DOCUMENTO PUBBLICO

Sempi Trust Kit

Perché fidarsi di Sempi — i fatti, con le loro fonti

SEMPI S.R.L.

Terrazza Solferino, Via Davide Bertolotti n. 7, 10121 Torino (TO), Italia

P.IVA IT12315280011 · REA TO-1280911

Generato il 2026-09-21 · revisione del codice 49777c844

Dati conservati su server in Romania (Unione Europea)

Documento in italiano e inglese — la versione inglese segue quella italiana.

© 2020–2026 SEMPI S.r.l. — Società Benefit. Tutti i diritti riservati.

Come leggere questo documento

Il criterio, dichiarato prima dei fatti.

Questo dossier raccoglie ciò che serve per decidere se affidarci il lavoro di uno studio o di un'azienda. È costruito su un criterio solo, e vale la pena dichiararlo subito perché è anche il modo per controllarci: **ogni affermazione qui dentro o è verificabile da fuori, o non c'è**.

Da questo criterio discendono tre conseguenze che noterete leggendo:

- **Ogni fatto porta scritto dove si verifica.** Non «i dati sono cifrati», ma quale algoritmo, in quale parte del sistema, e come potete controllarlo.
- **Le cose che non abbiamo sono scritte come le cose che abbiamo.** Troverete «non attiva» e «in preparazione» accanto a «attivo». Un dossier senza un solo punto debole non è rassicurante: è incompleto, e chi valuta lo sa.
- **Nulla è scritto a mano.** Il documento è generato dal codice della piattaforma. Se un dato cambia, cambia qui, sulla pagina pubblica e nei contratti insieme — e un controllo automatico impedisce che le tre versioni divergano.

> Una nota sull'onestà di questo documento, perché riguarda proprio voi. Scriverlo ci ha fatto scoprire che tre nostri documenti contrattuali dichiaravano certificazioni che non possediamo e misure di sicurezza che non erano in essere. Li abbiamo corretti e l'abbiamo scritto nella revisione, invece di sistemarli in silenzio. Se state facendo una due diligence, è un'informazione che vi serve.

La società

Chi firma il contratto, cosa risulta ai registri pubblici e cosa potete verificare senza chiederlo a noi.

Ragione sociale	SEMPI S.R.L.
Forma giuridica	Società a responsabilità limitata — Società Benefit
Sede legale	Terrazza Solferino, Via Davide Bertolotti n. 7, 10121 Torino (TO), Italia
P.IVA / Codice fiscale	IT12315280011
REA	TO-1280911
PEC (posta certificata)	sempi@legalmail.it
Operativa dal	Luglio 2020
Prodotto	SempiX

© 2020–2026 SEMPI S.r.l. — Società Benefit. Tutti i diritti riservati. — Documento pubblico

Società Benefit Attivo

Siamo una Società Benefit: lo statuto ci vincola a perseguire, oltre al profitto, finalità di beneficio comune e a renderne conto ogni anno. La qualifica è nell'oggetto sociale, introdotta nel 2021 — non nel nome: la denominazione iscritta è SEMPI S.R.L. Lo precisiamo perché su questa pagina i dati devono coincidere con la visura, non somigliarle.

> **COME SI VERIFICA:** VISURA ORDINARIA del Registro Imprese di Torino, doc. n. T 670662572 del 21/09/2026. La qualifica risulta dall'OGGETTO SOCIALE («in qualità di Società Benefit, la società intende altresì perseguire finalità di beneficio comune e operare in modo responsabile, sostenibile e trasparente…»), introdotto con l'atto rep. 117848 del 23 luglio 2021 che ha adeguato lo statuto alla normativa su start-up innovative e società benefit (D.L. 179/2012; L. 208/2015 art. 1 c. 376 ss.). ⚠️ NON è nella denominazione: quella iscritta è «SEMPI S.R.L.».

Non è un collegamento: è il documento che regge questo fatto, che teniamo agli atti e mandiamo a chi lo chiede. Alcuni non li pubblichiamo perché riportano dati personali — i certificati di deposito, per esempio, contengono l'indirizzo di residenza della depositante, e la data si prova lo stesso con il numero di deposito. Per averli scrivete a dpo@sempi.it

Startup innovativa Attivo

Iscritta dal 7 febbraio 2025 nella sezione speciale del Registro Imprese riservata alle startup innovative, che richiede requisiti verificati e confermati ogni anno. La società è iscritta nella sezione ordinaria dal 26 giugno 2020.

> **COME SI VERIFICA:** VISURA ORDINARIA del Registro Imprese di Torino, doc. n. T 670662572 del 21/09/2026: «Iscritta nell'apposita sezione speciale in qualità di START-UP INNOVATIVA il 07/02/2025». La società è iscritta nella sezione ORDINARIA dal 26/06/2020.

Non è un collegamento: è il documento che regge questo fatto, che teniamo agli atti e mandiamo a chi lo chiede. Alcuni non li pubblichiamo perché riportano dati personali — i certificati di deposito, per esempio, contengono l'indirizzo di residenza della depositante, e la data si prova lo stesso con il numero di deposito. Per averli scrivete a dpo@sempi.it

Codice depositato con data certa Attivo

Il codice di Sempix e quello di SempiPlancia sono depositati nel Patamu Registry — depositi 289744 e 289758 del 31 marzo 2026 — con marcatura temporale la cui validità è garantita dal Regolamento UE 910/2014 (eIDAS). Ogni deposito porta l'impronta SHA-256 dell'opera, che finisce nell'hash collettivo settimanale pubblicato da Patamu: chiunque abbia il file può ricalcolarla e vedere se coincide. Serve a stabilire chi ha scritto cosa e quando. È una prova di anteriorità con data opponibile, non una registrazione di proprietà: la differenza la scriviamo perché conta.

> **COME SI VERIFICA:** legal/depositi/patamu/2026-03-31_sempix_deposito-289744.pdf e …_sempiplancia_deposito-289758.pdf — certificati Patamu Registry con marcatura temporale 31/03/2026, validità della data certa ai sensi del Reg. UE 910/2014 (eIDAS). Ogni certificato ha la sua pagina pubblica su Patamu: deposito 289744 (SempiX) e 289758 (SempiPlancia), aperte da chiunque senza passare da noi.

Verificabile da fuori: l'indirizzo qui sotto si apre senza passare da noi. https://www.patamu.com/certificate/289744-907

© 2020–2026 SEMPI S.r.l. — Società Benefit. Tutti i diritti riservati. — Documento pubblico

Il Metodo Sempi, non solo il software Attivo

Il Metodo Sempi e la Plancia sono depositati come opere dal 20 settembre 2021, ciascuno con l'impronta SHA-256 del file depositato, presso un servizio di deposito che attesta l'anteriorità nei 176 paesi indicati dal certificato secondo la Convenzione di Berna. Il diritto d'autore nasce con l'opera e non richiede formalità: il deposito serve a datarla in modo che la data non si possa discutere.

> **COME SI VERIFICA:** legal/depositi/copyright/2021-09-20_metodo-sempi_DEP637677296077422688.pdf e …_sempiplancia_DEP637677297616258939.pdf — certificati di anteriorità del 20/09/2021 con impronta SHA-256 del file depositato.

Non è un collegamento: è il documento che regge questo fatto, che teniamo agli atti e mandiamo a chi lo chiede. Alcuni non li pubblichiamo perché riportano dati personali — i certificati di deposito, per esempio, contengono l'indirizzo di residenza della depositante, e la data si prova lo stesso con il numero di deposito. Per averli scrivete a dpo@sempi.it

Marchi depositati all'EUIPO Attivo

SEMPI (domanda 018556088) e METODO SEMPI (domanda 018556620) sono stati depositati all'EUIPO il 13 settembre 2021 come marchi figurativi con elementi verbali, per le classi 9, 35, 41 e 42. Lo stato aggiornato di ciascuna domanda si controlla sul registro pubblico dell'EUIPO con quei due numeri, senza doverlo chiedere a noi. Gli altri nomi che usiamo — Sempix, SempiPlancia, ARYA, Calcolino, e.Vai — non sono marchi depositati, e per questo non li scriviamo con la ®.

> **COME SI VERIFICA:** legal/depositi/euipo/2021-09-13_domanda-SEMPI_018556088.pdf e …_domanda-METODO-SEMPI_018556620.pdf — ricevute EUIPO di deposito del 13/09/2021; stato aggiornato di ciascuna domanda sul registro pubblico, con quei due numeri.

Verificabile da fuori: l'indirizzo qui sotto si apre senza passare da noi.
https://euipo.europa.eu/eSearch/#details/trademarks/018556088

Dichiarazione di paternità con data certa Attivo

Un documento solo elenca chi ha scritto il software, il metodo e i segni distintivi, con la data di ciascuno e la prova che lo dimostra — deposito, domanda di marchio o certificato. Il PDF porta una marca temporale qualificata incorporata, quindi la data dell'elenco non dipende da quello che diciamo noi, e accanto pubblichiamo la sua impronta SHA-256 per lasciarla ricalcolare a chi lo scarica.

> **COME SI VERIFICA:** sempix.org/documenti/DICHIARAZIONE_PATERNITA.pdf — elenco di software, metodo e segni distintivi con la data e la prova di ciascuno; marca temporale qualificata incorporata nel PDF (PAdES, Reg. UE 910/2014) apposta il 21/09/2026 alle 16:40:17 UTC. Impronta SHA-256 del file marcato: 0b36f9c45c6fd524a843f950869ff240fdf6e2c081740dfcc9d296dfab617ca9 — ricalcolabile da chiunque abbia una copia, per sapere se è la nostra versione o un'altra.

Verificabile da fuori: l'indirizzo qui sotto si apre senza passare da noi. sempix.it/documenti/DICHIARAZIONE_PATERNITA.pdf

© 2020–2026 SEMPI S.r.l. — Società Benefit. Tutti i diritti riservati. — Documento pubblico

Manifesto del codice sorgente Attivo

L’impronta SHA-256 dell’intero albero del codice a un commit preciso, dentro un PDF con marca temporale qualificata. Serve a una cosa sola, e conta: se un domani si discute di chi ha scritto cosa e quando, quel documento prova che a quella data quel codice esisteva ed era esattamente quello — non una versione riscritta dopo.

> **COME SI VERIFICA:** sempix.org/documenti/MANIFESTO_CODICE.pdf — impronta SHA-256 dell’albero del codice sorgente al commit c108c2e813f6; marca temporale qualificata incorporata nel PDF (PAdES, Reg. UE 910/2014) apposta il 21/09/2026 alle 16:40:17 UTC. Impronta SHA-256 del file marcato: 7d3468b576c5ad5f862e86ad1d33330a7db51e53e155c4a8d44beded78f3cf6c — ricalcolabile da chiunque abbia una copia, per sapere se è la nostra versione o un’altra.

Verificabile da fuori: l’indirizzo qui sotto si apre senza passare da noi. sempix.it/documenti/MANIFESTO_CODICE.pdf

I numeri, con la loro provenienza

Ogni misura porta il suo denominatore e la data in cui è stata presa. Un numero senza denominatore non è una misura, è una sensazione.

MISURA	SU COSA È CALCOLATA	FONTE E DATA
99,2% delle registrazioni le propone il motore, non una persona	17.958 registrazioni su 18.102 nate dentro SempiX (fattura ricevuta da SDI, fattura arrivata via email, inserimento manuale) su 86 aziende in produzione. Le scritture importate da altri gestionali sono escluse dal conteggio: quelle non le scrive il nostro motore. Le righe più vecchie, dove il sistema non annotava chi avesse scritto la registrazione, contano come manuali: quindi il numero è una stima per difetto.	Lettura degli 86 database di produzione con scripts/misura-automazione-tenant.ts — 2026-08-26
4,8 / 5 su Trustpilot	26 recensioni pubbliche sul profilo Sempi. È il punteggio che vedi sul profilo, non una media che ci siamo calcolati noi.	Profilo pubblico Trustpilot — 2026-08-25
5,0 / 5 su Google	5 recensioni pubbliche sul profilo Google Business «Sempi Srl — Torino». Sono poche, e preferiamo dirlo che nasconderlo dietro una media.	Profilo pubblico Google Business — 2026-08-25

© 2020–2026 SEMPI S.r.l. — Società Benefit. Tutti i diritti riservati. — Documento pubblico

Infrastruttura

Dove gira la piattaforma, chi tiene acceso il servizio e cosa succede ai vostri dati ogni notte.

Server nell’Unione Europea Attivo

La piattaforma gira su server in Romania, dentro l’Unione Europea. I dati di produzione non escono dallo Spazio Economico Europeo.

> **COME SI VERIFICA:** DATA_LOCATION in shared/trust/identity.ts — server Taz.ro in Romania (Unione Europea). Nessun dato di produzione fuori dallo SEE.

Verificabile da fuori: l’indirizzo qui sotto si apre senza passare da noi. https://taz.ro

Un archivio separato per ogni azienda Attivo

I dati di ogni azienda cliente stanno in uno spazio suo dentro il database, non mescolati agli altri con un filtro. È la differenza fra due archivi in due stanze diverse e due faldoni nello stesso cassetto: se il filtro sbaglia, nel secondo caso vedete i dati di qualcun altro. Controlli automatici a ogni rilascio verificano che nessuna interrogazione possa attraversare il confine.

> **COME SI VERIFICA:** Un solo schema PostgreSQL per azienda cliente (server/multiTenantDb.ts). L'isolamento è verificato dai test tests/unit/aryaTenantScopingGuards.test.ts e collaboratorPortalIsolation.test.ts, e dalle guardie check:salti-tenant, check:storage-tenant e check:sql-filtra-azienda in CI.

Non è un collegamento: è il file del nostro codice sorgente che rende vero questo fatto. Il repository è privato e resta privato, quindi non si apre da qui: si guarda insieme, a schermo, durante una verifica fornitore sotto accordo di riservatezza.

Copie cifrate, conservate 30 giorni Attivo

Le copie di sicurezza sono compresse e cifrate, su un disco che sopravvive ai rilasci, e si conservano 30 giorni. Attenzione a non confondere due cose diverse: la legge chiede di conservare i DOCUMENTI fiscali per dieci anni, e quello lo fa la conservazione sostitutiva a norma. Tenere 3.650 copie complete del database non servirebbe a nessuno e riempirebbe il disco.

> **COME SI VERIFICA:** server/services/backupService.ts — i dump sono compressi e cifrati salvo disattivazione esplicita (BACKUP_ENCRYPTION_ENABLED), scritti sul volume persistente /app/backups. Retention 30 giorni (BACKUP_RETENTION_DAYS): la conservazione decennale riguarda i DOCUMENTI fiscali ed è compito della conservazione sostitutiva a norma, non di 3.650 copie complete del database.

Non è un collegamento: è il file del nostro codice sorgente che rende vero questo fatto. Il repository è privato e resta privato, quindi non si apre da qui: si guarda insieme, a schermo, durante una verifica fornitore sotto accordo di riservatezza.

