificati. Un recapito diventa verificato quando arriva dalla fonte autoritativa o quando la persona conferma un OTP su quel recapito. Lo stato si deriva, non si imposta a mano. Ovunque il recapito compare mascherato (`ma****@azienda.it`, oppure le ultime tre cifre del telefono).

Ricerca

L'elenco dei soggetti è paginato, con le colonne di ricerca della tipologia e un filtro «contiene» per colonna (dai due caratteri, senza distinguere maiuscole e accenti). Una ricerca globale esatta lavora su tutte le tipologie. Le ricerche non aprono mai una scheda in automatico e non scelgono fra più risultati. Gli archiviati sono esclusi, salvo filtro esplicito riservato a compliance manager e auditor.

Archiviazione, cambio di tipologia, storia

- **Archiviazione.** Il soggetto esce da ricerche, distribuzioni e nuove richieste e in verifica risulta `unknown`. Le richieste aperte sono annullate; eventi, evidenze e audit restano.
- **Cambio di tipologia.** Per esempio «collaboratore → dipendente dal 1° del mese», con data di efficacia, motivazione e anteprima degli effetti. Una verifica a data anteriore vede la vecchia tipologia.
- **Storia degli attributi.** Per i campi che partecipano alle regole si sa com'erano a ogni data e da quando Attesta lo sapeva.

Unificazione dei doppioni (consolidamento)

Due posizioni della stessa persona si unificano a mano, solo dal compliance manager. La ricerca dei possibili doppioni è esatta, su uno o più campi scelti, senza punteggi di somiglianza.

1. Un confronto affiancato mostra attributi, identificativi, richieste aperte, rappresentanze, eventi e possibili conflitti.
2. Chi consolida sceglie la posizione canonica, scrive una motivazione e dichiara di aver verificato identità e fonti.
3. Nulla viene riscritto: le letture uniscono le due storie e indicano l'origine di ciascun evento.
4. Se le due storie si contraddicono con date non ordinabili, la posizione è `attention`: il sistema non sceglie d'ufficio e si risolve con una nuova raccolta o annullando il consolidamento.

Il consolidamento si può annullare con un nuovo evento.

Rappresentanze

Si registra chi può agire per conto della persona (genitore, tutore, amministratore di sostegno, delegato), con la fonte e gli estremi del documento che lo attesta (PDF facoltativo) e il periodo di validità. Alla cessazione si applica la regola del requisito: le scelte restano valide fino alla scadenza, oppure serve una nuova conferma.

Subject API

Il CRM o l'HR creano e aggiornano le persone con tre operazioni: upsert idempotente (ripetere la stessa chiamata dà `unchanged`), lettura del profilo minimo, risoluzione di un identificativo. In caso di conflitto la risposta non rivela l'identificativo del soggetto esistente: un'integrazione non scopre persone che non conosce. Archiviazione, unificazione e cambio di tipologia restano decisioni del backoffice.

Il dato anagrafico resta del sistema che lo possiede: Attesta non diventa un secondo CRM in conflitto con il primo, ma un registro che sa sempre da dove viene ogni valore.

7 Import dell'anagrafica e dello storico

Import dell'anagrafica da file

Serve al primo avvio, per caricare le persone già presenti nel CRM, e agli aggiornamenti periodici da CRM, HR o ERP. Ogni riga passa dallo stesso motore di riconciliazione della Subject API.

1. **Origine.** Si scelgono tipologia, fonte e file CSV o XLSX. Il separatore del CSV è rilevato da solo.
2. **Mapping.** Ogni colonna va su un campo, sull'ID esterno o su «Ignora». Il sistema propone il mapping quando i nomi coincidono e ripropone quello dell'ultimo import con le stesse intestazioni.
3. **Anteprima**, senza alcuna scrittura: righe da creare, aggiornare, invariate, ignorate per precedenza, duplicate nel file, in conflitto o in errore.
4. **Esecuzione in background.** Gli errori di riga non fermano il lavoro; dopo un guasto il lavoro riprende dalla prima riga non elaborata.
5. **Report per riga**, scaricabile in CSV e senza dati anagrafici. La somma degli esiti coincide sempre con le righe del file.

Limite predefinito: 50.000 righe per file. Il file caricato si cancella 30 giorni dopo la chiusura, mentre il report resta. L'import non archivia i soggetti assenti dal file.

Import dello storico di consensi e attestazioni

Un cliente parte senza perdere lo stato preesistente, per esempio i consensi marketing già nel CRM. Il principio guida: lo storico entra senza attribuirgli un livello di prova superiore a quello realmente disponibile.

- Si importano consensi, autorizzazioni, prese visione, accettazioni, dichiarazioni e revoche.
- Ogni riga valida diventa un evento con origine «importato», con la data dichiarata dalla fonte, la data dell'import e la propria evidenza nella catena.
- Il livello di prova è `none`, `declared` o `documented`; il terzo richiede almeno un artefatto (scansione del modulo, ricevuta, log), caricato in un archivio ZIP fino a 32 MB e 2.000 file.
- È il requisito a decidere se lo storico conta: `usable`, «utilizzabile se il livello è almeno L», oppure `not_usable` (predefinito). Un evento escluso resta conservato e consultabile.
- Un evento importato non si modifica né si cancella. Una correzione è una nuova riga che «corregge» la precedente. Ricaricare lo stesso file registra solo le righe nuove.

L'anteprima dice quante righe saranno utilizzabili, quante escluse per policy e quante già scadute.

> Esempio: il file del CRM contiene identificativo cliente, flag S/N, data e ID del record. S diventa `consent_granted`, N `consent_denied`, con livello `declared` e con la versione del testo usato allora caricata come versione storica. Dopo l'import la Verification API risponde `allowed` o `denied` senza una nuova raccolta. Con un `knowledge_as_of` anteriore all'import quegli eventi sono invisibili: si prova anche quando Attesta li ha saputi.

8 Documenti, ambiti, finalità e requisiti

Documenti e contenuti

Informative, policy, regolamenti e testi di consenso, autorizzazione e dichiarazione sono contenuto versionato. Chi deve agire, come e con quale prova si decide sul requisito, quindi lo stesso documento si riusa in più requisiti e per più tipologie.

- **Versioni.** Una versione è un PDF (fino a 20 MB) oppure un testo con formattazione semplice. Il ciclo di vita è bozza → attiva → superata / ritirata, con al massimo una versione efficace in ogni istante.
- **Sigillo.** All'attivazione il sistema calcola l'hash del contenuto e sigilla la versione nella catena. Contenuto e hash sono immutabili: un refuso si corregge con una nuova versione.
- **Efficacia futura.** Si attiva oggi una versione che vale dal 1° del mese; fino ad allora resta efficace la precedente.
- **Riesame e ritiro.** Una data di riesame genera un promemoria nel report delle scadenze. Il ritiro richiede una motivazione e annulla le richieste aperte su quella versione; le scelte già espresse restano valide.
- **Anteprima fedele**, con lo stesso hash che vedrà la persona.

A ogni data si dimostra quale testo era in vigore e che non è cambiato. Il contenuto di ogni versione, anche ritirata, si recupera integro per tutta la vita dell'installazione.

Nuove versioni senza sorprese

All'attivazione di una nuova versione il compliance manager sceglie due regole, valide dalla data di efficacia.