© 2020–2026 SEMPI S.r.l. — Società Benefit. Tutti i diritti riservati. — Documento pubblico

Il ripristino è stato provato davvero Attivo

Un backup che nessuno ha mai provato a ripristinare non è un backup: è un file. Abbiamo uno strumento che prende una copia, la ripristina su un database usa e getta e controlla non solo che i dati si leggano, ma che la contabilità quadri. È stato collaudato su tre casi: una copia sana, una con la contabilità sbilanciata e un file troncato. Riconosce i primi due per quello che sono e dichiara fallito il terzo.

> **COME SI VERIFICA:** scripts/backup-restore-drill.ts — ripristina un dump su un database temporaneo e verifica che i dati siano leggibili E che la Prima Nota quadri. Collaudato il 25/07/2026 su tre scenari (backup sano, contabilità sbilanciata, dump troncato): riconosce i primi due come tali e dichiara fallito il terzo. Un backup che non sai ripristinare non è un backup.

Non è un collegamento: è il file del nostro codice sorgente che rende vero questo fatto. Il repository è privato e resta privato, quindi non si apre da qui: si guarda insieme, a schermo, durante una verifica fornitore sotto accordo di riservatezza.

Ridondanza e scalabilità In preparazione

Oggi gli archivi delle aziende stanno su un unico database, senza cluster dedicato. Con il fornitore che tiene l’infrastruttura abbiamo definito a settembre 2026 il piano per portarla a database ridondato, cluster separato dall’applicazione e crescita orizzontale, dimensionato sulle circa 650 aziende attese entro l’inizio del 2027. Lo scriviamo come piano perché è un piano: il giorno in cui sarà in funzione, questa riga cambierà stato.

> **COME SI VERIFICA:** Piano architetturale concordato con TAZ IT Services (Mihai Ola) il 19/09/2026: ridondanza del database, cluster PostgreSQL separato dall'applicazione, più worker, scalabilità orizzontale e riduzione automatica delle risorse. Stato attuale: i tenant condividono lo stesso database, senza cluster dedicato né pool di connessioni.

Non è un collegamento: è il documento che regge questo fatto, che teniamo agli atti e mandiamo a chi lo chiede. Alcuni non li pubblichiamo perché riportano dati personali — i certificati di deposito, per esempio, contengono l’indirizzo di residenza della depositante, e la data si prova lo stesso con il numero di deposito. Per averli scrivete a dpo@sempi.it

Ambienti separati e ritorno alla versione precedente In preparazione

Oggi il rilascio va direttamente in produzione, protetto dagli oltre 120 controlli automatici che girano prima. Manca un ambiente di prova separato con ritorno automatico alla versione precedente, ed è il secondo punto del piano concordato con il fornitore dell’infrastruttura. Preferiamo dirlo noi adesso che farvelo scoprire durante una verifica.

> **COME SI VERIFICA:** Stato attuale verificabile nel repository: il ramo `Sempi` è il ramo di produzione e ogni push ricostruisce e rilascia (CLAUDE.md, scripts/rilascia.sh). Ambienti di prova e produzione separati, con ripristino automatico della versione precedente, sono concordati nel piano con TAZ del 19/09/2026 e non sono ancora in essere.

Non è un collegamento: è il file del nostro codice sorgente che rende vero questo fatto. Il repository è privato e resta privato, quindi non si apre da qui: si guarda insieme, a schermo, durante una verifica fornitore sotto accordo di riservatezza.

© 2020–2026 SEMPI S.r.l. — Società Benefit. Tutti i diritti riservati. — Documento pubblico

Oltre 120 controlli prima di ogni rilascio Attivo

I controlli automatici — tipi, stile, test, verifiche contabili e di isolamento fra aziende — girano dentro la costruzione della versione, non accanto. Vuol dire che una versione che non li supera non arriva in produzione: non è sconsigliato, è impossibile.

> **COME SI VERIFICA:** scripts/ci-nostra.mjs gira dentro Dockerfile.coolify: oltre 120 controlli automatici (typecheck, lint, test, guardie contabili e di isolamento) sono eseguiti DURANTE la costruzione dell'immagine. Un rilascio non controllato non è sconsigliato: è impossibile.

Non è un collegamento: è il file del nostro codice sorgente che rende vero questo fatto. Il repository è privato e resta privato, quindi non si apre da qui: si guarda insieme, a schermo, durante una verifica fornitore sotto accordo di riservatezza.

Sicurezza

Come sono protetti gli accessi e i dati, e come si ricostruisce chi ha fatto cosa.

Credenziali cifrate Attivo

Le credenziali e i dati sensibili sono cifrati con AES-256-GCM, un algoritmo che oltre a nascondere il contenuto si accorge se qualcuno l'ha manomesso. La chiave non è la password: se ne ricava una apposta, con 100.000 passaggi di calcolo, così indovinarla a forza bruta non conviene.

> **COME SI VERIFICA:** server/encryption.ts e server/services/credentialEncryptionService.ts — AES-256-GCM (cifratura autenticata) con chiave derivata via PBKDF2-SHA256 a 100.000 iterazioni. La guardia check:colonne-cifrate in CI verifica che le colonne sensibili non finiscano in chiaro.

Non è un collegamento: è il file del nostro codice sorgente che rende vero questo fatto. Il repository è privato e resta privato, quindi non si apre da qui: si guarda insieme, a schermo, durante una verifica fornitore sotto accordo di riservatezza.

Traffico cifrato Attivo

Tutte le comunicazioni fra il vostro browser e la piattaforma viaggiano su HTTPS.

> **COME SI VERIFICA:** HTTPS obbligatorio su tutti i domini di produzione, certificati gestiti da Coolify.

Non è un collegamento: è il documento che regge questo fatto, che teniamo agli atti e mandiamo a chi lo chiede. Alcuni non li pubblichiamo perché riportano dati personali — i certificati di deposito, per esempio, contengono l'indirizzo di residenza della depositante, e la data si prova lo stesso con il numero di deposito. Per averli scrivete a dpo@sempi.it

© 2020–2026 SEMPI S.r.l. — Società Benefit. Tutti i diritti riservati. — Documento pubblico

Permessi per ruolo Attivo

Ogni persona vede ciò che il suo ruolo prevede: titolare, contabile, operatore, sola lettura. ARYA ha un ruolo suo, il più limitato di tutti: può preparare bozze e leggere i report, non può registrare nulla da sola.

> **COME SI VERIFICA:** docs/compliance/RBAC_MATRIX.md — ruoli OWNER / ACCOUNTANT / CLERK / VIEWER più AI_BOT (ARYA, limitata alle bozze e alla lettura). Le operazioni ad alto rischio sono elencate con la loro frequenza di revisione. Pubblicata anche come PDF su sempix.org/documenti/MATRICE_PERMESSI.pdf, con marca temporale qualificata incorporata nel PDF (PAdES, Reg. UE 910/2014) apposta il 21/09/2026 alle 16:40:17 UTC. Impronta SHA-256 del file marcato: c2ad95ffdddbcad71386707782232da65b1a4bf2a6206bb87fef8e8526bc3747 — ricalcolabile da chiunque abbia una copia, per sapere se è la nostra versione o un'altra.

Verificabile da fuori: l'indirizzo qui sotto si apre senza passare da noi. sempix.it/documenti/MATRICE_PERMESSI.pdf

Accesso a due fattori Attivo

L'autenticazione a due fattori è disponibile per ogni utenza. È disponibile, non imposta: chi vuole renderla obbligatoria per tutto lo studio lo decide dal pannello. Lo scriviamo com'è, perché «abbiamo la doppia autenticazione» e «la doppia autenticazione è attiva su tutti» sono due frasi diverse.

> **COME SI VERIFICA:** Autenticazione a due fattori disponibile per ogni utenza (pagina /2fa-settings, server/services/codiceEmail2fa.ts). È disponibile, non imposta: chi deve renderla obbligatoria per il proprio studio lo decide dal pannello, e va detto com'è.

Non è un collegamento: è il file del nostro codice sorgente che rende vero questo fatto. Il repository è privato e resta privato, quindi non si apre da qui: si guarda insieme, a schermo, durante una verifica fornitore sotto accordo di riservatezza.

Registro degli accessi e delle modifiche Attivo

Creazioni, modifiche, cancellazioni, letture, esportazioni e accessi restano scritti con data, ora e autore. Ha una voce a sé il caso più delicato: quando un amministratore della piattaforma accede ai dati di un'azienda, quell'accesso è registrato come tale e si può chiedere l'elenco.

> **COME SI VERIFICA:** server/services/auditLogService.ts — registra creazioni, modifiche, cancellazioni, letture, esportazioni, accessi e — voce a sé — gli accessi amministrativi trasversali fra aziende (ADMIN_CROSS_COMPANY_ACCESS). Consultabile dalla pagina /admin-audit-log.

Non è un collegamento: è il file del nostro codice sorgente che rende vero questo fatto. Il repository è privato e resta privato, quindi non si apre da qui: si guarda insieme, a schermo, durante una verifica fornitore sotto accordo di riservatezza.

© 2020–2026 SEMPI S.r.l. — Società Benefit. Tutti i diritti riservati. — Documento pubblico

Ogni correzione contabile lascia traccia Attivo

Se una registrazione viene corretta, resta scritto chi l'ha cambiata, quando e cosa è cambiato. In contabilità italiana una scrittura sbagliata si corregge: riempire il giornale di storni e riemissioni per ogni correzione è tenuta irregolare, e l'Agenzia la sanziona. Quindi la traccia sta nella cronologia della registrazione, non in scritture di comodo.

COME SI VERIFICA: ARYA Tutela (server/services/aryaTutelaService.ts, pagine /aryatutela/*) — ogni modifica a una registrazione contabile lascia un evento con chi, quando e cosa è cambiato. In contabilità italiana una scrittura sbagliata si CORREGGE, non si storna per riemetterla: la traccia sta nella cronologia, non in scritture di comodo.

Non è un collegamento: è il file del nostro codice sorgente che rende vero questo fatto. Il repository è privato e resta privato, quindi non si apre da qui: si guarda insieme, a schermo, durante una verifica fornitore sotto accordo di riservatezza.

Piano di gestione degli incidenti Attivo

Gli incidenti sono classificati su tre livelli, ciascuno con il suo tempo di presa in carico: un'ora per i casi critici, quattro ore per quelli gravi, il giorno lavorativo successivo per i minori. Per i casi critici la notifica all'autorità competente è prevista entro 24 ore.

COME SI VERIFICA: docs/compliance/INCIDENT_RESPONSE_PLAN.md v1.0.0 (in vigore dal 14/07/2026) — tre livelli di gravità con tempi di presa in carico (1 ora / 4 ore / giorno lavorativo successivo) e notifica alle autorità entro 24 ore per gli incidenti critici, come richiesto da DORA e NIS2. Pubblicato anche come PDF su sempix.org/documenti/PIANO_RISPOSTA_INCIDENTI.pdf, con marca temporale qualificata incorporata nel PDF (PAdES, Reg. UE 910/2014) apposta il 21/09/2026 alle 16:40:17 UTC. Impronta SHA-256 del file marcato: abe8eeba49fbf6e13ba2c61a2c1759631fbb78af1a81c74b51b64948ada01598 — ricalcolabile da chiunque abbia una copia, per sapere se è la nostra versione o un'altra.

Verificabile da fuori: l'indirizzo qui sotto si apre senza passare da noi. sempix.it/documenti/PIANO_RISPOSTA_INCIDENTI.pdf

Canale di segnalazione su Sempi stessa Attivo

Chi vuole segnalare una condotta illecita che riguarda noi ha un canale suo, su /segnalazioni: si segnala in anonimo, si riceve un codice per seguire la pratica e per scrivere ai responsabili senza doversi rivelare. È lo stesso modulo che vendiamo ai clienti, puntato su di noi — se non funzionasse, i primi ad accorgercene saremmo noi.

COME SI VERIFICA: Canale pubblico su /segnalazioni (alias /whistleblowing), servito dal modulo ARYA Segnalazioni — lo stesso che la piattaforma offre ai clienti. Segnalazione anonima per impostazione predefinita, codice di riscontro per seguire la pratica e scrivere ai responsabili senza rivelarsi, istruttoria tracciata (server/services/segnalazioniService.ts, tabelle segnalazioni / segnalazioni_istruttorie / segnalazioni_comunicazioni). ⚠️ Se l'obbligo di legge (D.Lgs. 24/2023) ricada su Sempi è determinazione del DPO: qui si dichiara che il canale esiste e funziona, non che è dovuto.

Verificabile da fuori: l'indirizzo qui sotto si apre senza passare da noi. sempix.it/segnalazioni

© 2020–2026 SEMPI S.r.l. — Società Benefit. Tutti i diritti riservati. — Documento pubblico

Test di intrusione da terza parte In preparazione

Non è ancora stato svolto un test di intrusione da una società terza indipendente. Esistono test automatici che, a ogni rilascio, provano ad attraversare il confine fra i dati di due aziende e devono fallire. Il test da terza parte è programmato prima dell'audit di certificazione: finché non c'è, lo diciamo.

> **COME SI VERIFICA:** docs/compliance/ISO27001-DORA-NIS2-FRAMEWORK.md, Gap 3: i test di isolamento fra aziende esistono come test automatici, un penetration test formale da società terza indipendente non è ancora stato svolto. Programmato prima dell'audit di certificazione.

Non è un collegamento: è il documento che regge questo fatto, che teniamo agli atti e mandiamo a chi lo chiede. Alcuni non li pubblichiamo perché riportano dati personali — i certificati di deposito, per esempio, contengono l'indirizzo di residenza della depositante, e la data si prova lo stesso con il numero di deposito. Per averli scrivete a dpo@sempi.it

Conformità normativa

Le regole a cui la piattaforma risponde per costruzione, non per dichiarazione.

Fatturazione elettronica (SDI) Attivo

Le fatture sono emesse e ricevute attraverso il Sistema di Interscambio dell'Agenzia delle Entrate. Una fattura già consegnata non può più essere modificata né riportata a bozza: è bloccata dal sistema, non dalla buona volontà di chi lo usa.

> **COME SI VERIFICA:** Fatturazione elettronica verso il Sistema di Interscambio dell'Agenzia delle Entrate (server/services/sdi/, pipeline protetta da tests/unit/sdiInvoiceGuards.test.ts). Le fatture emesse sono immutabili e non possono essere declassate dopo la consegna.

Non è un collegamento: è il file del nostro codice sorgente che rende vero questo fatto. Il repository è privato e resta privato, quindi non si apre da qui: si guarda insieme, a schermo, durante una verifica fornitore sotto accordo di riservatezza.

Firma e marca temporale qualificate (eIDAS) Attivo

Le marche temporali e le firme che richiedono valore legale sono apposte tramite un prestatore di servizi fiduciari qualificato ai sensi del regolamento europeo eIDAS. È la qualifica del prestatore a dare valore legale al documento, non il fatto che ce lo mettiamo noi.

> **COME SI VERIFICA:** server/services/namirialTimestampService.ts — marca temporale qualificata eIDAS (Reg. UE 910/2014, art. 41) apposta tramite prestatore di servizi fiduciari qualificato. Firma qualificata (QES) per gli invii che la richiedono: server/services/cadesSignatureService.ts, statoFirmaQualificata.ts.

Non è un collegamento: è il file del nostro codice sorgente che rende vero questo fatto. Il repository è privato e resta privato, quindi non si apre da qui: si guarda insieme, a schermo, durante una verifica fornitore sotto accordo di riservatezza.

© 2020–2026 SEMPI S.r.l. — Società Benefit. Tutti i diritti riservati. — Documento pubblico

Lettura dei conti bancari (PSD2) Attivo

I movimenti bancari si leggono attraverso un istituto autorizzato come prestatore di servizi di informazione sui conti. L’accesso è in sola lettura, parte da un mandato che firmate voi e si revoca quando volete: la piattaforma non può disporre pagamenti dai vostri conti.

> **COME SI VERIFICA:** Lettura dei conti bancari via Open Banking attraverso GoCardless Bank Account Data, istituto autorizzato come AISP ai sensi della direttiva PSD2. Accesso in SOLA LETTURA, su mandato esplicito del cliente e revocabile: Sempix non dispone pagamenti.

Non è un collegamento: è il documento che regge questo fatto, che teniamo agli atti e mandiamo a chi lo chiede. Alcuni non li pubblichiamo perché riportano dati personali — i certificati di deposito, per esempio, contengono l’indirizzo di residenza della depositante, e la data si prova lo stesso con il numero di deposito. Per averli scrivete a dpo@sempi.it

GDPR Attivo

Responsabile del trattamento per conto vostro, con un DPO esterno nominato, l’accordo sul trattamento dei dati disponibile, l’elenco pubblico di chi altro tocca i dati e i diritti degli interessati esercitabili da una pagina apposita.

> **COME SI VERIFICA:** DPO esterno nominato (Alberto Tripoli, E.A. Enterprise S.r.l., shared/trust/identity.ts), DPA ex art. 28 disponibile (legal/ACCORDO_TRATTAMENTO_DATI_PERSONALI_v1.1.0.md), registro dei sub-responsabili pubblico su /trust, diritti degli interessati esercitabili da /gdpr-rights.

Non è un collegamento: è il file del nostro codice sorgente che rende vero questo fatto. Il repository è privato e resta privato, quindi non si apre da qui: si guarda insieme, a schermo, durante una verifica fornitore sotto accordo di riservatezza.

Conservazione a norma (CAD / AgID) Attivo

La conservazione con valore legale dei documenti fiscali è affidata a conservatori accreditati. Non la svolgiamo noi e non ci attribuiamo il loro accreditamento — è una distinzione che molti fornitori non fanno.

> **COME SI VERIFICA:** Conservazione sostitutiva a norma (CAD / linee guida AgID) affidata a conservatori accreditati. Non la svolgiamo noi e non ci attribuiamo il loro accreditamento — shared/trust/identity.ts, voce trust.cert.agid.

Non è un collegamento: è il file del nostro codice sorgente che rende vero questo fatto. Il repository è privato e resta privato, quindi non si apre da qui: si guarda insieme, a schermo, durante una verifica fornitore sotto accordo di riservatezza.

© 2020–2026 SEMPI S.r.l. — Società Benefit. Tutti i diritti riservati. — Documento pubblico

Regolamento europeo sull’IA In preparazione

La registrazione al registro europeo dei sistemi di intelligenza artificiale non è stata effettuata; il termine rilevante è stato differito al 2 dicembre 2027. Se ARYA vada classificata ad alto rischio è una valutazione ancora aperta: due nostri documenti interni la leggono in modo diverso e la decisione spetta al responsabile della protezione dei dati. Preferiamo scriverlo così piuttosto che darvi la versione che ci conviene di più.

> **COME SI VERIFICA:** Dichiarazione di conformità AI Act (in legal/) e documento di preparazione al registro (in docs, cartella compliance). ⚠️ I due documenti interni si contraddicono sulla classificazione di rischio di ARYA: la Dichiarazione sostiene che nessun sistema rientra nell'Allegato III del Regolamento (UE) 2024/1689 e ne dà la motivazione; il documento ISO27001-DORA-NIS2 la dà per alto rischio senza indicare il punto applicabile. La determinazione spetta al DPO ed è aperta. Quello che è certo e non dipende da quale lettura prevalga: la registrazione al registro europeo NON è stata effettuata, e il termine rilevante è stato differito al 2 dicembre 2027. Pagina pubblica /ai-act.

Verificabile da fuori: l’indirizzo qui sotto si apre senza passare da noi. sempix.it/ai-act

Accessibilità Attivo

La dichiarazione di accessibilità è pubblicata. Due controlli automatici impediscono che una schermata nuova nasca con testo illeggibile o con contrasto insufficiente in tema scuro.

> **COME SI VERIFICA:** Dichiarazione di accessibilità pubblicata su /dichiarazione-accessibilita. In CI le guardie check:a11y-legibility e check:dark-contrast impediscono che una schermata nuova nasca illeggibile.

Verificabile da fuori: l’indirizzo qui sotto si apre senza passare da noi. sempix.it/dichiarazione-accessibilita

Certificazioni

La distinzione fra «posseduta» e «in preparazione» la manteniamo anche quando è a nostro sfavore. Una certificazione dichiarata e non posseduta non è un arrotondamento: è una dichiarazione non veritiera.

RIFERIMENTO	STATO	SIGNIFICATO
ISO/IEC 27001	In preparazione — NON posseduta	Percorso avviato. Non siamo certificati: quando lo saremo, il certificato sarà pubblicato qui con il numero e l’ente che l’ha emesso.
SOC 2 Type II	In preparazione — NON posseduta	Percorso avviato. Nessuna attestazione ancora emessa da un revisore indipendente.
GDPR — protezione dei dati fin dalla progettazione (art. 25)	Applicato	Misure adottate e documentate nel DPA e nel registro dei trattamenti, con separazione dei dati per azienda e registro degli accessi.

© 2020–2026 SEMPI S.r.l. — Società Benefit. Tutti i diritti riservati. — Documento pubblico

RIFERIMENTO	STATO	SIGNIFICATO
Conservazione a norma CAD / AgID	Applicato	La conservazione sostitutiva a norma è affidata a conservatori accreditati AgID (Aruba, InfoCert, Namirial e altri). Non la svolgiamo noi, e non ci attribuiamo il loro accreditamento.

Governance dell’intelligenza artificiale

ARYA è l’assistente che prepara il lavoro contabile. La frase che descrive il suo ruolo è questa: il modello scrive la spiegazione, il motore contabile applica la regola, la persona decide. Ecco cosa succede a una fattura, passo per passo.

ARYA è l’assistente che prepara il lavoro contabile. La frase che descrive il suo ruolo è questa: il modello scrive la spiegazione, il motore contabile applica la regola, la persona decide. Ecco cosa succede a una fattura, passo per passo.

1. **Legge il documento, non lo indovina**
   Fornitore, numero, data, imponibile, IVA e descrizione vengono letti dal PDF o dall’XML. Se un dato nel documento non c’è, resta vuoto e viene segnalato: non viene dedotto da una fattura simile.
2. **Propone la registrazione, con il motivo**
   La proposta arriva con il conto suggerito e la ragione in italiano leggibile — non il nome di una funzione interna — più un grado di confidenza che dice quanto è sicura.
3. **Il motore contabile controlla la proposta**
   Partita doppia, aliquota IVA, coerenza del conto con il piano dei conti, reverse charge, ritenute. Una proposta che non supera questi controlli non arriva nemmeno alla tua conferma.
4. **Confermi tu, e puoi correggere**
   Niente entra in Prima Nota senza che una persona lo confermi. Puoi accettare, correggere o rifiutare: correggere è la strada normale, non un ripiego.
5. **Resta la traccia di chi ha deciso cosa**
   Ogni conferma e ogni correzione successiva finisce nella cronologia della registrazione con chi, quando e cosa è cambiato. Una registrazione sbagliata si corregge e la modifica resta tracciata: non si cancella e non si storna per finta.

> **Esempio.** «Costi di sviluppo, IVA in reverse charge: il fornitore è extra-UE e la descrizione “Autorecharge credits” corrisponde ai crediti di sviluppo già registrati su questo conto tre volte quest’anno. Confidenza alta. Confermi o correggi?»

I limiti, detti chiaramente: ARYA sbaglia, soprattutto su fornitori nuovi e su casistiche che non ha mai visto. Per questo la conferma umana non è una formalità che toglieremo quando il modello sarà più bravo — è il punto in cui la responsabilità professionale resta di chi ce l’ha per legge.

© 2020–2026 SEMPI S.r.l. — Società Benefit. Tutti i diritti riservati. — Documento pubblico

Cosa NON facciamo

Non conosciamo le credenziali della tua banca.

Il collegamento passa da GoCardless, autorizzato AISP ai sensi della PSD2: le credenziali le inserisci sulle pagine della tua banca, non sulle nostre. A noi arriva un consenso a tempo, che puoi revocare quando vuoi e che dà accesso in sola lettura ai movimenti.

Non disponiamo pagamenti dal tuo conto.

La sincronizzazione bancaria è in sola lettura: legge i movimenti, non li origina. Gli addebiti SEPA esistono in piattaforma per gli incassi che sei TU ad attivare verso i TUOI clienti, con un mandato che firmano loro: è un’altra funzione, si accende separatamente e la vedi nel contratto.

I tuoi dati non addestrano modelli di intelligenza artificiale.

Né i nostri né quelli dei fornitori. Verso il modello esterno esce il testo della domanda e il documento in lavorazione, con codice fiscale e IBAN mascherati, sotto contratto che esclude l’uso per addestramento.

L’intelligenza artificiale non scrive in contabilità da sola.

Propone una registrazione; a scriverla è il motore contabile, che applica regole deterministiche e non un modello linguistico, dopo la conferma di una persona. Una proposta rifiutata non lascia traccia in Prima Nota.

Se te ne vai, i dati vengono con te.

Esportazione di anagrafiche, prima nota, fatture e allegati in formati aperti, in qualsiasi momento, senza chiedere il permesso a noi e senza costi di uscita. Alla chiusura del rapporto i dati vengono restituiti e poi cancellati, salvo quanto la legge ci obbliga a conservare.

Assicurazioni

Cosa è coperto e cosa non lo è. Una copertura che non abbiamo la scriviamo lo stesso: scoprirlo dopo un

© 2020–2026 SEMPI S.r.l. — Società Benefit. Tutti i diritti riservati. — Documento pubblico

problema è peggio che saperlo prima.

Responsabilità civile professionale Attivo

Copertura di responsabilità civile professionale tramite l'adesione ad APCO, l'associazione dei consulenti di management: assicuratore Lloyd's, massimale 150.000 € per sinistro e in aggregato annuo più il 25% per le spese legali, franchigia 2.500 €, retroattività al 31 dicembre 2014, mondo intero esclusi USA e Canada. ⚠️ Copre l'attività di CONSULENZA, che è una cosa diversa dal software: non è una Tech E&O sul prodotto né una polizza cyber. Ve lo diciamo noi perché è la distinzione che conta se state valutando il rischio di affidarci i vostri dati.

Compagnia: Lloyd's Insurance Company S.A. · **Massimale:** € 150.000 per sinistro e in aggregato annuo, +25% per spese legali · **Scadenza:** 2027-06-27

Polizza cyber Non attiva

Copre i danni da attacco informatico, violazione di dati e interruzione del servizio: i costi di notifica, il ripristino, le richieste di terzi. Oggi non l'abbiamo. Va detto perché è la copertura che uno studio strutturato si aspetta di trovare, e sarebbe scorretto lasciare che la desuma dalle altre.

Tech E&O (errori del software) Non attiva

Copre i danni causati da un difetto del prodotto software, che è una cosa diversa dalla responsabilità del consulente. Oggi non l'abbiamo, e una copertura sulla consulenza non la sostituisce.

Continuità

La domanda scomoda: e se domani Sempi non ci fosse più? La risposta non è «non succederà», è rendere basso il costo di andarsene, prima che serva.

I vostri dati escono in formati aperti Attivo

Bilanci, Prima Nota, registri IVA, anagrafiche e fatture si esportano in formati che altri gestionali sanno leggere. Non esiste un formato proprietario sulla via d'uscita: è la prima cosa da controllare in qualsiasi fornitore, perché è quella che decide se potrete andarvene davvero.

> **COME SI VERIFICA:** Esportazioni in formati aperti e leggibili da altri gestionali: bilanci e Prima Nota (server/routes/accountingExportRoutes.ts, bilancioExportRoutes.ts), registri IVA (vatExportRoutes.ts), anagrafiche (anagraficheImportExportRoutes.ts), fatture in XML SDI. Nessun formato proprietario sulla via d'uscita.

Non è un collegamento: è il file del nostro codice sorgente che rende vero questo fatto. Il repository è privato e resta privato, quindi non si apre da qui: si guarda insieme, a schermo, durante una verifica fornitore sotto accordo di riservatezza.

© 2020–2026 SEMPI S.r.l. — Società Benefit. Tutti i diritti riservati. — Documento pubblico

Dopo la disdetta i dati restano leggibili Attivo

Alla fine dell’abbonamento resta garantito l’accesso in lettura e l’esportazione: quello che si blocca è l’inserimento di nuove scritture. Non è una cortesia, discende dall’obbligo di conservare le scritture contabili e dal diritto alla portabilità dei dati.

> **COME SI VERIFICA:** server/services/subscriptionAccessGate.ts — alla cessazione dell'abbonamento restano garantiti la lettura e l'esportazione dei dati; è l'inserimento di nuove scritture a essere bloccato. Deriva dagli obblighi di conservazione (art. 2220 c.c.) e dal diritto alla portabilità (art. 20 GDPR).

Non è un collegamento: è il file del nostro codice sorgente che rende vero questo fatto. Il repository è privato e resta privato, quindi non si apre da qui: si guarda insieme, a schermo, durante una verifica fornitore sotto accordo di riservatezza.

Portabilità dei dati (art. 20 GDPR) Attivo

La richiesta di portabilità si presenta da una pagina dedicata, indicando anche in quale formato volete i dati.

> **COME SI VERIFICA:** server/routes/gdprRoutes.ts — richiesta di portabilità (art. 20 GDPR) esercitabile dalla pagina /gdpr-rights, con indicazione del formato dati desiderato.

Verificabile da fuori: l’indirizzo qui sotto si apre senza passare da noi. sempix.it/gdpr-rights

I documenti con valore legale non stanno solo qui Attivo

I documenti fiscali in conservazione a norma sono presso conservatori accreditati, non dentro la piattaforma. Restano raggiungibili anche indipendentemente da noi: è la parte di risposta più concreta alla domanda «e se domani sparite?».

> **COME SI VERIFICA:** La conservazione sostitutiva a norma dei documenti fiscali è presso conservatori accreditati AgID, non dentro Sempix: i documenti con valore legale restano raggiungibili dal cliente anche indipendentemente dalla piattaforma.