Regola	Opzioni	Predefinito
Richieste aperte	Completarle sulla versione precedente, oppure annullarle e ricrearle sulla nuova	Annulla e ricrea
Scelte già espresse	Restano valide, oppure diventano «superate» e serve una nuova azione	Nuova azione

Il dialogo riassume l'effetto in italiano corrente, per esempio: «Dal 1° ottobre le richieste aperte sulla versione 2 saranno annullate e ricreate sulla versione 3; le prese visione già raccolte sulla versione 2 non saranno più valide». Nessuna sostituzione silenziosa: chi ha accettato la versione 2 resta registrato sulla versione 2.

Versioni storiche

Prima di importare lo storico si caricano le versioni dei testi usati negli anni passati, con contenuto, date e fonte. Ricevono un hash e un sigillo con la data di caricamento, non diventano mai efficaci sopra una versione successiva, non vengono mai proposte in nuove richieste e portano ovunque l'etichetta «legacy».

Ambiti

Gli ambiti sono organizzati ad albero con codici stabili come `marketing.email`: il figlio è il codice del padre più un segmento, e codice e padre non cambiano mai. Il tipo di valutazione (`completion`, `permission`, `mixed`) è obbligatorio e la sua coerenza con i requisiti è controllata al salvataggio. Un ambito si ritira e non si cancella: interrogato dopo il ritiro risponde `scope_retired`, mai un permesso. I sistemi esterni leggono l'elenco degli ambiti dal registro pubblico e usano gli stessi codici.

Finalità

Catalogo delle finalità con codice, nome, descrizione e base giuridica descrittiva. Ogni consenso ha la sua finalità; il canale (email, SMS) si rappresenta con finalità o ambiti distinti.

Requisiti

Per ogni tipologia c'è un elenco ordinato di requisiti, nell'ordine in cui la persona vedrà le azioni. Il requisito è l'unico punto in cui vivono azione, obbligatorietà, prova, validità e policy.

Attributo	Che cosa decide
Azione e documento	Quale delle sei azioni, su quale documento. La finalità serve solo per il consenso
Obbligatorio	Se una mancanza o un esito negativo rendono la posizione incompleta
Concorre allo stato generale	Se entra nella verifica senza ambito. Il consenso marketing tipico non concorre e si valuta solo su `marketing.email`
Modalità ed effetto della mancanza	`completion` o `permission`. Per i permessi, che cosa produce una scelta mai espressa: `denied` (predefinito) o `action_required`
Livello di prova	`base` o `reinforced` con OTP, con canale preferito: email, SMS, qualsiasi
Revocabile, rifiuto ammesso	La revoca vale per consenso e autorizzazione; il rifiuto per l'accettazione
Validità in giorni	Per esempio una presa visione annuale. Alla scadenza lo stato diventa «scaduto»
Regola della sola consegna	Messa a disposizione, consegna confermata dal provider o visualizzazione
Fine della rappresentanza	Le scelte restano fino alla scadenza, oppure serve una nuova conferma
Eventi importati	Se e da quale livello lo storico conta. Predefinito: non conta
Eventi dichiarati da siti web	`usable` / `not_usable`. Predefinito: non conta. Non ammesso insieme alla prova rafforzata

Ogni modifica crea una nuova versione sigillata e il form avvisa: «Salvando crei la versione n+1». La data di efficacia può essere futura. Disattivare un requisito chiude la sua validità: le azioni pendenti diventano non applicabili, mentre eventi ed evidenze restano intatti e le verifiche a date passate continuano a vederlo. Una procedura guidata a passi crea in un'unica sessione documento, versione, finalità, ambito e requisito.

9 Motore di verifica

Il motore risponde a due domande: «questa persona è in regola?» e «per questo ambito si può procedere?». Il risultato non è un flag. Contiene i due esiti distinti, l'ambito valutato e la dichiarazione dei tempi (per esempio «efficacia al 1/3, conoscenza a oggi»), il dettaglio di ogni requisito (stato, ultimo evento con le due date, origine, livello di prova, scadenza), le azioni che servirebbero per completare e le motivazioni con codici stabili.

Lo stesso servizio alimenta la scheda nel backoffice, la Verification API, il controllo massivo e la dashboard: una sola logica, quindi una sola risposta.

Come si arriva alla decisione negli ambiti di permesso

1. Persona non trovata, ambigua o archiviata → `unknown`.
2. Nessun requisito di permesso applicabile → `denied`: l'assenza di regole non è un via libera.
3. Almeno un esito negativo (negato, revocato) → `denied`.
4. Una scelta mancante con effetto «negato» → `denied`.
5. Una scelta mancante con effetto «azione richiesta» → `action_required`.
6. Tutto soddisfatto → `allowed`.

Negli ambiti di completezza la decisione segue la completezza: `complete` → `allowed`; `incomplete` → `action_required`; `attention` e `unknown` → `unknown`.

Quando il sistema non sa

Ogni integrazione dichiara in anticipo come trattare un esito `unknown` sugli ambiti di permesso: `keep_unknown` (predefinito) lo lascia tale, `unknown_as_denied` lo trasforma in `denied` conservando il valore originario nelle motivazioni. La scelta è dell'azienda ed è tracciata. Per `marketing.email` si raccomanda il comportamento fail-closed: senza un `allowed` valido non si invia. Un timeout o un'indisponibilità non sono mai trasformati in una decisione.

La scheda della persona

Affianca completezza e decisione, ma distinte, con selettore di ambito e di data. Ha una riga per requisito, con le mancanze raggruppate come «azioni richieste», le richieste aperte, lo storico degli eventi con il collegamento alle evidenze, il pannello dei consolidamenti e il comando «Avvia richiesta» con le mancanze già preselezionate. Mentre una richiesta è aperta la scheda si aggiorna da sola ogni 5 secondi. Ogni apertura del fascicolo entra nell'audit.

Verification API

In ingresso riceve l'identificativo della persona (interno, oppure fonte + ID esterno), l'ambito, l'inclusione dei sottoambiti e una data facoltativa. In uscita restituisce i due esiti, i motivi, i requisiti valutati e le azioni richieste, senza alcun dato anagrafico. Il riferimento di prestazione è 60 chiamate al minuto con p95 sotto i 500 ms su 50.000 soggetti.

Il contratto di integrazione prescrive quattro regole: leggere `decision` per il permesso e `completion_status` per il fascicolo, senza dedurre l'uno dall'altro; trattare `scope_not_found` e `scope_retired` come errori, mai come permessi; non tenere in cache i permessi usati come gate; per le liste, non superare le 24 ore dal controllo.

Il sistema di marketing chiede «posso scrivere a questo cliente via email?» prima di ogni invio e riceve una risposta motivata e riproducibile. Se un'ispezione contesta l'invio, la stessa domanda con `as_of` alla data dell'invio dà la stessa risposta di allora.

10 Richieste e percorso del destinatario

Una richiesta è il pacchetto di azioni che una persona già nota deve compiere. È l'unità di lavoro: non il messaggio inviato, ma la richiesta assegnata alla persona, con il suo stato, le sue azioni e le sue prove.