Non è un collegamento: è il documento che regge questo fatto, che teniamo agli atti e mandiamo a chi lo chiede. Alcuni non li pubblichiamo perché riportano dati personali — i certificati di deposito, per esempio, contengono l’indirizzo di residenza della depositante, e la data si prova lo stesso con il numero di deposito. Per averli scrivete a dpo@sempi.it

Prova di ripristino completa In preparazione

Gli obiettivi di tempo di ripristino sono definiti e la procedura è collaudata su database di prova. Una prova completa e cronometrata sull’ambiente reale non è ancora stata fatta: finché non la facciamo, un obiettivo dichiarato resta un obiettivo, non una misura.

> **COME SI VERIFICA:** Obiettivi RTO/RPO definiti nei documenti contrattuali e la procedura di ripristino è collaudata (scripts/backup-restore-drill.ts). Non è invece ancora stata eseguita una prova di disaster recovery completa e cronometrata sull'ambiente di produzione: finché non lo è, gli obiettivi restano obiettivi.

Non è un collegamento: è il file del nostro codice sorgente che rende vero questo fatto. Il repository è privato e resta privato, quindi non si apre da qui: si guarda insieme, a schermo, durante una verifica fornitore sotto accordo di riservatezza.

© 2020–2026 SEMPI S.r.l. — Società Benefit. Tutti i diritti riservati. — Documento pubblico

Deposito del codice presso terzi In preparazione

L’impegno formale a depositare il codice sorgente presso un terzo, o a rilasciarlo in caso di cessazione dell’attività, non è ad oggi sottoscritto. È la richiesta tipica di uno studio strutturato ed è nel programma. Chiedetecelo in sede di trattativa: è una cosa che si può negoziare.

> **COME SI VERIFICA:** Un impegno formale di deposito del codice sorgente presso terzi (source code escrow) o di rilascio in caso di cessazione dell'attività non è ad oggi sottoscritto. È la richiesta tipica di uno studio strutturato ed è nel programma; finché non c'è, si dichiara assente.

Non è un collegamento: è il documento che regge questo fatto, che teniamo agli atti e mandiamo a chi lo chiede. Alcuni non li pubblichiamo perché riportano dati personali — i certificati di deposito, per esempio, contengono l’indirizzo di residenza della depositante, e la data si prova lo stesso con il numero di deposito. Per averli scrivete a dpo@sempi.it

Se Sempi viene venduta, o ne viene ceduto un ramo Attivo

Il contratto lo prevede per iscritto: in caso di acquisizione, fusione o cessione di ramo d'azienda dobbiamo avvisarvi 60 giorni prima, e voi potete recedere senza penali entro 30 giorni dalla notifica (art. 13.3). Alla cessazione, per qualsiasi motivo, restano 30 giorni di accesso in sola lettura per esportare tutto; i dati si cancellano dopo 60. Non è una promessa di non vendere mai: è la garanzia che una vendita non vi trovi legati.

> **COME SI VERIFICA:** legal/CONTRATTO_FORNITURA_SERVIZI_SEMPIX_v1.0.0.md, art. 13.3 — in caso di acquisizione, fusione o cessione di ramo d'azienda il Fornitore deve notificare 60 giorni prima, e il Cliente può recedere senza penali entro 30 giorni dalla notifica. Art. 14.4 dei Termini: alla cessazione restano 30 giorni di accesso in sola lettura per esportare tutto, cancellazione dopo 60.

Non è un collegamento: è il documento che regge questo fatto, che teniamo agli atti e mandiamo a chi lo chiede. Alcuni non li pubblichiamo perché riportano dati personali — i certificati di deposito, per esempio, contengono l’indirizzo di residenza della depositante, e la data si prova lo stesso con il numero di deposito. Per averli scrivete a dpo@sempi.it

Piano di Continuità con data certa Attivo

Le misure di continuità stanno in un documento pubblico e versionato, con una marca temporale qualificata incorporata nel PDF: la data non dipende da quello che diciamo noi. Accanto al documento pubblichiamo la sua impronta SHA-256, così chi lo scarica può ricalcolarla e sapere se ha in mano la nostra versione o una modificata — è la differenza fra dire «è autentico» e lasciarlo verificare.

> **COME SI VERIFICA:** sempix.org/documenti/PIANO_CONTINUITA_SEMPIX.pdf — marca temporale qualificata incorporata nel PDF (PAdES, Reg. UE 910/2014) apposta il 21/09/2026 alle 16:28:17 UTC. Impronta SHA-256 del file marcato: 97b9c6a83232ab42b1953b05fa079a627c4054b537fad9147443b54e4cbcba6e — ricalcolabile da chiunque abbia una copia, per sapere se è la nostra versione o un’altra.

Verificabile da fuori: l’indirizzo qui sotto si apre senza passare da noi. sempix.it/documenti/PIANO_CONTINUITA_SEMPIX.pdf

© 2020–2026 SEMPI S.r.l. — Società Benefit. Tutti i diritti riservati. — Documento pubblico

Se la persona chiave non c'è più Non attiva

Qui non abbiamo ancora una risposta, e preferiamo scriverlo. Non esiste un successore designato per la direzione tecnica, né una delega che sopravviva alla persona, né un deposito del codice sorgente presso un terzo con clausola di rilascio. Quello che esiste, e che non dipende da noi, sono le vie d'uscita: esportazione in formati aperti, scarico del backup della vostra azienda direttamente dall'applicazione, e conservazione a norma dei documenti fiscali presso conservatori accreditati AgID, che sta fuori da Sempix. È la domanda giusta da farci, e la stiamo affrontando: quando ci sarà un atto, comparirà qui con la sua data.

> **COME SI VERIFICA:** Nessun atto agli atti: non esiste un successore designato per la direzione tecnica, né una procura o delega operativa che sopravviva alla persona, né un deposito del codice sorgente presso un terzo con clausola di rilascio (vedi continuity.exit-strategy). Restano comunque esigibili, perché sono del Cliente e non nostri: export in formati aperti, scarico del backup della propria azienda dall'applicazione, e conservazione a norma presso conservatori accreditati AgID, che è fuori da Sempix.

Non è un collegamento: è il documento che regge questo fatto, che teniamo agli atti e mandiamo a chi lo chiede. Alcuni non li pubblichiamo perché riportano dati personali — i certificati di deposito, per esempio, contengono l'indirizzo di residenza della depositante, e la data si prova lo stesso con il numero di deposito. Per averli scrivete a dpo@sempi.it

Piano di Continuità del Servizio

Le misure di continuità sono raccolte in un documento a sé, pubblico e versionato, e tradotte in un articolo dei Termini di Servizio (art. 9-bis): 30 giorni di accesso in sola lettura per esportare tutto alla cessazione — impegno senza riserve, perché i dati sono del cliente — 60 giorni di preavviso in caso di cessione della società o del ramo d'azienda, e il rilascio del codice sorgente necessario alla continuità se Sempix cessasse definitivamente senza una soluzione sostitutiva, con licenza limitata all'uso interno e alla manutenzione.

> Due limiti, detti qui invece che scoperti dopo. Primo: un deposito del codice presso un terzo indipendente (escrow) NON è in essere, e non lo dichiariamo — si può attivare, ed è una cosa che si negozia. Secondo: in caso di liquidazione giudiziale il codice è un bene del patrimonio e la sua sorte è rimessa agli organi della procedura, che possono sciogliersi dai rapporti pendenti (art. 172 CCII). Un impegno del fornitore non vincola la procedura: è esattamente il motivo per cui un escrow costituito prima darebbe una garanzia che il Piano da solo non dà.

> **COME SI VERIFICA:** Il Piano è pubblicato su sempix.it/documenti/PIANO_CONTINUITA_SEMPIX.pdf e l'art. 9-bis è nei Termini di Servizio pubblici. Il Piano riporta versione e data; la versione sottoscritta con firma digitale e marca temporale qualificata è pubblicata insieme alla propria impronta SHA-256, che chiunque può ricalcolare sulla copia che ha.

Partner tecnologici

Una società giovane non può garantire per sé stessa con l'anzianità. Può però dire su quali spalle sta: ogni fornitore qui sotto porta un'autorizzazione che qualcuno gli ha dato dopo averlo controllato, e che potete verificare

© 2020–2026 SEMPI S.r.l. — Società Benefit. Tutti i diritti riservati. — Documento pubblico

senza fidarvi di noi.

TAZ IT Services

Server della piattaforma e direzione tecnica dell’infrastruttura.

> **AUTORIZZAZIONE:** Data center nell’Unione Europea (Romania). È il fornitore che risponde della disponibilità fisica delle macchine su cui girano i vostri dati.

GoCardless Ltd.

Lettura dei conti bancari via Open Banking e incassi ricorrenti con addebito diretto SEPA.

> **AUTORIZZAZIONE:** Istituto autorizzato e vigilato per i servizi di informazione sui conti e di disposizione di pagamento ai sensi della PSD2. L’autorizzazione è sua e vale per il canale: non rende autorizzati noi.

Stripe Payments Europe, Ltd.

Incassi con carta di credito e gestione degli abbonamenti.

> **AUTORIZZAZIONE:** Istituto di moneta elettronica autorizzato in Irlanda e vigilato dalla banca centrale irlandese. I numeri delle carte non passano mai dai nostri sistemi: li tratta direttamente Stripe.

OpenAPI S.p.A.

Dati d’impresa italiani (visure, anagrafiche) e servizi documentali.

> **AUTORIZZAZIONE:** Società italiana: i dati di questo servizio sono trattati in Italia, senza trasferimenti fuori dall’Unione Europea.

Namirial S.p.A.

Marca temporale qualificata e firma digitale qualificata.

> **AUTORIZZAZIONE:** Prestatore di servizi fiduciari QUALIFICATO ai sensi del regolamento eIDAS, iscritto nella Trusted List europea. È quell’iscrizione a dare valore legale alla marca temporale: si può controllare sull’elenco pubblico europeo.

Anthropic, PBC

Modelli linguistici che alimentano ARYA.

> **AUTORIZZAZIONE:** Trasferimento fuori dall’Unione Europea coperto da Clausole Contrattuali Standard. I vostri dati non vengono usati per addestrare modelli: è scritto nell’accordo sul trattamento, non solo qui.

© 2020–2026 SEMPI S.r.l. — Società Benefit. Tutti i diritti riservati. — Documento pubblico

Canali istituzionali

L’Agenzia delle Entrate non è un nostro fornitore: è l’autorità a cui si trasmette. Quello che possiamo dire è per quali canali siamo abilitati, e con quale prova.

Accreditati al Sistema di Interscambio Attivo

L’Agenzia delle Entrate ci ha accreditati come canale di trasmissione: abbiamo superato le prove di interoperabilità con i suoi sistemi e ricevuto i certificati elettronici con cui i nostri si identificano ai suoi. Tre servizi accreditati: invio e ricezione delle fatture verso la Pubblica Amministrazione, e trasmissione dei file dati. È una cosa che si ottiene, non che si dichiara — e l’accordo lo prova.

COME SI VERIFICA: Accordo di Servizio del Sistema di Accreditamento dell'Agenzia delle Entrate, sottoscrittore SEMPI S.R.L. (12315280011), riferimento Rotariu Liana Gabriela. Tre servizi accreditati: SdICoop — Invio della FatturaPA tramite Web Service, SdICoop — Ricezione della FatturaPA tramite Web Service, SdICoop — File Dati trasmessi tramite Web Service. L'accordo copre la trasmissione delle fatture elettroniche verso la Pubblica Amministrazione (D.M. 3 aprile 2013 n. 55), i dati delle fatture emesse e ricevute (D.Lgs. 127/2015, D.L. 193/2016) e le comunicazioni delle liquidazioni periodiche IVA. Documento rilasciato dal portale dell'Agenzia, informazioni valide al 21/09/2026.

Non è un collegamento: è il documento che regge questo fatto, che teniamo agli atti e mandiamo a chi lo chiede. Alcuni non li pubblichiamo perché riportano dati personali — i certificati di deposito, per esempio, contengono l’indirizzo di residenza della depositante, e la data si prova lo stesso con il numero di deposito. Per averli scrivete a dpo@sempi.it

Sistema di Interscambio Attivo

Le fatture elettroniche passano dal canale ufficiale dell’Agenzia delle Entrate. Controlli automatici impediscono che una fattura già consegnata venga modificata o riportata indietro di stato.

COME SI VERIFICA: Invio e ricezione delle fatture elettroniche attraverso il Sistema di Interscambio dell'Agenzia delle Entrate (server/services/sdi/, worker sdiSendWorker). Il canale è protetto da tests/unit/sdiInvoiceGuards.test.ts: una fattura consegnata non può essere declassata né modificata.

Non è un collegamento: è il file del nostro codice sorgente che rende vero questo fatto. Il repository è privato e resta privato, quindi non si apre da qui: si guarda insieme, a schermo, durante una verifica fornitore sotto accordo di riservatezza.

Entratel — invio delle dichiarazioni Attivo

Utenza Entratel intestata alla società, con invii verificati sul campo: la dichiarazione IRAP 2026 è stata trasmessa il 14 settembre 2026 e il protocollo rilasciato dall’Agenzia ne prova la presa in carico. È un fatto controllabile, non una dichiarazione d’intenti.

COME SI VERIFICA: Utenza Entratel intestata a SEMPI S.R.L. (12315280011-000). Trasmissione verificata sul campo: IRAP 2026 inviata il 14/09/2026 alle 14:32 con protocollo 26091414320534330 (shared/fatti-accertati.json). Il protocollo prova la presa in carico da parte dell'Agenzia.

Non è un collegamento: è il file del nostro codice sorgente che rende vero questo fatto. Il repository è privato e resta privato, quindi non si apre da qui: si guarda insieme, a schermo, durante una verifica fornitore sotto accordo di riservatezza.

© 2020–2026 SEMPI S.r.l. — Società Benefit. Tutti i diritti riservati. — Documento pubblico

Deleghe all’Agenzia Attivo

Una delega è un atto che firma il cliente e che va comunicato all’Agenzia. La piattaforma la registra, non la crea: se una delega non è ancora attiva resta in attesa e lo dice, invece di lasciar credere che ci sia.

> **COME SI VERIFICA:** server/services/evai/registroIntermediari.ts — una delega all'Agenzia è un atto firmato dal cliente e comunicato all'Agenzia: la piattaforma la REGISTRA, non la crea. Una delega non ancora attiva resta in attesa e lo dice, invece di far credere che ci sia.

Non è un collegamento: è il file del nostro codice sorgente che rende vero questo fatto. Il repository è privato e resta privato, quindi non si apre da qui: si guarda insieme, a schermo, durante una verifica fornitore sotto accordo di riservatezza.

Conservatori accreditati AgID Attivo

La conservazione a norma è svolta da conservatori accreditati presso l’Agenzia per l’Italia Digitale. L’accreditamento è loro: ci appoggiamo al servizio senza attribuircene la qualifica.

> **COME SI VERIFICA:** Conservazione sostitutiva a norma presso conservatori accreditati AgID. L'accreditamento è loro: noi ci appoggiamo al servizio e non ce ne attribuiamo la qualifica (shared/trust/identity.ts, trust.cert.agid).

Non è un collegamento: è il file del nostro codice sorgente che rende vero questo fatto. Il repository è privato e resta privato, quindi non si apre da qui: si guarda insieme, a schermo, durante una verifica fornitore sotto accordo di riservatezza.

Documenti con data certa

Pubblici, scaricabili senza chiedere niente a nessuno, con una marca temporale qualificata dentro il PDF e l’impronta per riconoscerli.

Questi documenti non sono «disponibili su richiesta»: stanno online e chiunque può scaricarli. Ognuno porta dentro di sé una marca temporale qualificata (PAdES, Reg. UE 910/2014) apposta da un prestatore di servizi fiduciari: la data in cui quel testo esisteva non dipende da quello che diciamo noi, e non possiamo spostarla dopo.

DOCUMENTO	MARCA TEMPORALE	IMPRONTA SHA-256 DEL FILE MARCATO
Piano di Continuità del Servizio SempiX `sempix.it/documenti/PIANO_CONTINUITA_SEMPIX.pdf`	21/09/2026 16:28:17 UTC	`97b9c6a83232ab42b1953b05fa079a627c4054b537fad9147443b54e4cbcba6e`
Dichiarazione di paternità delle opere `sempix.it/documenti/DICHIARAZIONE_PATERNITA.pdf`	21/09/2026 16:40:17 UTC	`0b36f9c45c6fd524a843f950869ff240fdf6e2c081740dfcc9d296dfab617ca9`
Manifesto del codice sorgente `sempix.it/documenti/MANIFESTO_CODICE.pdf`	21/09/2026 16:40:17 UTC	`7d3468b576c5ad5f862e86ad1d33330a7db51e53e155c4a8d44beded78f3cf6c`

© 2020–2026 SEMPI S.r.l. — Società Benefit. Tutti i diritti riservati. — Documento pubblico

DOCUMENTO	MARCA TEMPORALE	IMPRONTA SHA-256 DEL FILE MARCATO
Piano di risposta agli incidenti `sempix.it/documenti/PIANO_RISPOSTA_INCIDENTI.pdf`	21/09/2026 16:40:17 UTC	`abe8eeba49fbf6e13ba2c61a2c1759631fbb78af1a81c74b51b64948ada01598`
Matrice dei permessi per ruolo `sempix.it/documenti/MATRICE_PERMESSI.pdf`	21/09/2026 16:40:17 UTC	`c2ad95ffdddbcad71386707782232da65b1a4bf2a6206bb87fef8e8526bc3747`

> L’impronta serve a una cosa sola, e conta: se la ricalcolate sulla copia che avete scaricato e viene quel numero, avete in mano esattamente il nostro documento. Se viene un numero diverso, qualcuno ve ne ha dato un altro — e vogliamo saperlo.

Chi altro tocca i dati

L’elenco completo dei sub-responsabili, con cosa riceve ciascuno e su quale base giuridica, se fuori dall’Unione Europea.

FORNITORE	DATI CHE RICEVE	DOVE	BASE DEL TRASFERIMENTO
Taz.ro Hosting e infrastruttura (data center, backup)	Tutti i dati della piattaforma, cifrati a riposo. È qui che vive il database della tua azienda.	Romania (Unione Europea)	Nessun trasferimento fuori dall’Unione Europea
Anthropic, PBC Modelli di intelligenza artificiale che alimentano ARYA	Il testo della domanda e i dati del documento in lavorazione, con codice fiscale e IBAN mascherati. Non l’intero database, non lo storico contabile, e senza uso per addestramento.	Stati Uniti	Clausole Contrattuali Standard UE 2021/914
Stripe Payments Europe, Ltd. Incasso dell’abbonamento SempiX con carta	I dati di fatturazione dell’abbonamento. Il numero di carta lo raccoglie Stripe sulle proprie pagine: non passa dai nostri server e non lo conserviamo.	Irlanda (UE) / Stati Uniti	Clausole Contrattuali Standard UE per gli eventuali flussi verso gli USA
GoCardless Ltd. Lettura dei movimenti bancari (Open Banking PSD2) e addebiti SEPA verso i tuoi clienti	IBAN, saldi e movimenti dei conti che colleghi tu, solo dopo il tuo consenso esplicito e per la durata del consenso, che scade e va rinnovato.	Regno Unito / Unione Europea	Decisione di adeguatezza UE–Regno Unito

© 2020–2026 SEMPI S.r.l. — Società Benefit. Tutti i diritti riservati. — Documento pubblico

FORNITORE	DATI CHE RICEVE	DOVE	BASE DEL TRASFERIMENTO
OpenAPI S.p.A. Canale accreditato SDI per trasmettere e ricevere le fatture elettroniche	Le fatture elettroniche XML che invii e ricevi, nel formato previsto dal tracciato dell'Agenzia delle Entrate.	Italia (Unione Europea)	Nessun trasferimento fuori dall'Unione Europea

Contatti

A chi scrivere, per cosa, e in quanto tempo rispondiamo.

Responsabile della protezione dei dati (DPO)

Alberto Tripoli — E.A. Enterprise S.r.l.
dpo@sempi.it

Il nostro DPO è esterno, non un dipendente di Sempi. È una scelta, non un ripiego: chi controlla come trattiamo i dati non deve rispondere a chi sviluppa il prodotto (art. 38.6 GDPR). Puoi scrivergli direttamente, anche per contestarci qualcosa.

PER COSA	INDIRIZZO	TEMPO DI RISPOSTA
Domande commerciali e informazioni	info@sempi.it	
Assistenza sulla piattaforma (clienti attivi)	assistenza@sempi.it	Lunedì–venerdì, in orario di ufficio
Diritti GDPR: accesso, rettifica, cancellazione, portabilità	privacy@sempi.it	Nei termini dell'art. 12 GDPR: un mese, prorogabile con avviso motivato
Responsabile della protezione dei dati (DPO)	dpo@sempi.it	
Segnalare una vulnerabilità o un incidente di sicurezza	privacy@sempi.it	Presa in carico entro 24 ore lavorative

© 2020–2026 SEMPI S.r.l. — Società Benefit. Tutti i diritti riservati. — Documento pubblico

ENGLISH VERSION

Sempi Trust Kit

Why trust Sempi — the facts, with their sources

The English text that follows is the same dossier, generated from the same source as the Italian one. Where they differ, the Italian version prevails — it is the one the contracts are written in.

© 2020–2026 SEMPI S.r.l. — Società Benefit. Tutti i diritti riservati. — Documento pubblico

How to read this document

The criterion, stated before the facts.

This dossier gathers what you need in order to decide whether to entrust us with the work of a firm or a company. It is built on a single criterion, and it is worth stating it up front because it is also how you can hold us to it: **every statement in here is either verifiable from outside, or it is not here**.

Three consequences follow from that criterion, and you will notice them as you read:

- **Every fact says where it can be verified.** Not «the data is encrypted», but which algorithm, in which part of the system, and how you can check it.
- **What we do not have is written down like what we do.** You will find «not active» and «in preparation» next to «active». A dossier without a single weak point is not reassuring: it is incomplete, and whoever is assessing it knows that.
- **Nothing is written by hand.** The document is generated from the platform's own code. If a figure changes, it changes here, on the public page and in the contracts together — and an automated check prevents the three versions from diverging.

> A note on this document's honesty, because it concerns you directly. Writing it made us discover that three of our contractual documents declared certifications we do not hold and security measures that were not in place. We corrected them and wrote it in the revision note, rather than fixing them quietly. If you are running a due diligence, that is information you need.

The company

Who signs the contract, what the public registers say, and what you can check without asking us.

Registered name	SEMPI S.R.L.
Legal form	Limited liability company — Benefit Corporation (Società Benefit)
Registered office	Terrazza Solferino, Via Davide Bertolotti n. 7, 10121 Torino (TO), Italy
VAT / tax number	IT12315280011
REA	TO-1280911
Certified e-mail (PEC)	sempi@legalmail.it
Operating since	July 2020
Product	SempiX

© 2020–2026 SEMPI S.r.l. — Società Benefit. Tutti i diritti riservati. — Documento pubblico

Benefit Corporation Active

We are a Società Benefit (Italian benefit corporation): our articles bind us to pursue, alongside profit, purposes of common benefit and to report on them every year. The status sits in the corporate purpose, introduced in 2021 — not in the name: the registered name is SEMPI S.R.L. We spell this out because on this page the data must match the company register extract, not merely resemble it.

> **HOW TO VERIFY IT:** VISURA ORDINARIA del Registro Imprese di Torino, doc. n. T 670662572 del 21/09/2026. La qualifica risulta dall'OGGETTO SOCIALE («in qualità di Società Benefit, la società intende altresì perseguire finalità di beneficio comune e operare in modo responsabile, sostenibile e trasparente…»), introdotto con l'atto rep. 117848 del 23 luglio 2021 che ha adeguato lo statuto alla normativa su start-up innovative e società benefit (D.L. 179/2012; L. 208/2015 art. 1 c. 376 ss.). ⚠️ NON è nella denominazione: quella iscritta è «SEMPI S.R.L.».

This is not a link: it is the document behind this fact, which we keep on file and send to anyone who asks. Some we do not publish because they carry personal data — the deposit certificates, for instance, contain the depositor's home address, and the date is proven just as well by the deposit number. To obtain them, write to dpo@sempi.it

Innovative startup Active

Registered since 7 February 2025 in the special section of the Italian Business Register reserved for innovative startups, which requires criteria that are verified and reconfirmed every year. The company has been in the ordinary section since 26 June 2020.

> **HOW TO VERIFY IT:** VISURA ORDINARIA del Registro Imprese di Torino, doc. n. T 670662572 del 21/09/2026: «Iscritta nell'apposita sezione speciale in qualità di START-UP INNOVATIVA il 07/02/2025». La società è iscritta nella sezione ORDINARIA dal 26/06/2020.

This is not a link: it is the document behind this fact, which we keep on file and send to anyone who asks. Some we do not publish because they carry personal data — the deposit certificates, for instance, contain the depositor's home address, and the date is proven just as well by the deposit number. To obtain them, write to dpo@sempi.it

Code deposited with a certified date Active

The code of Sempix and of SempiPlancia is deposited in the Patamu Registry — deposits 289744 and 289758 of 31 March 2026 — with a timestamp whose validity is guaranteed by EU Regulation 910/2014 (eIDAS). Each deposit carries the work's SHA-256 fingerprint, which goes into the weekly collective hash Patamu publishes: anyone holding the file can recompute it and see whether it matches. It establishes who wrote what, and when. It is proof of anteriority with an assertable date, not a registration of ownership: we write the difference down because it matters.

> **HOW TO VERIFY IT:** legal/depositi/patamu/2026-03-31_sempix_deposito-289744.pdf e …_sempiplancia_deposito-289758.pdf — certificati Patamu Registry con marcatura temporale 31/03/2026, validità della data certa ai sensi del Reg. UE 910/2014 (eIDAS). Ogni certificato ha la sua pagina pubblica su Patamu: deposito 289744 (SempiX) e 289758 (SempiPlancia), aperte da chiunque senza passare da noi.

Verifiable from outside: the address below opens without going through us. https://www.patamu.com/certificate/289744-907

© 2020–2026 SEMPI S.r.l. — Società Benefit. Tutti i diritti riservati. — Documento pubblico

The Metodo Sempi, not just the software Active

The Metodo Sempi and the Plancia have been deposited as works since 20 September 2021, each with the SHA-256 fingerprint of the deposited file, at a deposit service that attests anteriority in the 176 countries named on the certificate under the Berne Convention. Copyright arises with the work and requires no formality: the deposit serves to date it in a way that cannot be argued with.

> **HOW TO VERIFY IT:** legal/depositi/copyright/2021-09-20_metodo-sempi_DEP637677296077422688.pdf e …_sempiplancia_DEP637677297616258939.pdf — certificati di anteriorità del 20/09/2021 con impronta SHA-256 del file depositato.

This is not a link: it is the document behind this fact, which we keep on file and send to anyone who asks. Some we do not publish because they carry personal data — the deposit certificates, for instance, contain the depositor's home address, and the date is proven just as well by the deposit number. To obtain them, write to dpo@sempi.it

Trade marks filed with the EUIPO Active

SEMPI (application 018556088) and METODO SEMPI (application 018556620) were filed with the EUIPO on 13 September 2021 as figurative marks with word elements, for classes 9, 35, 41 and 42. The current status of each application can be checked on the EUIPO public register with those two numbers, without asking us. The other names we use — Sempix, SempiPlancia, ARYA, Calcolino, e.Vai — are not filed trade marks, and that is why we do not write them with the ® sign.

> **HOW TO VERIFY IT:** legal/depositi/euipo/2021-09-13_domanda-SEMPI_018556088.pdf e …_domanda-METODO-SEMPI_018556620.pdf — ricevute EUIPO di deposito del 13/09/2021; stato aggiornato di ciascuna domanda sul registro pubblico, con quei due numeri.

Verifiable from outside: the address below opens without going through us.
https://euipo.europa.eu/eSearch/#details/trademarks/018556088

Declaration of authorship with a certified date Active

A single document lists who wrote the software, the method and the distinctive signs, with the date of each one and the evidence that proves it — a deposit, a trademark application or a certificate. The PDF carries an embedded qualified timestamp, so the date of the list does not depend on what we say, and next to it we publish its SHA-256 fingerprint so anyone who downloads it can recompute it.

> **HOW TO VERIFY IT:** sempix.org/documenti/DICHIARAZIONE_PATERNITA.pdf — elenco di software, metodo e segni distintivi con la data e la prova di ciascuno; marca temporale qualificata incorporata nel PDF (PAdES, Reg. UE 910/2014) apposta il 21/09/2026 alle 16:40:17 UTC. Impronta SHA-256 del file marcato: 0b36f9c45c6fd524a843f950869ff240fdf6e2c081740dfcc9d296dfab617ca9 — ricalcolabile da chiunque abbia una copia, per sapere se è la nostra versione o un'altra.

Verifiable from outside: the address below opens without going through us.
sempix.it/documenti/DICHIARAZIONE_PATERNITA.pdf

© 2020–2026 SEMPI S.r.l. — Società Benefit. Tutti i diritti riservati. — Documento pubblico

Source code manifest Active

The SHA-256 fingerprint of the whole source tree at a precise commit, inside a PDF with a qualified timestamp. It serves one purpose, and it matters: if one day there is an argument about who wrote what and when, that document proves that on that date the code existed and was exactly that one — not a version rewritten afterwards.

> **HOW TO VERIFY IT:** sempix.org/documenti/MANIFESTO_CODICE.pdf — impronta SHA-256 dell'albero del codice sorgente al commit c108c2e813f6; marca temporale qualificata incorporata nel PDF (PAdES, Reg. UE 910/2014) apposta il 21/09/2026 alle 16:40:17 UTC. Impronta SHA-256 del file marcato: 7d3468b576c5ad5f862e86ad1d33330a7db51e53e155c4a8d44beded78f3cf6c — ricalcolabile da chiunque abbia una copia, per sapere se è la nostra versione o un'altra.

Verifiable from outside: the address below opens without going through us. sempix.it/documenti/MANIFESTO_CODICE.pdf

The numbers, with where they come from

Every measure carries its denominator and the date it was taken. A number without a denominator is not a measurement, it is a feeling.