Da dove nasce

- **Dalla scheda della persona.** Attesta compone il pacchetto da sola: preseleziona i requisiti mancanti (mai espressi, scaduti, superati), rende selezionabili ma non preselezionati quelli negati o revocati, mostra come informazione quelli soddisfatti, esclude con il motivo quelli senza un testo in vigore.
- **Da un modello di richiesta**, preparato dal compliance manager: precompila requisiti, canale, schermo del desk e OTP di conferma. L'operatore può comunque cambiare tutto.
- **Da un sistema esterno**, con la Distribution API: crea la richiesta, ottiene il link o il QR, chiede un invio e legge lo stato. È idempotente.
- **Da una distribuzione massiva** e **dal self-service**, quando la persona vuole ridare un consenso.

Una richiesta aperta sullo stesso requisito non si duplica.

Come arriva alla persona

Canale	Uso tipico e comportamento
QR dinamico a schermo	Allo sportello. QR grande con conto alla rovescia di 15 minuti, monouso, rigenerabile. Il token esiste solo come hash
Link via SMS	Per chi non è presente o preferisce rispondere dopo. Messaggio neutro con mittente, link e scadenza; il link vale 7 giorni
Link via email	Dipendenti, fornitori, invii massivi. Template con il marchio del cliente; nessun titolo di documento e nessun nome nel messaggio
Indirizzo restituito via API	Portali e applicazioni dell'azienda che ospitano l'ingresso al percorso

Ogni invio registra recapito mascherato, fonte e stato di verifica. La consegna segue gli stati inviato → consegnato / fallito, con l'orario del provider. Una consegna fallita è evidenziata all'operatore, non cambia lo stato della richiesta e si può reinviare, anche su un altro recapito o canale.

Allo sportello, in diretta

1. L'operatore apre la scheda del cliente, crea la richiesta e mostra il QR.
2. Il cliente lo inquadra con il proprio telefono e la scheda segna «in corso».
3. Ogni azione risolta compare con il suo esito, con l'indicazione «aggiornato alle hh:mm:ss».
4. Al completamento la scheda ricalcola completezza e decisione senza una nuova ricerca.

Il cliente usa il proprio telefono: niente tablet condivisi, niente firme su carta da scansionare. L'operatore sa in pochi secondi se può procedere.

Il percorso della persona

Le pagine sono mobile-first, con il marchio dell'azienda, conformi a WCAG 2.1 AA e usabili anche da desktop.

1. **Accoglienza.** «L'organizzazione X ti chiede di completare N attività», con la scadenza. Prima di questo punto non compare nessun dato personale.
2. **«Confermiamo che sei tu».** La persona vede i dati configurati come visibili, mascherati, e completa quelli mancanti modificabili. Con «Non sono io» la sessione si chiude senza registrare nulla.
3. **Elenco delle attività**, completabili in qualunque ordine, con tipo e stato scritti per esteso.
4. **Pagine delle azioni.** Il documento si legge nella pagina, anche il PDF. Ogni scelta usa comandi espliciti non preselezionati.
5. **Riepilogo delle scelte.** Con più scelte, le si rivede tutte e le si registra con un solo comando: un evento e un'evidenza per ciascuna, «tutto o niente».
6. **Codice OTP**, se la prova rafforzata lo richiede: uno solo per tutte le scelte della sessione.
7. **Pagina finale** con ciò che è stato registrato e la data. Per email arriva una ricevuta con il collegamento al self-service; dopo un percorso confermato via SMS, il link personale all'area riservata.

Un percorso interrotto si riprende dallo stesso dispositivo finché il link è valido. Il link aperto da un altro dispositivo è rifiutato con un messaggio neutro.

Gestione delle eccezioni

- **Scadenza.** Predefinita a 30 giorni, modificabile per richiesta. Alla scadenza le scelte già registrate restano valide.
- **Annullamento.** Con motivazione obbligatoria; la persona riceve un messaggio neutro e i link sono revocati.
- **Nuova versione del testo** durante una richiesta aperta: si applica la regola scelta all'attivazione.
- **Problema tecnico.** «La tua scelta non è stata registrata. Riprova». Non è mai contato fra i rifiuti; si riprende alla riapertura del link o con il comando «Riprendi» dell'operatore.
- **Rappresentante.** Il genitore o il tutore agisce dal QR «per conto di» la persona. L'evento registra entrambi; se la rappresentanza cessa prima della conferma, la conferma è rifiutata.

Stati della richiesta: `available`, `in_progress`, `completed` (nessuna azione aperta, anche con esiti negativi), `expired`, `cancelled`, `technical_error` (recuperabile), `draft` (solo per le distribuzioni massive). Stato della consegna, stato della richiesta e stato delle singole azioni sono tenuti e mostrati separatamente.

11 Self-service e revoca

La persona rivede e revoca le proprie scelte da sola, senza account né password. La revoca vale subito: la verifica successiva, anche via API, ne tiene già conto. Esercitare il diritto di revoca è facile quanto dare il consenso, con la stessa forza probatoria.

Accesso

1. Nella pagina pubblica la persona sceglie email o cellulare e inserisce il recapito.
2. La risposta è sempre la stessa: «Se il recapito è registrato ti abbiamo mandato un codice». Non rivela mai chi è censito.
3. Se il recapito appartiene a una persona attiva, arriva un PIN sullo stesso canale, senza link, con la stessa politica dell'OTP: 6 cifre, 5 minuti, 5 tentativi.
4. Il PIN corretto apre una sessione di 30 minuti che vale già come prova rafforzata.

Dopo un percorso confermato via SMS la persona riceve anche un link personale all'area riservata. Il link non scade, ma da solo non apre nulla: chiede comunque il PIN.

Area personale

- **Le tue scelte:** consensi e autorizzazioni con stato attuale (concesso, negato, revocato, scaduto, nuova versione disponibile), data, versione del testo e revocabilità.
- **Documenti:** prese visione, accettazioni e conferme con versione e data; le sole consegne come «consegnato il...».
- **Storico** delle proprie scelte, con l'origine: da richiesta, da self-service, archivio precedente, modulo online.
- **Download** della versione esatta su cui la persona ha agito, anche se oggi superata, con hash coincidente con la prova.

Revoca

Si revocano i consensi e le autorizzazioni revocabili e attivi, con un comando esplicito, per esempio «Revoco il consenso a...». La revoca è un nuovo evento che cita la scelta revocata, con la sua evidenza in catena; la scelta originale resta. Parte una conferma via email o SMS, e se l'invio fallisce la revoca resta valida.

Sul consenso marketing, dopo la revoca la posizione resta `complete` e la decisione su `marketing.email` diventa `denied` con motivo «revocato». Il sistema di marketing lo vede alla prima interrogazione successiva.

Ridare il consenso

Per un consenso negato, revocato, scaduto o superato la persona può chiedere di esprimerlo di nuovo. Attesta crea una richiesta con una sola azione e la porta nel percorso del destinatario, con le stesse regole di prova. Nel self-service non si passa mai direttamente da «negato» ad «attivo».

12 Evidence vault: il registro delle prove

L'evidence vault conserva, in modo append-only e verificabile, la prova di ciò che la persona (o chi agisce per lei) ha espresso e del contesto in cui lo ha fatto. Non interpreta e non calcola stati: registra, concatena, conserva, verifica ed esporta. Non cancella e non corregge mai niente.