MEASURE	WHAT IT IS CALCULATED ON	SOURCE AND DATE
99,2% of entries are proposed by the engine, not typed by a person	17,958 entries out of 18,102 created inside SempiX (invoice received from SDI, invoice arriving by email, manual entry) across 86 companies in production. Entries imported from other accounting systems are excluded: our engine did not write those. Older rows, where the system did not record who wrote the entry, count as manual — so the figure is an underestimate.	Read from the 86 production databases with scripts/misura-automazione-tenant.ts — 2026-08-26
4,8 / 5 on Trustpilot	26 public reviews on the Sempi profile. It is the score shown on the profile, not an average we computed ourselves.	Public Trustpilot profile — 2026-08-25
5,0 / 5 on Google	5 public reviews on the "Sempi Srl — Torino" Google Business profile. That is few, and we would rather say so than hide it behind an average.	Public Google Business profile — 2026-08-25

© 2020–2026 SEMPI S.r.l. — Società Benefit. Tutti i diritti riservati. — Documento pubblico

Infrastructure

Where the platform runs, who keeps the service up, and what happens to your data every night.

Servers in the European Union Active

The platform runs on servers in Romania, inside the European Union. Production data does not leave the European Economic Area.

> **HOW TO VERIFY IT:** DATA_LOCATION in shared/trust/identity.ts — server Taz.ro in Romania (Unione Europea). Nessun dato di produzione fuori dallo SEE.

Verifiable from outside: the address below opens without going through us. https://taz.ro

A separate store for each company Active

Each client company's data lives in its own space inside the database, not mixed with the others behind a filter. It is the difference between two archives in two different rooms and two folders in the same drawer: if the filter goes wrong, in the second case you see someone else's data. Automated checks at every release verify that no query can cross the boundary.

> **HOW TO VERIFY IT:** Un solo schema PostgreSQL per azienda cliente (server/multiTenantDb.ts). L'isolamento è verificato dai test tests/unit/aryaTenantScopingGuards.test.ts e collaboratorPortalIsolation.test.ts, e dalle guardie check:salti-tenant, check:storage-tenant e check:sql-filtra-azienda in CI.

This is not a link: it is the file in our source code that makes this fact true. The repository is private and stays private, so it does not open from here: we look at it together, on screen, during a supplier assessment under a non-disclosure agreement.

Encrypted copies, kept for 30 days Active

Backups are compressed and encrypted, on a disk that survives deployments, and are kept for 30 days. Two different things should not be confused: the law requires tax DOCUMENTS to be retained for ten years, and that is what certified archiving does. Keeping 3,650 full copies of the database would serve no one and would fill the disk.

> **HOW TO VERIFY IT:** server/services/backupService.ts — i dump sono compressi e cifrati salvo disattivazione esplicita (BACKUP_ENCRYPTION_ENABLED), scritti sul volume persistente /app/backups. Retention 30 giorni (BACKUP_RETENTION_DAYS): la conservazione decennale riguarda i DOCUMENTI fiscali ed è compito della conservazione sostitutiva a norma, non di 3.650 copie complete del database.

This is not a link: it is the file in our source code that makes this fact true. The repository is private and stays private, so it does not open from here: we look at it together, on screen, during a supplier assessment under a non-disclosure agreement.

© 2020–2026 SEMPI S.r.l. — Società Benefit. Tutti i diritti riservati. — Documento pubblico

Restoring has actually been tested Active

A backup nobody has ever tried to restore is not a backup: it is a file. We have a tool that takes a copy, restores it onto a throwaway database and checks not only that the data reads back, but that the books balance. It was calibrated on three cases: a healthy copy, one with unbalanced accounts and a truncated file. It recognises the first two for what they are and declares the third failed.

> **HOW TO VERIFY IT:** scripts/backup-restore-drill.ts — ripristina un dump su un database temporaneo e verifica che i dati siano leggibili E che la Prima Nota quadri. Collaudato il 25/07/2026 su tre scenari (backup sano, contabilità sbilanciata, dump troncato): riconosce i primi due come tali e dichiara fallito il terzo. Un backup che non sai ripristinare non è un backup.

This is not a link: it is the file in our source code that makes this fact true. The repository is private and stays private, so it does not open from here: we look at it together, on screen, during a supplier assessment under a non-disclosure agreement.

Redundancy and scalability In preparation

Today the companies' data sits on a single database, with no dedicated cluster. With the partner that runs our infrastructure we defined, in September 2026, the plan to move to a redundant database, a cluster separate from the application and horizontal scaling, sized for the roughly 650 companies expected by early 2027. We write it as a plan because it is a plan: the day it is live, this line will change status.

> **HOW TO VERIFY IT:** Piano architetturale concordato con TAZ IT Services (Mihai Ola) il 19/09/2026: ridondanza del database, cluster PostgreSQL separato dall'applicazione, più worker, scalabilità orizzontale e riduzione automatica delle risorse. Stato attuale: i tenant condividono lo stesso database, senza cluster dedicato né pool di connessioni.

This is not a link: it is the document behind this fact, which we keep on file and send to anyone who asks. Some we do not publish because they carry personal data — the deposit certificates, for instance, contain the depositor's home address, and the date is proven just as well by the deposit number. To obtain them, write to dpo@sempi.it

Separate environments and rollback In preparation

Today a release goes straight to production, protected by the 120-plus automated checks that run beforehand. A separate staging environment with automatic rollback is still missing, and it is the second item of the plan agreed with our infrastructure partner. We would rather tell you now than have you find it during an audit.

> **HOW TO VERIFY IT:** Stato attuale verificabile nel repository: il ramo `Sempi` è il ramo di produzione e ogni push ricostruisce e rilascia (CLAUDE.md, scripts/rilascia.sh). Ambienti di prova e produzione separati, con ripristino automatico della versione precedente, sono concordati nel piano con TAZ del 19/09/2026 e non sono ancora in essere.

This is not a link: it is the file in our source code that makes this fact true. The repository is private and stays private, so it does not open from here: we look at it together, on screen, during a supplier assessment under a non-disclosure agreement.

© 2020–2026 SEMPI S.r.l. — Società Benefit. Tutti i diritti riservati. — Documento pubblico

More than 120 checks before every release Active

The automated checks — types, style, tests, accounting verifications and isolation between companies — run inside the build of the release, not alongside it. Which means a build that fails them never reaches production: it is not discouraged, it is impossible.

> **HOW TO VERIFY IT:** scripts/ci-nostra.mjs gira dentro Dockerfile.coolify: oltre 120 controlli automatici (typecheck, lint, test, guardie contabili e di isolamento) sono eseguiti DURANTE la costruzione dell'immagine. Un rilascio non controllato non è sconsigliato: è impossibile.

This is not a link: it is the file in our source code that makes this fact true. The repository is private and stays private, so it does not open from here: we look at it together, on screen, during a supplier assessment under a non-disclosure agreement.

Security

How access and data are protected, and how it is reconstructed who did what.

Encrypted credentials Active

Credentials and sensitive data are encrypted with AES-256-GCM, an algorithm that besides hiding the content notices if someone has tampered with it. The key is not the password: a dedicated one is derived from it with 100,000 rounds, so brute-forcing it is not worth the effort.

> **HOW TO VERIFY IT:** server/encryption.ts e server/services/credentialEncryptionService.ts — AES-256-GCM (cifratura autenticata) con chiave derivata via PBKDF2-SHA256 a 100.000 iterazioni. La guardia check:colonne-cifrate in CI verifica che le colonne sensibili non finiscano in chiaro.

This is not a link: it is the file in our source code that makes this fact true. The repository is private and stays private, so it does not open from here: we look at it together, on screen, during a supplier assessment under a non-disclosure agreement.

Encrypted traffic Active

All communication between your browser and the platform travels over HTTPS.

> **HOW TO VERIFY IT:** HTTPS obbligatorio su tutti i domini di produzione, certificati gestiti da Coolify.

This is not a link: it is the document behind this fact, which we keep on file and send to anyone who asks. Some we do not publish because they carry personal data — the deposit certificates, for instance, contain the depositor's home address, and the date is proven just as well by the deposit number. To obtain them, write to dpo@sempi.it

© 2020–2026 SEMPI S.r.l. — Società Benefit. Tutti i diritti riservati. — Documento pubblico

Role-based permissions Active

Each person sees what their role allows: owner, accountant, operator, read-only. ARYA has a role of its own, the most limited of all: it can prepare drafts and read reports, it cannot post anything by itself.

> **HOW TO VERIFY IT:** docs/compliance/RBAC_MATRIX.md — ruoli OWNER / ACCOUNTANT / CLERK / VIEWER più AI_BOT (ARYA, limitata alle bozze e alla lettura). Le operazioni ad alto rischio sono elencate con la loro frequenza di revisione. Pubblicata anche come PDF su sempix.org/documenti/MATRICE_PERMESSI.pdf, con marca temporale qualificata incorporata nel PDF (PAdES, Reg. UE 910/2014) apposta il 21/09/2026 alle 16:40:17 UTC. Impronta SHA-256 del file marcato: c2ad95ffdddbcad71386707782232da65b1a4bf2a6206bb87fef8e8526bc3747 — ricalcolabile da chiunque abbia una copia, per sapere se è la nostra versione o un'altra.

Verifiable from outside: the address below opens without going through us. sempix.it/documenti/MATRICE_PERMESSI.pdf

Two-factor sign-in Active

Two-factor authentication is available for every account. Available, not enforced: whoever wants to make it mandatory for the whole firm decides that from the panel. We write it as it is, because «we have two-factor authentication» and «two-factor authentication is on for everyone» are two different sentences.

> **HOW TO VERIFY IT:** Autenticazione a due fattori disponibile per ogni utenza (pagina /2fa-settings, server/services/codiceEmail2fa.ts). È disponibile, non imposta: chi deve renderla obbligatoria per il proprio studio lo decide dal pannello, e va detto com'è.

This is not a link: it is the file in our source code that makes this fact true. The repository is private and stays private, so it does not open from here: we look at it together, on screen, during a supplier assessment under a non-disclosure agreement.

Log of access and changes Active

Creations, changes, deletions, reads, exports and logins are recorded with date, time and author. The most delicate case has an entry of its own: when a platform administrator accesses a company's data, that access is recorded as such and the list can be requested.

> **HOW TO VERIFY IT:** server/services/auditLogService.ts — registra creazioni, modifiche, cancellazioni, letture, esportazioni, accessi e — voce a sé — gli accessi amministrativi trasversali fra aziende (ADMIN_CROSS_COMPANY_ACCESS). Consultabile dalla pagina /admin-audit-log.

This is not a link: it is the file in our source code that makes this fact true. The repository is private and stays private, so it does not open from here: we look at it together, on screen, during a supplier assessment under a non-disclosure agreement.

© 2020–2026 SEMPI S.r.l. — Società Benefit. Tutti i diritti riservati. — Documento pubblico

Every accounting correction leaves a trace Active

If an entry is corrected, it stays on record who changed it, when, and what changed. In Italian accounting a wrong entry is corrected: filling the journal with reversals and re-issues for every correction is irregular bookkeeping, and the Revenue Agency penalises it. So the trace sits in the entry's own history, not in convenience postings.

> **HOW TO VERIFY IT:** ARYA Tutela (server/services/aryaTutelaService.ts, pagine /aryatutela/*) — ogni modifica a una registrazione contabile lascia un evento con chi, quando e cosa è cambiato. In contabilità italiana una scrittura sbagliata si CORREGGE, non si storna per riemetterla: la traccia sta nella cronologia, non in scritture di comodo.

This is not a link: it is the file in our source code that makes this fact true. The repository is private and stays private, so it does not open from here: we look at it together, on screen, during a supplier assessment under a non-disclosure agreement.

Incident response plan Active

Incidents are classified on three levels, each with its own response time: one hour for critical cases, four hours for serious ones, the next working day for minor ones. For critical cases, notification to the competent authority is foreseen within 24 hours.

> **HOW TO VERIFY IT:** docs/compliance/INCIDENT_RESPONSE_PLAN.md v1.0.0 (in vigore dal 14/07/2026) — tre livelli di gravità con tempi di presa in carico (1 ora / 4 ore / giorno lavorativo successivo) e notifica alle autorità entro 24 ore per gli incidenti critici, come richiesto da DORA e NIS2. Pubblicato anche come PDF su sempix.org/documenti/PIANO_RISPOSTA_INCIDENTI.pdf, con marca temporale qualificata incorporata nel PDF (PAdES, Reg. UE 910/2014) apposta il 21/09/2026 alle 16:40:17 UTC. Impronta SHA-256 del file marcato: abe8eeba49fbf6e13ba2c61a2c1759631fbb78af1a81c74b51b64948ada01598 — ricalcolabile da chiunque abbia una copia, per sapere se è la nostra versione o un’altra.

Verifiable from outside: the address below opens without going through us.
sempix.it/documenti/PIANO_RISPOSTA_INCIDENTI.pdf

A whistleblowing channel pointed at Sempi itself Active

Anyone who wants to report unlawful conduct concerning us has a channel of their own, at /segnalazioni: reports can be anonymous, you get a code to follow the case and to write to those responsible without having to identify yourself. It is the same module we sell to clients, pointed at ourselves — if it did not work, we would be the first to notice.

> **HOW TO VERIFY IT:** Canale pubblico su /segnalazioni (alias /whistleblowing), servito dal modulo ARYA Segnalazioni — lo stesso che la piattaforma offre ai clienti. Segnalazione anonima per impostazione predefinita, codice di riscontro per seguire la pratica e scrivere ai responsabili senza rivelarsi, istruttoria tracciata (server/services/segnalazioniService.ts, tabelle segnalazioni / segnalazioni_istruttorie / segnalazioni_comunicazioni). ⚠️ Se l'obbligo di legge (D.Lgs. 24/2023) ricada su Sempi è determinazione del DPO: qui si dichiara che il canale esiste e funziona, non che è dovuto.

Verifiable from outside: the address below opens without going through us. sempix.it/segnalazioni

© 2020–2026 SEMPI S.r.l. — Società Benefit. Tutti i diritti riservati. — Documento pubblico

Third-party penetration test In preparation

A penetration test by an independent third-party firm has not been carried out yet. There are automated tests that, at every release, try to cross the boundary between two companies' data and must fail. The third-party test is scheduled before the certification audit: until it exists, we say so.

> **HOW TO VERIFY IT:** docs/compliance/ISO27001-DORA-NIS2-FRAMEWORK.md, Gap 3: i test di isolamento fra aziende esistono come test automatici, un penetration test formale da società terza indipendente non è ancora stato svolto. Programmato prima dell'audit di certificazione.

This is not a link: it is the document behind this fact, which we keep on file and send to anyone who asks. Some we do not publish because they carry personal data — the deposit certificates, for instance, contain the depositor's home address, and the date is proven just as well by the deposit number. To obtain them, write to dpo@sempi.it

Regulatory compliance

The rules the platform answers to by construction, not by declaration.

Electronic invoicing (SdI) Active

Invoices are issued and received through the Revenue Agency's Interchange System. An invoice that has been delivered can no longer be modified or moved back to draft: it is locked by the system, not by the good intentions of whoever is using it.

> **HOW TO VERIFY IT:** Fatturazione elettronica verso il Sistema di Interscambio dell'Agenzia delle Entrate (server/services/sdi/, pipeline protetta da tests/unit/sdiInvoiceGuards.test.ts). Le fatture emesse sono immutabili e non possono essere declassate dopo la consegna.

This is not a link: it is the file in our source code that makes this fact true. The repository is private and stays private, so it does not open from here: we look at it together, on screen, during a supplier assessment under a non-disclosure agreement.

Qualified signatures and timestamps (eIDAS) Active

Timestamps and signatures that need legal value are applied through a qualified trust service provider under the European eIDAS Regulation. It is the provider's qualification that gives the document its legal value, not the fact that we apply it.

> **HOW TO VERIFY IT:** server/services/namirialTimestampService.ts — marca temporale qualificata eIDAS (Reg. UE 910/2014, art. 41) apposta tramite prestatore di servizi fiduciari qualificato. Firma qualificata (QES) per gli invii che la richiedono: server/services/cadesSignatureService.ts, statoFirmaQualificata.ts.

This is not a link: it is the file in our source code that makes this fact true. The repository is private and stays private, so it does not open from here: we look at it together, on screen, during a supplier assessment under a non-disclosure agreement.

© 2020–2026 SEMPI S.r.l. — Società Benefit. Tutti i diritti riservati. — Documento pubblico

Bank account access (PSD2) Active

Bank transactions are read through an institution authorised as an account information service provider. Access is read-only, starts from a mandate you sign and can be revoked whenever you want: the platform cannot initiate payments from your accounts.

> **HOW TO VERIFY IT:** Lettura dei conti bancari via Open Banking attraverso GoCardless Bank Account Data, istituto autorizzato come AISP ai sensi della direttiva PSD2. Accesso in SOLA LETTURA, su mandato esplicito del cliente e revocabile: Sempix non dispone pagamenti.

This is not a link: it is the document behind this fact, which we keep on file and send to anyone who asks. Some we do not publish because they carry personal data — the deposit certificates, for instance, contain the depositor's home address, and the date is proven just as well by the deposit number. To obtain them, write to dpo@sempi.it

GDPR Active

Processor on your behalf, with an external DPO appointed, the data processing agreement available, a public list of who else touches the data, and data subject rights exercisable from a dedicated page.

> **HOW TO VERIFY IT:** DPO esterno nominato (Alberto Tripoli, E.A. Enterprise S.r.l., shared/trust/identity.ts), DPA ex art. 28 disponibile (legal/ACCORDO_TRATTAMENTO_DATI_PERSONALI_v1.1.0.md), registro dei sub-responsabili pubblico su /trust, diritti degli interessati esercitabili da /gdpr-rights.

This is not a link: it is the file in our source code that makes this fact true. The repository is private and stays private, so it does not open from here: we look at it together, on screen, during a supplier assessment under a non-disclosure agreement.

Certified long-term archiving (CAD / AgID) Active

Legally valid archiving of tax documents is entrusted to accredited providers. We do not perform it ourselves and we do not claim their accreditation — a distinction many suppliers fail to make.

> **HOW TO VERIFY IT:** Conservazione sostitutiva a norma (CAD / linee guida AgID) affidata a conservatori accreditati. Non la svolgiamo noi e non ci attribuiamo il loro accreditamento — shared/trust/identity.ts, voce trust.cert.agid.

This is not a link: it is the file in our source code that makes this fact true. The repository is private and stays private, so it does not open from here: we look at it together, on screen, during a supplier assessment under a non-disclosure agreement.

© 2020–2026 SEMPI S.r.l. — Società Benefit. Tutti i diritti riservati. — Documento pubblico

EU Artificial Intelligence Act In preparation

Registration in the European database of AI systems has not been carried out; the relevant deadline has been postponed to 2 December 2027. Whether ARYA should be classified as high-risk is still an open assessment: two of our internal documents read it differently, and the decision rests with the data protection officer. We prefer to write it this way rather than give you whichever version suits us best.

> **HOW TO VERIFY IT:** Dichiarazione di conformità AI Act (in legal/) e documento di preparazione al registro (in docs, cartella compliance). ⚠️ I due documenti interni si contraddicono sulla classificazione di rischio di ARYA: la Dichiarazione sostiene che nessun sistema rientra nell'Allegato III del Regolamento (UE) 2024/1689 e ne dà la motivazione; il documento ISO27001-DORA-NIS2 la dà per alto rischio senza indicare il punto applicabile. La determinazione spetta al DPO ed è aperta. Quello che è certo e non dipende da quale lettura prevalga: la registrazione al registro europeo NON è stata effettuata, e il termine rilevante è stato differito al 2 dicembre 2027. Pagina pubblica /ai-act.

Verifiable from outside: the address below opens without going through us. sempix.it/ai-act

Accessibility Active

The accessibility statement is published. Two automated checks prevent a new screen from being born with unreadable text or with insufficient contrast in dark mode.

> **HOW TO VERIFY IT:** Dichiarazione di accessibilità pubblicata su /dichiarazione-accessibilita. In CI le guardie check:a11y-legibility e check:dark-contrast impediscono che una schermata nuova nasca illeggibile.

Verifiable from outside: the address below opens without going through us. sempix.it/dichiarazione-accessibilita

Certifications

We keep the distinction between «held» and «in preparation» even when it works against us. A certification declared and not held is not a rounding error: it is an untrue statement.

REFERENCE	STATUS	WHAT IT MEANS
ISO/IEC 27001	In preparation — NOT held	Process started. We are not certified: when we are, the certificate will be published here with its number and the issuing body.
SOC 2 Type II	In preparation — NOT held	Process started. No attestation issued by an independent auditor yet.
GDPR — data protection by design (art. 25)	Applied	Measures adopted and documented in the DPA and the record of processing activities, with per-company data separation and access logging.

© 2020–2026 SEMPI S.r.l. — Società Benefit. Tutti i diritti riservati. — Documento pubblico

REFERENCE	STATUS	WHAT IT MEANS
Legal digital preservation under CAD / AgID	Applied	Legally compliant digital preservation is handled by AgID-accredited providers (Aruba, InfoCert, Namirial and others). We do not perform it ourselves, and we do not claim their accreditation.

Artificial intelligence governance

ARYA is the assistant that prepares the accounting work. The sentence that describes its role is this: the model writes the explanation, the accounting engine applies the rule, the person decides. Here is what happens to an invoice, step by step.

ARYA is the assistant that prepares the accounting work. The sentence that describes its role is this: the model writes the explanation, the accounting engine applies the rule, the person decides. Here is what happens to an invoice, step by step.

1. **It reads the document, it does not guess it**
   Supplier, number, date, taxable amount, VAT and description are read from the PDF or the XML. If a value is not in the document it stays empty and is flagged: it is never inferred from a similar invoice.
2. **It proposes the entry, with the reason**
   The proposal arrives with the suggested account and the reason in plain language — not the name of an internal function — plus a confidence level saying how sure it is.
3. **The accounting engine checks the proposal**
   Double entry, VAT rate, consistency of the account with the chart of accounts, reverse charge, withholding tax. A proposal that fails these checks never even reaches your confirmation.
4. **You confirm, and you can correct**
   Nothing enters the journal without a person confirming it. You can accept, correct or reject: correcting is the normal path, not a fallback.
5. **A record of who decided what remains**
   Every confirmation and every later correction goes into the entry’s history with who, when and what changed. A wrong entry is corrected and the change stays on record: it is not deleted, and it is not reversed for show.

> **Example.** “Development costs, VAT under reverse charge: the supplier is outside the EU and the description ‘Autorecharge credits’ matches development credits already booked to this account three times this year. High confidence. Confirm or correct?”

The limits, said plainly: ARYA gets things wrong, especially with new suppliers and cases it has never seen. That is why human confirmation is not a formality we will remove once the model gets better — it is the point where professional responsibility stays with whoever carries it by law.

© 2020–2026 SEMPI S.r.l. — Società Benefit. Tutti i diritti riservati. — Documento pubblico

What we do NOT do

We do not know your bank credentials.

The connection goes through GoCardless, authorised as an AISP under PSD2: you enter your credentials on your bank's own pages, not on ours. What reaches us is a time-limited consent you can revoke at any moment, granting read-only access to movements.

We do not initiate payments from your account.

Bank synchronisation is read-only: it reads movements, it does not originate them. SEPA direct debits exist in the platform for the collections YOU set up towards YOUR customers, under a mandate they sign: that is a separate feature, switched on separately and named in the contract.

Your data does not train AI models.

Neither ours nor our suppliers'. What goes to the external model is the text of the question and the document being processed, with tax codes and IBANs masked, under a contract that excludes use for training.

The AI does not write into your books on its own.

It proposes an entry; what writes it is the accounting engine, applying deterministic rules rather than a language model, after a person confirms. A rejected proposal leaves no trace in the journal.

If you leave, the data leaves with you.

Export of master data, journal entries, invoices and attachments in open formats, at any time, without asking our permission and with no exit fee. When the relationship ends the data is returned and then deleted, except for what the law requires us to keep.

Insurance

What is covered and what is not. A cover we do not have we write down anyway: finding out after an incident is

© 2020–2026 SEMPI S.r.l. — Società Benefit. Tutti i diritti riservati. — Documento pubblico

worse than knowing beforehand.

Professional indemnity Active

Professional indemnity cover through membership of APCO, the Italian association of management consultants: insurer Lloyd's, limit €150,000 per claim and in the annual aggregate plus 25% for legal costs, €2,500 deductible, retroactive to 31 December 2014, worldwide excluding the USA and Canada. ⚠️ It covers CONSULTING work, which is a different thing from software: it is neither a Tech E&O on the product nor a cyber policy. We tell you ourselves because that is the distinction that matters if you are assessing the risk of entrusting us with your data.

Insurer: Lloyd's Insurance Company S.A. · **Limit:** € 150.000 per sinistro e in aggregato annuo, +25% per spese legali · **Expiry:** 2027-06-27

Cyber insurance Not active

It covers damage from a cyber attack, a data breach and service interruption: notification costs, recovery, third-party claims. We do not have it today. It has to be said, because it is the cover a structured firm expects to find, and it would be unfair to let them infer it from the others.

Tech E&O (software errors) Not active

It covers damage caused by a defect in the software product, which is a different thing from the consultant's liability. We do not have it today, and a consulting cover is no substitute.

Continuity

The awkward question: what if Sempi were not here tomorrow? The answer is not «it will not happen» — it is to keep the cost of leaving low, before you need to.

Your data leaves in open formats Active

Financial statements, the journal, VAT registers, master data and invoices export in formats other accounting systems can read. There is no proprietary format on the way out: it is the first thing to check in any supplier, because it decides whether you can really leave.

> **HOW TO VERIFY IT:** Esportazioni in formati aperti e leggibili da altri gestionali: bilanci e Prima Nota (server/routes/accountingExportRoutes.ts, bilancioExportRoutes.ts), registri IVA (vatExportRoutes.ts), anagrafiche (anagraficheImportExportRoutes.ts), fatture in XML SDI. Nessun formato proprietario sulla via d'uscita.

This is not a link: it is the file in our source code that makes this fact true. The repository is private and stays private, so it does not open from here: we look at it together, on screen, during a supplier assessment under a non-disclosure agreement.

© 2020–2026 SEMPI S.r.l. — Società Benefit. Tutti i diritti riservati. — Documento pubblico

After cancellation your data stays readable Active

When the subscription ends, read access and export remain guaranteed: what stops is entering new bookkeeping entries. It is not a courtesy — it follows from the duty to retain accounting records and from the right to data portability.

> **HOW TO VERIFY IT:** server/services/subscriptionAccessGate.ts — alla cessazione dell'abbonamento restano garantiti la lettura e l'esportazione dei dati; è l'inserimento di nuove scritture a essere bloccato. Deriva dagli obblighi di conservazione (art. 2220 c.c.) e dal diritto alla portabilità (art. 20 GDPR).

This is not a link: it is the file in our source code that makes this fact true. The repository is private and stays private, so it does not open from here: we look at it together, on screen, during a supplier assessment under a non-disclosure agreement.

Data portability (art. 20 GDPR) Active

A portability request is made from a dedicated page, where you also state the format you want the data in.

> **HOW TO VERIFY IT:** server/routes/gdprRoutes.ts — richiesta di portabilità (art. 20 GDPR) esercitabile dalla pagina /gdpr-rights, con indicazione del formato dati desiderato.

Verifiable from outside: the address below opens without going through us. sempix.it/gdpr-rights

Legally valid documents are not only here Active

Tax documents under certified archiving sit with accredited providers, not inside the platform. They remain reachable independently of us: it is the most concrete part of the answer to «what if you disappear tomorrow?».

> **HOW TO VERIFY IT:** La conservazione sostitutiva a norma dei documenti fiscali è presso conservatori accreditati AgID, non dentro Sempix: i documenti con valore legale restano raggiungibili dal cliente anche indipendentemente dalla piattaforma.

This is not a link: it is the document behind this fact, which we keep on file and send to anyone who asks. Some we do not publish because they carry personal data — the deposit certificates, for instance, contain the depositor's home address, and the date is proven just as well by the deposit number. To obtain them, write to dpo@sempi.it

Full restore drill In preparation

Recovery time objectives are defined and the procedure is tested on test databases. A full, timed drill on the live environment has not been carried out yet: until we do it, a stated objective remains an objective, not a measurement.

> **HOW TO VERIFY IT:** Obiettivi RTO/RPO definiti nei documenti contrattuali e la procedura di ripristino è collaudata (scripts/backup-restore-drill.ts). Non è invece ancora stata eseguita una prova di disaster recovery completa e cronometrata sull'ambiente di produzione: finché non lo è, gli obiettivi restano obiettivi.

This is not a link: it is the file in our source code that makes this fact true. The repository is private and stays private, so it does not open from here: we look at it together, on screen, during a supplier assessment under a non-disclosure agreement.

© 2020–2026 SEMPI S.r.l. — Società Benefit. Tutti i diritti riservati. — Documento pubblico

Source code escrow In preparation

A formal undertaking to deposit the source code with a third party, or to release it should the business cease, is not in place today. It is the typical request of a structured firm and it is on the plan. Ask us for it during negotiation: it is something that can be agreed.

> **HOW TO VERIFY IT:** Un impegno formale di deposito del codice sorgente presso terzi (source code escrow) o di rilascio in caso di cessazione dell'attività non è ad oggi sottoscritto. È la richiesta tipica di uno studio strutturato ed è nel programma; finché non c'è, si dichiara assente.

This is not a link: it is the document behind this fact, which we keep on file and send to anyone who asks. Some we do not publish because they carry personal data — the deposit certificates, for instance, contain the depositor's home address, and the date is proven just as well by the deposit number. To obtain them, write to dpo@sempi.it

If Sempi is sold, or a business unit is transferred Active

The contract says so in writing: in the event of an acquisition, a merger or the transfer of a business unit we must give you 60 days' notice, and you may withdraw without penalty within 30 days of that notice (art. 13.3). On termination, for any reason, you keep 30 days of read-only access to export everything; data is deleted after 60. It is not a promise never to sell: it is the guarantee that a sale will not find you tied in.