Che cosa contiene un'evidenza

Blocco	Contenuto
Evento	Tipo, quando è accaduto, quando è stato registrato, origine (nativa, importata, self-service, integrazione)
Chi	Soggetto ed eventuale actor, con la rappresentanza valida in quel momento
Regole	Requisito com'era al tempo dell'evento, con il riferimento al sigillo della sua versione
Contenuto	Documento, versione, hash e una copia propria del contenuto mostrato
Gesto	Il testo esatto del pulsante confermato; per le dichiarazioni, i valori confermati così come mostrati
Sessione	Canale di accesso (QR, link, self-service), livello di autenticazione, recapito mascherato, dati dell'OTP
Contesto tecnico	User agent e indirizzo IP
Integrità	Numero progressivo, hash del record, hash del record precedente

I valori descrittivi restano quelli al tempo dell'evento e non si aggiornano mai. Anche consegne, visualizzazioni e ogni attivazione di configurazione (versioni di documenti, requisiti, ambiti, rappresentanze, tipologie) entrano nella catena.

La catena, in parole semplici

Ogni registrazione è un anello numerato. Contiene l'impronta SHA-256 del proprio contenuto e quella dell'anello precedente: se qualcuno modifica, toglie o inserisce un anello, le impronte successive non tornano più e il punto di rottura si individua. L'ordine è quello di registrazione: un consenso del 2023 importato oggi è l'anello di oggi, con la data del fatto dichiarata nel manifest, così la storia consolidata non si riscrive.

A questo si aggiunge il database: l'utenza applicativa non ha i permessi di modifica né di cancellazione sulle tabelle probatorie, e un test lo verifica.

Controlli di integrità

- **Controllo della catena** ogni giorno, sull'intera installazione.

- **Controllo profondo progressivo:** ogni evidenza è ricontrollata integralmente, artefatti compresi, almeno una volta ogni 30 giorni, a blocchi e non a campione. La copertura è dichiarabile.
- **Verifica su richiesta** di un record o della catena, riservata a compliance manager e auditor, con la tabella elemento per elemento: hash atteso, hash ricalcolato, esito.

Gli esiti sono tre: `ok`; `alterata` (discordanza, anello mancante, oppure artefatto assente da uno storage che risponde); `non_verificabile` (lo storage non risponde: un allarme operativo, non di manomissione). Tenerli distinti evita di dare l'allarme a ogni manutenzione, o di non darlo quando una prova è persa davvero.

Pacchetto probatorio

Per una persona (con le posizioni unificate) o per una richiesta si scarica uno ZIP con il manifest leggibile, un manifest per evidenza, le copie dei contenuti, le ricevute OTP e gli artefatti storici, la posizione in catena e la radice della catena al momento dell'export, e un file di istruzioni.

Il manifest è firmato con Ed25519 con una chiave dedicata dell'installazione, che non esce mai dal gestore di segreti. Le chiavi pubbliche, anche quelle ritirate, restano pubblicate con il loro periodo di validità. La verifica si fa fuori da Attesta, senza strumenti forniti: si ricalcolano gli hash con `sha256sum`, si confrontano con il manifest, si controlla la concatenazione dei record, si verifica la firma con una libreria standard. Ogni export entra nell'audit.

Atomicità

Evento, evidenza, anello di catena e chiusura dell'azione stanno nella stessa unità di lavoro. Se l'evidenza non si scrive, l'evento non esiste e la persona vede un problema tecnico, mai un esito negativo. Non esiste un consenso senza la sua prova.

13 Notifiche e OTP

Email e SMS raggiungono la persona fuori dall'applicazione, con un fornitore per canale dietro un adattatore: il cuore del prodotto non dipende dal fornitore. L'amministratore tecnico abilita o disabilita ciascun canale.

Messaggi

I template sono fissi, con il marchio del cliente: invito alla richiesta, codice OTP, ricevuta (solo email), conferma di revoca, richiesta annullata, link personale all'area riservata (SMS). Il contenuto è minimo e neutro: niente nome della persona, titoli di documenti, finalità o esiti. L'invito riporta solo il numero di attività e la scadenza, e il link contiene solo un token opaco.

La consegna è una prova. Ogni transizione (inviato, consegnato, fallito) è un evento append-only con l'orario del fornitore e quello di Attesta. «Consegnato» vale solo su conferma del fornitore e può soddisfare un requisito di sola consegna. Un esito tardivo entra con il proprio orario; un «non consegnato» dopo un «consegnato» viene registrato ma non fa regredire la consegna.

OTP e controllo dei costi

Parametro	Valore predefinito
Codice	6 cifre, valido 5 minuti, 5 tentativi, conservato solo come hash
Nuovo invio	Dopo 60 secondi; il nuovo codice annulla il precedente
Blocco dopo i tentativi esauriti	15 minuti
Tetti di emissione	5 per sessione; per recapito 5 all'ora e 10 al giorno; per IP 20 all'ora

L'OTP va solo a recapiti già noti prima della sessione, mai a un numero digitato nella pagina. Se manca il recapito preferito si usa l'altro canale abilitato. Se il codice non è consegnabile, la persona vede un problema tecnico, distinto da una scelta. I tetti proteggono dall'abuso degli SMS (SMS pumping) e la risposta oltre il tetto è neutra.

Il pannello tecnico mostra SMS e OTP inviati per ora, giorno e mese, con soglie di allarme. L'anteprima di una distribuzione dichiara quanti SMS partiranno.

14 Controllo massivo e distribuzione massiva

Controllo massivo

Verifica un elenco di persone o di operazioni, caricato da file, avviato dal backoffice o inviato da un sistema esterno via Batch API, e restituisce un risultato riga per riga più un report aggregato. Usa esattamente il motore del controllo singolo: la risposta è la stessa, perché la logica è una sola.

Esempio: il CRM esporta i 12.000 destinatari della newsletter con l'identificativo e il codice della campagna, avvia il controllo sull'ambito `marketing.email`, scarica il risultato e invia la campagna solo alle righe `allowed`. Il compliance manager esporta le eccezioni e le usa come elenco di una distribuzione per raccogliere i consensi mancanti.

- **Il file.** CSV o XLSX con intestazioni fisse. Ogni riga indica la persona con identificativo interno, con fonte + ID esterno, oppure con tipologia + campo univoco + valore; facoltativamente ambito, data passata per la verifica retrospettiva e un riferimento libero (fattura, campagna, pratica) restituito tal quale. Limite: 50.000 righe, configurabile, elaborate entro un'ora senza rallentare la verifica in tempo reale.
- **Esiti.** Ogni riga porta `completion_status` e `decision`, l'ambito, i tempi applicati e, per ogni requisito mancante o negativo, lo stato e l'origine dell'ultimo evento. Una riga malformata o con un ambito inesistente è in errore: non produce un esito e non blocca il lavoro. Un refuso non diventa mai un permesso.
- **Report aggregato** con totali per esito, righe in errore per codice e `unknown` trasformati dalla policy dell'integrazione. Si filtra e si esporta in CSV; ogni export entra nell'audit.
- **Istante di riferimento unico:** l'avvio del lavoro, per tutte le righe. Un lavoro di un'ora è coerente e ripetibile, e dopo un guasto riprende sulle righe mancanti con lo stesso istante.

Distribuzione massiva

Il compliance manager raggiunge migliaia di persone, ma senza scorciatoie: ogni persona ha la propria richiesta, il proprio link, i propri eventi e la propria prova. Non esiste un evento collettivo che li sostituisca.

1. **Chi.** Una tipologia, con filtri sui campi ricercabili, oppure un elenco da file.
2. **Cosa.** Uno o più requisiti, con tutte e sei le azioni ammesse.
3. **Come.** Canale email oppure SMS, e scadenza (predefinita 30 giorni).
4. **Anteprima** calcolata su tutta la popolazione: richieste da creare e da riusare, esclusi perché già in regola, esclusi perché hanno già detto no, persone senza recapito del canale, archiviati e posizioni unificate, righe dell'elenco senza corrispondenza, SMS previsti per controllare i costi.
5. **Conferma.** Attesta crea e consegna le richieste in background; la pagina si può lasciare.
6. **Monitoraggio** in tempo quasi reale, con contatori separati per consegna, completamento e scelte negative. Da ogni richiesta si reinvia una consegna fallita.

Regole che proteggono il cliente:

- **A ciascuno solo ciò che gli manca.** Chi è già in regola non riceve nulla. Chi ha detto no non riceve nulla: la distribuzione non serve a insistere con chi ha rifiutato.
- **Nessun doppione.** Una richiesta già aperta, per esempio creata al desk, viene riusata con un nuovo link. Dopo un guasto si riprende sui soli destinatari rimasti.
- **Annullamento rispettoso.** Si annullano le richieste non ancora aperte; quelle già aperte restano attive e le scelte già registrate restano valide.
- **Report per destinatario** con esito e motivo di esclusione, in CSV e con recapito mascherato. Ogni download entra nell'audit.

Limiti predefiniti: 50.000 destinatari; link valido 7 giorni; file dell'elenco cancellato 30 giorni dopo la chiusura.

15 Dashboard e report

Il cockpit risponde a colpo d'occhio alle domande di chi risponde della compliance: quante persone sono in regola, quante sono contattabili via email, quante richieste dal desk sono andate a buon fine. Non calcola stati propri: ogni numero deriva da eventi e configurazioni ed è ricostruibile.

Vista	Che cosa mostra
Dashboard generale	Persone per completezza, per tipologia e per ambito. Negli ambiti di permesso, la decisione con i «negato» distinti per causa: negato, revocato, scaduto, mai espresso. Richieste per stato, consegne fallite non recuperate. Ogni numero apre l'elenco già filtrato
Report per documento e versione	Destinatari, messe a disposizione, consegne, visualizzazioni, prese visione, accettazioni e rifiuti, consensi e dinieghi, revoche. I mancati completamenti sono divisi fra richieste aperte, scadute e annullate. Consegna e visualizzazione non sono mai presentate come presa visione

Vista	Che cosa mostra
Fascicolo della persona	Cronologia completa con le due date, richieste, consegne, consolidamenti, rappresentanze ed evidenze
Elenchi di lavoro	Persone incomplete, da verificare o sconosciute, con le azioni che servono e il comando «Crea richiesta» già precompilato
Scadenze	Scelte in scadenza, documenti da riesaminare, richieste che stanno per scadere (predefinito: 30 giorni)
Storico delle azioni	Tutte le scelte registrate, filtrabili per periodo, finalità, origine e livello di prova
Richieste e consegne	Esiti di invio per canale, per origine (desk, API, distribuzione) e per distribuzione
Consolidamenti	Posizioni unificate, da chi, con quale motivazione e quali conflitti hanno generato
Consensi cookie	Andamento di consensi e rifiuti del banner del sito, con export (capitolo 17)

I conteggi sulla popolazione vengono da una fotografia ricalcolata ogni notte e su richiesta; la dashboard dichiara «dati aggiornati al…» e avvisa se nel frattempo la configurazione è cambiata. Le altre viste leggono gli eventi in tempo reale.

Ogni elenco si filtra, si ordina e si esporta in CSV con le sole colonne che il ruolo può vedere; ogni export entra nell'audit. Il CSV di un elenco di lavoro si carica così com'è come elenco di una distribuzione. L'amministratore tecnico vede solo numeri aggregati, senza dettaglio.

16 Accettazioni raccolte da siti web

Molte organizzazioni raccolgono consensi e accettazioni anche dai moduli dei propri siti: iscrizione alla newsletter, form di contatto, area clienti. Attesta li porta nel registro in due modi, con garanzie diverse e dichiarate.

Modello	Funzionamento	Prova
A. Passaggio ad Attesta	Il sito crea la persona e la richiesta con la Distribution API, anche da un modello di richiesta, e passa la persona al percorso di Attesta	Nativa: `base`, oppure `reinforced` con OTP. È il modello per i requisiti che chiedono una prova forte
B. Spunta nel modulo del sito	Il sito raccoglie la spunta e la dichiara ad Attesta, che registra l'evento	`integration_declared`: inferiore a `base`, mai innalzata. Attesta registra la dichiarazione del sito, non la scelta

Le garanzie del modello B

- **Spento per default.** Il compliance manager abilita l'uso di questi eventi requisito per requisito. Non è ammesso su un requisito che chiede l'OTP. Un invio su un requisito non abilitato è rifiutato e non lascia traccia.
- **Controllo del testo.** Il sito invia l'hash della versione mostrata; se non è quella in vigore alla data dichiarata, l'invio è rifiutato. Il sito legge testi e requisiti dal catalogo (capacità `catalog_read`).
- **Solo scelte esplicite.** Una spunta assente non è mai un rifiuto. Il «no» si registra solo da un sì/no esplicito. Sono ammessi consenso, autorizzazione, accettazione e presa visione.
- **Finestra di 24 ore** sulla data dichiarata, mai nel futuro. Le scelte più vecchie passano dall'import storico. L'idempotenza è obbligatoria.
- **Difese contro una chiave rubata.** Capacità dedicata (`acceptance_record`), elenco dei modelli consentiti, restrizione per indirizzo IP obbligatoria, policy controllata sia alla data dichiarata sia alla ricezione: spegnerla non si aggira retrodatando.
- **Manifest trasparente.** Separa ciò che Attesta ha osservato (integrazione autenticata, IP della chiamata, ora), ciò che il sito ha dichiarato e Attesta ha controllato (modello, hash del testo) e ciò che il sito ha soltanto dichiarato (modulo, testo della spunta, ora, IP e browser della persona).
- **Revoca dal self-service**, come ogni altra scelta.

Persone già censite: doppio opt-in

Se un modulo anonimo contiene un dato che coincide con una persona già censita, Attesta non aggancia la scelta e non modifica i dati: nessuno può dare un consenso a nome di un altro scrivendone l'email. Attesta invia invece una richiesta (modello A) solo a un recapito già noto che coincide con quello del modulo, al massimo 3 volte al giorno. Il sito riceve sempre la stessa risposta neutra.

Limiti dichiarati

L'hash prova che il sito aveva il testo giusto, non che lo abbia mostrato. Che la spunta non fosse preselezionata è un obbligo del contratto di integrazione, che Attesta non può verificare. I limiti sono dichiarati al cliente perché fanno parte della prova.

17 Banner cookie e registro dei consensi del sito web

Il banner cookie dei siti istituzionali è integrato con Attesta: ogni scelta del visitatore diventa un record conservato lato server, consultabile ed esportabile, che prova che il consenso è stato dato o negato e quando (GDPR art. 7(1) e art. 5(2), principio di responsabilizzazione).