> **HOW TO VERIFY IT:** legal/CONTRATTO_FORNITURA_SERVIZI_SEMPIX_v1.0.0.md, art. 13.3 — in caso di acquisizione, fusione o cessione di ramo d'azienda il Fornitore deve notificare 60 giorni prima, e il Cliente può recedere senza penali entro 30 giorni dalla notifica. Art. 14.4 dei Termini: alla cessazione restano 30 giorni di accesso in sola lettura per esportare tutto, cancellazione dopo 60.

This is not a link: it is the document behind this fact, which we keep on file and send to anyone who asks. Some we do not publish because they carry personal data — the deposit certificates, for instance, contain the depositor's home address, and the date is proven just as well by the deposit number. To obtain them, write to dpo@sempi.it

Continuity Plan with a certified date Active

The continuity measures live in a public, versioned document carrying a qualified timestamp embedded in the PDF: the date does not depend on what we say. Next to the document we publish its SHA-256 fingerprint, so whoever downloads it can recompute it and know whether they hold our version or an altered one — the difference between saying «it is genuine» and letting you check.

> **HOW TO VERIFY IT:** sempix.org/documenti/PIANO_CONTINUITA_SEMPIX.pdf — marca temporale qualificata incorporata nel PDF (PAdES, Reg. UE 910/2014) apposta il 21/09/2026 alle 16:28:17 UTC. Impronta SHA-256 del file marcato: 97b9c6a83232ab42b1953b05fa079a627c4054b537fad9147443b54e4cbcba6e — ricalcolabile da chiunque abbia una copia, per sapere se è la nostra versione o un'altra.

Verifiable from outside: the address below opens without going through us.
sempix.it/documenti/PIANO_CONTINUITA_SEMPIX.pdf

© 2020–2026 SEMPI S.r.l. — Società Benefit. Tutti i diritti riservati. — Documento pubblico

If the key person is no longer there Not active

Here we do not have an answer yet, and we would rather write that down. There is no designated successor for technical leadership, no mandate that survives the person, and no source-code escrow with a release clause. What does exist, and does not depend on us, are the ways out: export in open formats, download of your company's backup straight from the application, and certified long-term archiving of tax documents with AgID-accredited providers, which sits outside Sempix. It is the right question to ask us, and we are working on it: when there is a deed, it will appear here with its date.

HOW TO VERIFY IT: Nessun atto agli atti: non esiste un successore designato per la direzione tecnica, né una procura o delega operativa che sopravviva alla persona, né un deposito del codice sorgente presso un terzo con clausola di rilascio (vedi continuity.exit-strategy). Restano comunque esigibili, perché sono del Cliente e non nostri: export in formati aperti, scarico del backup della propria azienda dall'applicazione, e conservazione a norma presso conservatori accreditati AgID, che è fuori da Sempix.

This is not a link: it is the document behind this fact, which we keep on file and send to anyone who asks. Some we do not publish because they carry personal data — the deposit certificates, for instance, contain the depositor's home address, and the date is proven just as well by the deposit number. To obtain them, write to dpo@sempi.it

Service Continuity Plan

The continuity measures are collected in a document of their own, public and versioned, and translated into an article of the Terms of Service (art. 9-bis): 30 days of read-only access to export everything on termination — an unconditional commitment, because the data belongs to the client — 60 days' notice if the company or a business unit is sold, and the release of the source code needed for continuity should Sempix be discontinued for good with no replacement available, under a licence limited to internal use and maintenance.

> Two limits, stated here rather than discovered later. First: a source-code deposit with an independent third party (escrow) is NOT in place, and we do not claim it is — it can be set up, and it is something to be negotiated. Second: in a judicial liquidation the code is an asset of the estate and its fate rests with the insolvency bodies, which may withdraw from pending contracts (art. 172 of the Italian insolvency code). A supplier's undertaking does not bind the procedure: which is precisely why an escrow set up beforehand would give a guarantee the Plan alone does not.

HOW TO VERIFY IT: The Plan is published at sempix.it/documenti/PIANO_CONTINUITA_SEMPIX.pdf and art. 9-bis is in the public Terms of Service. The Plan carries a version and a date; the version signed with a digital signature and a qualified timestamp is published together with its SHA-256 fingerprint, which anyone can recompute on the copy they hold.

Technology partners

A young company cannot vouch for itself with seniority. It can, however, say whose shoulders it stands on: every supplier below carries an authorisation someone granted after checking them, and which you can verify without

© 2020–2026 SEMPI S.r.l. — Società Benefit. Tutti i diritti riservati. — Documento pubblico

trusting us.

TAZ IT Services

Platform servers and technical direction of the infrastructure.

> **AUTHORISATION:** Data centre in the European Union (Romania). This is the supplier answerable for the physical availability of the machines your data runs on.

GoCardless Ltd.

Reading bank accounts via Open Banking and recurring collections by SEPA direct debit.

> **AUTHORISATION:** An institution authorised and supervised for account information and payment initiation services under PSD2. The authorisation is theirs and applies to the channel: it does not make us authorised.

Stripe Payments Europe, Ltd.

Card payments and subscription management.

> **AUTHORISATION:** An electronic money institution authorised in Ireland and supervised by the Central Bank of Ireland. Card numbers never pass through our systems: Stripe handles them directly.

OpenAPI S.p.A.

Italian company data (register extracts, master data) and document services.

> **AUTHORISATION:** An Italian company: the data of this service is processed in Italy, with no transfers outside the European Union.

Namirial S.p.A.

Qualified timestamping and qualified electronic signature.

> **AUTHORISATION:** A QUALIFIED trust service provider under the eIDAS Regulation, listed on the European Trusted List. It is that listing that gives the timestamp its legal value: it can be checked on the public European list.

Anthropic, PBC

The language models behind ARYA.

> **AUTHORISATION:** Transfer outside the European Union covered by Standard Contractual Clauses. Your data is not used to train models: it is written in the processing agreement, not only here.

© 2020–2026 SEMPI S.r.l. — Società Benefit. Tutti i diritti riservati. — Documento pubblico

Institutional channels

The Italian Revenue Agency is not a supplier of ours: it is the authority you transmit to. What we can state is which channels we are authorised for, and with what proof.

Accredited with the Interchange System (SdI) Active

The Italian Revenue Agency has accredited us as a transmission channel: we passed the interoperability tests against its systems and received the electronic certificates our systems use to identify themselves to its own. Three accredited services: sending and receiving invoices to and from public administrations, and transmitting data files. It is something you obtain, not something you declare — and the agreement proves it.

> **HOW TO VERIFY IT:** Accordo di Servizio del Sistema di Accreditamento dell'Agenzia delle Entrate, sottoscrittore SEMPI S.R.L. (12315280011), riferimento Rotariu Liana Gabriela. Tre servizi accreditati: SdICoop — Invio della FatturaPA tramite Web Service, SdICoop — Ricezione della FatturaPA tramite Web Service, SdICoop — File Dati trasmessi tramite Web Service. L'accordo copre la trasmissione delle fatture elettroniche verso la Pubblica Amministrazione (D.M. 3 aprile 2013 n. 55), i dati delle fatture emesse e ricevute (D.Lgs. 127/2015, D.L. 193/2016) e le comunicazioni delle liquidazioni periodiche IVA. Documento rilasciato dal portale dell'Agenzia, informazioni valide al 21/09/2026.

This is not a link: it is the document behind this fact, which we keep on file and send to anyone who asks. Some we do not publish because they carry personal data — the deposit certificates, for instance, contain the depositor's home address, and the date is proven just as well by the deposit number. To obtain them, write to dpo@sempi.it

Interchange System (SdI) Active

Electronic invoices go through the Revenue Agency's official channel. Automatic checks prevent an invoice that has already been delivered from being modified or moved back to an earlier status.

> **HOW TO VERIFY IT:** Invio e ricezione delle fatture elettroniche attraverso il Sistema di Interscambio dell'Agenzia delle Entrate (server/services/sdi/, worker sdiSendWorker). Il canale è protetto da tests/unit/sdiInvoiceGuards.test.ts: una fattura consegnata non può essere declassata né modificata.

This is not a link: it is the file in our source code that makes this fact true. The repository is private and stays private, so it does not open from here: we look at it together, on screen, during a supplier assessment under a non-disclosure agreement.

Entratel — filing tax returns Active

An Entratel account in the company's name, with filings verified in the field: the 2026 IRAP return was transmitted on 14 September 2026 and the receipt number issued by the Revenue Agency proves it was taken in charge. That is a checkable fact, not a statement of intent.

> **HOW TO VERIFY IT:** Utenza Entratel intestata a SEMPI S.R.L. (12315280011-000). Trasmissione verificata sul campo: IRAP 2026 inviata il 14/09/2026 alle 14:32 con protocollo 26091414320534330 (shared/fatti-accertati.json). Il protocollo prova la presa in carico da parte dell'Agenzia.

This is not a link: it is the file in our source code that makes this fact true. The repository is private and stays private, so it does not open from here: we look at it together, on screen, during a supplier assessment under a non-disclosure agreement.

© 2020–2026 SEMPI S.r.l. — Società Benefit. Tutti i diritti riservati. — Documento pubblico

Mandates with the Revenue Agency Active

A mandate is a deed the client signs and that must be notified to the Revenue Agency. The platform records it, it does not create it: if a mandate is not active yet it stays pending and says so, instead of letting you believe it is in place.

> **HOW TO VERIFY IT:** server/services/evai/registroIntermediari.ts — una delega all'Agenzia è un atto firmato dal cliente e comunicato all'Agenzia: la piattaforma la REGISTRA, non la crea. Una delega non ancora attiva resta in attesa e lo dice, invece di far credere che ci sia.

This is not a link: it is the file in our source code that makes this fact true. The repository is private and stays private, so it does not open from here: we look at it together, on screen, during a supplier assessment under a non-disclosure agreement.

AgID-accredited archiving providers Active

Certified long-term archiving is carried out by providers accredited with the Agency for Digital Italy. The accreditation is theirs: we rely on the service without claiming their status.

> **HOW TO VERIFY IT:** Conservazione sostitutiva a norma presso conservatori accreditati AgID. L'accreditamento è loro: noi ci appoggiamo al servizio e non ce ne attribuiamo la qualifica (shared/trust/identity.ts, trust.cert.agid).

This is not a link: it is the file in our source code that makes this fact true. The repository is private and stays private, so it does not open from here: we look at it together, on screen, during a supplier assessment under a non-disclosure agreement.

Documents with a certified date

Public, downloadable without asking anyone for anything, with a qualified timestamp inside the PDF and the fingerprint to recognise them.

These documents are not «available on request»: they are online and anyone can download them. Each carries inside itself a qualified timestamp (PAdES, Reg. EU 910/2014) applied by a trust service provider: the date on which that text existed does not depend on what we say, and we cannot move it afterwards.

DOCUMENT	TIMESTAMP	SHA-256 FINGERPRINT OF THE TIMESTAMPED FILE
SempiX Service Continuity Plan `sempix.it/documenti/PIANO_CONTINUITA_SEMPIX.pdf`	21/09/2026 16:28:17 UTC	`97b9c6a83232ab42b1953b05fa079a627c4054b537fad9147443b54e4cbcba6e`
Declaration of authorship of the works `sempix.it/documenti/DICHIARAZIONE_PATERNITA.pdf`	21/09/2026 16:40:17 UTC	`0b36f9c45c6fd524a843f950869ff240fdf6e2c081740dfcc9d296dfab617ca9`
Source code manifest `sempix.it/documenti/MANIFESTO_CODICE.pdf`	21/09/2026 16:40:17 UTC	`7d3468b576c5ad5f862e86ad1d33330a7db51e53e155c4a8d44beded78f3cf6c`

© 2020–2026 SEMPI S.r.l. — Società Benefit. Tutti i diritti riservati. — Documento pubblico

DOCUMENT	TIMESTAMP	SHA-256 FINGERPRINT OF THE TIMESTAMPED FILE
Incident response plan `sempix.it/documenti/PIANO_RISPOSTA_INCIDENTI.pdf`	21/09/2026 16:40:17 UTC	`abe8eeba49fbf6e13ba2c61a2c1759631fbb78af1a81c74b51b64948ada01598`
Role permission matrix `sempix.it/documenti/MATRICE_PERMESSI.pdf`	21/09/2026 16:40:17 UTC	`c2ad95ffdddbcad71386707782232da65b1a4bf2a6206bb87fef8e8526bc3747`

> The fingerprint serves one purpose, and it matters: if you recompute it on the copy you downloaded and get that number, you hold exactly our document. If you get a different number, someone gave you another one — and we want to know.

Who else touches the data

The full list of sub-processors, with what each one receives and on what legal basis, where outside the European Union.

SUPPLIER	DATA IT RECEIVES	WHERE	BASIS FOR THE TRANSFER
Taz.ro Hosting and infrastructure (data centre, backups)	All platform data, encrypted at rest. This is where your company's database lives.	Romania (European Union)	No transfer outside the European Union
Anthropic, PBC The artificial intelligence models behind ARYA	The text of the question and the data of the document being processed, with tax codes and IBANs masked. Not the whole database, not the accounting history, and with no use for training.	United States	EU Standard Contractual Clauses 2021/914
Stripe Payments Europe, Ltd. Collecting the SempiX subscription by card	Subscription billing details. Card numbers are collected by Stripe on its own pages: they never pass through our servers and we do not store them.	Ireland (EU) / United States	EU Standard Contractual Clauses for any flows to the US
GoCardless Ltd. Reading bank movements (PSD2 Open Banking) and SEPA direct debits towards your customers	IBANs, balances and movements of the accounts you connect, only after your explicit consent and for the duration of that consent, which expires and must be renewed.	United Kingdom / European Union	EU–UK adequacy decision

© 2020–2026 SEMPI S.r.l. — Società Benefit. Tutti i diritti riservati. — Documento pubblico

SUPPLIER	DATA IT RECEIVES	WHERE	BASIS FOR THE TRANSFER
OpenAPI S.p.A. Accredited SDI channel for sending and receiving e-invoices	The XML e-invoices you send and receive, in the format prescribed by the Italian Revenue Agency.	Italy (European Union)	No transfer outside the European Union

Contacts

Who to write to, what for, and how quickly we answer.

Data Protection Officer (DPO)

Alberto Tripoli — E.A. Enterprise S.r.l.
dpo@sempi.it

Our DPO is external, not a Sempi employee. That is a choice, not a fallback: whoever checks how we handle data should not report to whoever builds the product (art. 38.6 GDPR). You can write to them directly, including to challenge us.

WHAT FOR	ADDRESS	RESPONSE TIME
Sales questions and information	info@sempi.it	
Platform support (active customers)	assistenza@sempi.it	Monday–Friday, office hours
GDPR rights: access, rectification, erasure, portability	privacy@sempi.it	Within the terms of art. 12 GDPR: one month, extendable with a reasoned notice
Data Protection Officer (DPO)	dpo@sempi.it	
Report a vulnerability or a security incident	privacy@sempi.it	Acknowledged within 24 working hours

© 2020–2026 SEMPI S.r.l. — Società Benefit. Tutti i diritti riservati. — Documento pubblico