Il banner cookie

Il banner è basato su FidesJS, la libreria open source di consenso cookie, già attivo sui siti del cliente. Presenta le categorie di cookie con testi in italiano, offre «Accetta tutti», «Rifiuta tutti» e il pannello delle preferenze, e consente di rivedere la scelta in qualsiasi momento dall'icona dedicata. Gli script delle categorie non consentite non vengono attivati. Il segnale Global Privacy Control del browser è rispettato: un visitatore che lo ha attivo riceve un opt-out automatico alla prima visita, e anche questo passa dal registro.



Che cosa registra il registro

Ogni scelta (accetta tutti, rifiuta tutti, salva preferenze, opt-out automatico GPC) produce un nuovo record. La revoca è un record con le categorie a `false`, quindi la storia delle scelte di un visitatore si ricostruisce per intero. Il rifiuto è un dato da registrare quanto l'accettazione.

Dato	Contenuto
`event_id`, `record_id`	Identificativo unico del record, generato dal browser; un invio ripetuto dello stesso record viene scartato dal server
`device_id`	Identificativo del dispositivo creato dal banner, stabile per la durata del cookie (365 giorni). È l'ID consenso mostrato al visitatore e la chiave per ricostruire la storia delle sue scelte
`received_at`, `client_time`	Ora del server in UTC, che fa fede, e ora del dispositivo, solo indicativa
`method`	Come è stata fatta la scelta: `accept`, `reject`, `save`, `gpc`
`consent`	Mappa categoria → `true` / `false`, con le categorie del sito (per esempio `analytics`, `marketing`)
Versione del banner	Identificativi di versione di configurazione e notice, più l'impronta SHA-256 del banner mostrato: provano *che cosa* è stato detto al visitatore

Dato	Contenuto
`site_config_version`	Versione di ciò che il visitatore vede ma sta fuori dal banner (interruttori, pre-selezioni, colori)
Pagina e lingua	Origine del sito e percorso della pagina, senza query string né frammento; lingua del banner
`ip_anon`, `user_agent`	IP troncato dal server prima di qualunque scrittura (IPv4 /16, IPv6 /32); user agent della richiesta
`consent_group`, `propagated_from`	Gruppo di siti di appartenenza e, per le scelte propagate fra domini, il record di origine

Secondo il principio di minimizzazione il registro non conserva l'IP completo, la query string, il referrer, altri cookie né alcun identificativo che leghi il record a una persona (email, account). Il registro non collega mai un `device_id` a un soggetto del dominio documentale di Attesta: sono due registri distinti.

Come funziona nel browser

Il banner invia il record al collector di Attesta nel momento esatto in cui salverebbe la scelta, senza attendere la rete: l'invio non rallenta il banner né lo sblocco degli script consentiti. Se il collector è irraggiungibile o una estensione del browser blocca la richiesta, il banner funziona comunque e non mostra errori al visitatore. L'integrazione si attiva per sito: con il registro disattivato il banner si comporta esattamente come prima.

I parametri `fides_*` dell'indirizzo della pagina sono filtrati prima dell'avvio del banner: un link non può dare il consenso al posto del visitatore né impedire la registrazione della sua scelta. L'unica eccezione è la propagazione fra siti dello stesso gruppo.

L'ID consenso del visitatore

La pagina cookie del sito mostra «ID del tuo consenso» e la data dell'ultima scelta, così il visitatore può citarli in una richiesta. La ricerca per ID nell'area di consultazione restituisce l'intera storia delle sue scelte.

Funzioni del registro

Funzione	Descrizione
Ricezione	Endpoint pubblico del modulo, separato dalle API di Attesta, con percorso dal nome neutro. Risponde sempre in modo neutro e registra i rifiuti come eventi di sicurezza, così chi prova non scopre quali siti esistono
Validazione e anti-abuso	Sito presente in anagrafica, origine ammessa, schema valido, dimensione massima, limite di frequenza per IP. I record da origini di sviluppo sono accettati solo su siti marcati di prova
Anonimizzazione	Troncamento dell'IP prima di ogni scrittura, compresi i log del server web
Conservazione	Parametro di installazione, predefinito 365 giorni, con valore diverso per sito. Un job giornaliero cancella i record scaduti, anche se nessuno apre l'area di consultazione. Un anno copre esattamente la vita del cookie del banner

Funzione	Descrizione
Sospensione della cancellazione	In caso di contestazione o richiesta di un'autorità si sospende la cancellazione per un sito o per un `device_id`, con motivo, autore e data
Consultazione	Area riservata: ricerca per ID consenso, sito, intervallo di date, metodo. Il dettaglio mostra la versione del banner vista dal visitatore
Archivio versioni del banner	Per ogni impronta si conserva il banner (testi e categorie) e per ogni versione la configurazione del sito, finché esiste un record che la cita
Export	CSV per sito e periodo, con formato documentato, con gli stessi filtri del grafico: si esporta quello che si vede. Estrazione per ID consenso per le richieste dell'interessato
Anagrafica siti	Per ogni sito: chiave pubblica, origini ammesse, conservazione, ambiente (produzione o prova), referente
Grafico dei consensi	Vedi sotto
Monitoraggio	Controllo periodico dell'endpoint e avviso «nessun record dal sito X da N giorni», con soglia impostabile per sito

Grafico dei consensi

Nella stessa pagina dell'export, l'andamento giornaliero di consensi e rifiuti per sito, calcolato direttamente dai record.

- **Filtri:** sito (con le origini raggruppate, per esempio il dominio con e senza `www`), data di inizio e di fine. Predefinito: ultimi 30 giorni.
- **Serie:** consensi (almeno una categoria non necessaria a `true`) e rifiuti (tutte a `false`), con i totali del periodo e, per i consensi, il dettaglio per categoria. I rifiuti automatici GPC sono contati fra i rifiuti ma riconoscibili in legenda.
- **Giorno** calcolato sull'ora italiana (Europe/Rome), anche se i record sono salvati in UTC. Oltre circa 90 giorni un punto per settimana, oltre circa un anno un punto per mese.
- **Ambiente:** i siti di prova sono esclusi di default.
- **Riepilogo** con la percentuale di consensi e rifiuti sul periodo, e una tabella con gli stessi numeri sotto il grafico, leggibile anche senza il grafico.

Più siti dello stesso cliente

Caso	Esempio	Come lo gestisce il registro
Siti indipendenti, ciascuno con il suo consenso	Due domini con banner e scelte separate	Un sito per riga in anagrafica, ciascuno con la propria chiave. Il grafico si filtra per sito o li somma
Sottodomini con consenso condiviso	`www`, `shop`, `careers` dello stesso dominio	Il banner scrive il cookie sul dominio principale, quindi la scelta vale su tutti. Un gruppo in anagrafica con le origini dei sottodomini; lo stesso ID consenso compare su tutti e ricostruisce la storia del gruppo

Caso	Esempio	Come lo gestisce il registro
Sottodomini con consenso separato	Sottodominio con scelte proprie	Un suffisso di cookie diverso per sottodominio mantiene i consensi indipendenti

Accesso al registro

Il registro è per installazione: riguarda i siti istituzionali del cliente titolare di quell'installazione. Si accede con gli utenti e i ruoli di Attesta, con TOTP obbligatorio.

Operazione	Compliance manager	Auditor	Amministratore tecnico	Operatore
Elenco e dettaglio dei siti	Lettura	Lettura	Lettura	—
Creazione, modifica e sospensione dei siti	—	—	Scrittura	—
Consultazione e ricerca dei record, anche per ID consenso	Lettura	Lettura	—	—
Grafico	Lettura	Lettura	Solo conteggi aggregati	—
Export CSV ed estrazione per l'interessato	Export	Export (CSV)	—	—
Sospensione della cancellazione	Scrittura	—	—	—
Modifica o cancellazione manuale di un record	—	—	—	—

Nessun ruolo può modificare o cancellare un record: l'unica cancellazione è la scadenza automatica. Consultazione, ricerca, export, sospensione della cancellazione e modifiche ai siti producono un evento di audit. Dell'audit entrano solo il fatto, il sito, i filtri non identificativi e il numero di risultati, mai l'ID consenso cercato. Con il registro spento nessuna voce di menu e nessuna rotta è raggiungibile, compresa quella del browser. La schermata «Stato dell'installazione» include un blocco con siti, ultimo record ricevuto e avvisi di inattività.

Valore di prova nel tempo

Il registro serve a dimostrare un consenso anche a distanza di mesi. Per questo:

- backup periodici cifrati con prova di ripristino, e scadenza anche per le copie, così che la conservazione valga per il database e per i backup;
- le versioni del banner e della configurazione durano quanto i record che le citano;
- login con TOTP e registro degli accessi su ogni consultazione;
- sospensione della cancellazione in caso di contestazione;
- hosting nell'Unione europea.

18 Ruoli e permessi

Quattro ruoli fissi, uno per utente. L'autorizzazione è deny-by-default: un'operazione non esplicitamente consentita è negata dal backend, anche se qualcuno ne conosce l'indirizzo. L'interfaccia nasconde ciò che il ruolo non può fare, ma la protezione vera sta nel backend.

Ruolo	Che cosa fa
Compliance manager	Governa tipologie, campi, fonti, documenti, ambiti, finalità, requisiti e modelli di richiesta. Gestisce soggetti, consolidamenti, rappresentanze, import, distribuzioni e controlli massivi. Verifica ed esporta le prove e gestisce il registro dei consensi cookie
Operatore	Al desk: cerca, consulta la scheda, crea e modifica soggetti senza archiviarli, crea e segue le richieste. Vede le evidenze nel fascicolo, senza esportarle
Auditor	In sola lettura su tutto: storico, evidenze, report, consolidamenti, audit, log, registro cookie. Ricostruisce il passato, verifica la catena, esporta prove, report e audit. È l'unico che esporta l'audit
Amministratore tecnico	Installazione, parametri, marchio, utenti e ruoli, canali di invio, integrazioni, siti del registro cookie. Non vede dati personali né prove, nemmeno aprendo l'indirizzo diretto

Matrice sintetica

Legenda: S scrittura · L lettura · E export · A solo dati aggregati · — nessun accesso.

Area	Amm. tecnico	Compliance	Operatore	Auditor
Configurazione, marchio, utenti	S	L	L	L
Integrazioni	S	L	—	L
Soggetti: ricerca e scheda	—	L	L	L
Soggetti: creazione e modifica	—	S	S	—
Archiviazione, consolidamento	—	S	—	L
Import anagrafico e storico	A	S	—	L
Documenti, requisiti	L	S	L	L
Richieste	—	S	S	L
Distribuzioni	—	S / E	L (stato)	L / E
Evidenze: lettura	—	L	L	L
Evidenze: export e verifica di catena	A (esito)	E / S	—	E / S
Dashboard	A	L	L	L

Area	Amm. tecnico	Compliance	Operatore	Auditor
Export CSV dei report	—	E	—	E
Controllo massivo	—	S / E	L	L / E
Registro consensi cookie	A	L / E / S	—	L / E
Audit	L limitata	L	—	L / E

Nessun ruolo può modificare o cancellare evidenze, eventi, configurazioni sigillate o audit. L'assegnazione dei ruoli che danno accesso alle prove è tracciata e il dialogo lo avverte.

19 Integrazioni e API

Ogni sistema esterno è un'Integration registrata dall'amministratore tecnico, con un codice di fonte immutabile, una chiave API e un insieme di capacità abilitate una per una sul principio del minimo privilegio. Il sistema esterno interroga Attesta e la revoca è visibile alla prima interrogazione successiva.

Capacità	A che cosa serve
`subject_upsert`	Subject API: creare e aggiornare le persone dal CRM o dall'HR
`scope_read`	Registro degli ambiti: leggere i codici validi
`verification`	Verification API: chiedere se si può procedere per una persona e un ambito
`distribution`	Distribution API: creare richieste, ottenere il link o il QR, chiedere un invio, leggere lo stato
`batch`	Batch API: controllo massivo di migliaia di righe
`catalog_read`	Catalogo: tipologie, campi visibili, modelli di richiesta, requisiti, testi in vigore con l'hash
`acceptance_record`	Registrare le accettazioni dichiarate da un sito; restrizione per IP obbligatoria

- La chiave API è opaca, mostrata una sola volta e conservata solo come hash. Si ruota a mano con revoca immediata della precedente. L'integrazione si sospende e non si cancella.
- Le API sono versionate (`/api/v1`) e documentate in OpenAPI. Dentro una versione si aggiunge, non si rimuove e non si cambia il significato.
- Le creazioni sono idempotenti: ripetere una chiamata non crea doppioni.
- Gli errori usano il formato standard RFC 9457, con codici stabili e senza dettagli interni.
- Ogni chiamata, anche rifiutata o con una chiave sconosciuta, lascia una riga di log con esito e durata, senza dati personali, conservata 90 giorni.
- Il contratto di integrazione consegnato al cliente dichiara il comportamento su errore (`fail_closed` raccomandato per `marketing.email`), vieta la cache sui permessi usati come gate e fissa l'uso corretto dei due esiti.

20 Sicurezza, privacy e conformità

Attesta protegge, in quest'ordine: l'integrità delle prove (una prova alterata non si ricostruisce e farebbe dubitare di tutte le altre), la riservatezza dei dati personali (sono dati dei clienti del cliente, che non hanno scelto Attesta), il materiale crittografico (con la chiave del sigillo si fabbricherebbero pacchetti credibili) e la disponibilità.

Area	Misura
Isolamento	Installazione dedicata per cliente. Database, storage, gestore delle chiavi e cache non sono raggiungibili da Internet
Cifratura	Cifratura applicativa di ogni dato riferibile a persona e di ogni contenuto, oltre a quella dei dischi. Chiavi in un gestore di segreti separato (Vault), mai in file o configurazioni. Una chiave per ogni uso (dati, indice di ricerca, sigillo, segreti TOTP); rotazione ogni 365 giorni senza fermo
Ricerca senza esporre	Indice cieco per la ricerca esatta sui dati cifrati. Gli hash probatori si calcolano sul dato in chiaro, così la rotazione delle chiavi non tocca la prova
Append-only	L'utenza applicativa del database non ha `UPDATE` né `DELETE` sulle tabelle probatorie, e un test lo verifica
Accessi	TOTP, blocco dopo 5 tentativi, messaggi neutri, sessioni a scadenza, autorizzazione deny-by-default, segregazione dell'amministratore tecnico
Pagine pubbliche	Token solo come hash e legati al primo browser, limiti di frequenza, anti-enumerazione, tetti OTP, CSP con nonce, TLS con HSTS
Log	Solo ciò che un'allowlist consente: mai dati personali, token, OTP, chiavi o password. Recapiti solo mascherati
Ambienti	Solo dati sintetici fuori dalla produzione. I componenti di prova sono ammessi solo in sviluppo: una configurazione che li chieda altrove ferma l'avvio

Conformità

- **Linee guida AgID per lo sviluppo del software sicuro. Progetto verificato punto per punto rispetto alle linee guida AgID.** La verifica ha coperto prescrizione per prescrizione i quattro allegati ed è accompagnata da threat model, profilo di rischio e specifica dei requisiti di sicurezza. L'esito è un impianto solido, con conformità parziale e un piano di 26 azioni di miglioramento.
- **GDPR.** Il prodotto supporta il titolare con la prova del consenso e della revoca, la minimizzazione nei messaggi e nei report e l'accesso dell'interessato alle proprie scelte. Fornisce documenti di supporto alla valutazione d'impatto. Il registro dei consensi cookie va citato nell'informativa del sito e nel registro dei trattamenti del titolare (art. 30).
- **Ruoli privacy.** Il cliente è titolare. Chi gestisce l'installazione ha per il registro cookie lo stesso ruolo che ha per il resto di Attesta.

Che cosa Attesta non è

- Non è un sistema di firma elettronica qualificata né di marcatura temporale di terze parti: produce evidenze, non firme.
- Non è un sistema di conservazione a norma.
- Non identifica legalmente la persona: l'OTP prova il controllo di un recapito.
- Non è un DMS: i documenti sono contenuti versionati da mostrare, senza workflow editoriali.

21 Modello di erogazione e parametri

Installazione dedicata per cliente: istanza, database MySQL, object storage S3-compatibile, Vault e Redis propri. Il provisioning è automatizzabile. Il backend è Laravel su PHP, con API REST; tre interfacce web separate (backoffice, percorso del destinatario, self-service) sono realizzate in React e TypeScript. L'invio usa un fornitore per canale: SMTP per l'email, un fornitore SMS; le credenziali sono segreti dell'installazione. L'interfaccia è in italiano, con tutti i testi in cataloghi traducibili. Il registro dei consensi cookie condivide lo stesso stack e la stessa installazione.

Il contratto si traduce in feature flag impostati al provisioning e nei parametri qui sotto.

Riferimenti di dimensionamento

Grandezza	Riferimento
Soggetti	50.000
Richieste al giorno	500
Chiamate API	60 al minuto
Verification API	p95 < 500 ms
Controllo massivo	50.000 righe entro un'ora
Import, distribuzione, controllo massivo	Fino a 50.000 righe per file (configurabile)

Parametri e valori predefiniti

Ciascun parametro ha un intervallo ammesso e ogni modifica entra nell'audit.

Parametro	Predefinito	Intervallo / note
Validità del QR dinamico	15 minuti	5–60
Validità del link email/SMS	7 giorni	1–30
Sessione del destinatario	30 minuti scorrevoli	10–120

Parametro	Predefinito	Intervallo / note
Scadenza della richiesta	30 giorni	1–365, anche per singola richiesta
OTP: cifre, durata, tentativi	6 cifre, 5 minuti, 5 tentativi	cifre 6–8, mai meno di 6
OTP: nuovo invio, blocco	60 secondi, 15 minuti	—
Tetti di emissione OTP	5 per sessione; 5/ora e 10/giorno per recapito; 20/ora per IP	anti SMS pumping
Pagine pubbliche	30 aperture al minuto per IP; 10 token non validi in 10 minuti → blocco di 15 minuti	risposta neutra
Aggiornamento della scheda al desk	5 secondi	2–60
Sessione del backoffice	8 ore; 30 minuti di inattività	avviso 2 minuti prima
Blocco dell'account	5 tentativi → 15 minuti	—
Password	Almeno 12 caratteri	il pavimento non si abbassa
Codici di recupero	8	5–20
Invito utente	72 ore	—
Righe per file (import, controllo, distribuzione)	50.000	1.000–200.000
File di contenuto	PDF, 20 MB	il tetto non si alza
Archivio degli artefatti storici	ZIP fino a 32 MB e 2.000 file; 20 MB per file	limiti fissi
Retention dei file caricati	30 giorni dopo la chiusura del lavoro	i report restano
Retention del log delle integrazioni	90 giorni	30–365
Conservazione del registro consensi cookie	365 giorni	configurabile, anche per sito
Controllo della catena	Ogni giorno	1–7 giorni
Controllo profondo di ogni evidenza	Almeno una volta in 30 giorni	7–90
Rotazione della chiave dati	365 giorni	30–730
Finestra delle accettazioni dichiarate	24 ore	—
Doppio opt-in	3 invii al giorno per recapito	—

Non sono configurabili: la conformità WCAG 2.1 AA delle pagine pubbliche e il mascheramento dei recapiti (email: due caratteri più il dominio; telefono: ultime tre cifre).

22 Glossario

Termine	Significato
Actor	Chi ha compiuto materialmente l'azione, se diverso dal soggetto (genitore, tutore, delegato)
Alias, canonico	Dopo un consolidamento, la posizione unificata (alias) rimanda a quella principale (canonico). Nulla viene riscritto
Ambito (scope)	Classificazione gerarchica dei trattamenti, con codice stabile, lungo cui si chiede una verifica
`as_of`	La data a cui si chiede la verifica: «com'era allora»
Banner cookie	Avviso con cui il visitatore del sito sceglie le categorie di cookie
Bitemporale	Che tiene distinti il tempo in cui un fatto è accaduto e quello in cui il sistema lo ha saputo
`completion_status`	Esito sulla completezza della posizione rispetto ai requisiti
`decision`	Esito sulla possibilità di procedere in un ambito
`device_id` / **ID consenso**	Identificativo del dispositivo creato dal banner cookie; è l'ID consenso mostrato al visitatore
Evidenza	La prova di un evento: manifest, copia del contenuto, ricevute, anello di catena
Fail-closed	Comportamento del sistema esterno che, senza una risposta positiva, non procede
Feature flag	Interruttore impostato al provisioning che rende una funzione disponibile o irraggiungibile
GPC	Global Privacy Control: segnale del browser con cui la persona rifiuta tracciamento e marketing
Hash chain	Catena di impronte crittografiche in cui ogni anello contiene l'impronta del precedente
Integration	Sistema esterno registrato, con chiave API e capacità
`knowledge_as_of`	La data di conoscenza: «che cosa sapevamo allora». Strumento di audit interno
Manifest	Descrizione strutturata e firmabile del contenuto di un'evidenza o di un pacchetto
Modello di richiesta	Configurazione salvata che precompila una richiesta: requisiti, canale, OTP

Termine	Significato
OTP	Codice monouso inviato a un recapito già noto: prova il controllo del recapito, non l'identità legale
Registro dei consensi cookie	Archivio lato server delle scelte fatte sul banner cookie dei siti istituzionali
Requisito	Ciò che serve a una tipologia di persone: azione, documento, obbligatorietà, prova, validità, policy
Richiesta	Pacchetto di azioni assegnato a una persona, con il suo stato, i suoi link e le sue prove
Sigillo	Registrazione in catena di una versione di configurazione al momento dell'attivazione
Soggetto	La persona a cui si riferiscono gli obblighi
Tipologia	Categoria di soggetto configurabile (cliente, dipendente, fornitore…), con campi e requisiti propri