STESEI
Corso Unione Sovietica 612/15B - 10135 Torino - Tel. 011.3473620

# Privacy Policy

## 1. TRATTAMENTO DI DATI PERSONALI

**3.1 Finalità del trattamento:** la finalità del trattamento dei Dati è la fornitura ed il successivo uso della piattaforma INDAGOR.

**3.2** Per l'uso di INDAGOR, il Responsabile del Trattamento tratterà, per conto del Titolare, determinate categorie di Dati personali raccolti dal Titolare e inseriti da quest'ultimo nei server di **STESEI SNC** nella fase di censimento degli utenti. In aggiunta ai dati personali inseriti dal Titolare, il Responsabile potrà trattare categorie di dati generati dagli utenti nelle fasi di utilizzo della piattaforma (a titolo esemplificativo: log di sistema, report generati, etc.).

**3.3** Per "Dati personali" si intende qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato») come definito dall'art. 4 del GDPR. Le categorie di Dati personali trattati dal Responsabile del Trattamento per conto del Titolare sono elencate nel *Sub-Allegato A*. Il Responsabile svolge esclusivamente le attività di trattamento necessarie e rilevanti ad assicurare la regolare erogazione al titolare degli applicativi e dei Servizi connessi.

**3.4** Il Responsabile del Trattamento adotta un registro delle attività di trattamento in conformità con l'art. 30, par. 2 del GDPR.

## 2. ISTRUZIONI

**2.1** Il Titolare del Trattamento garantisce di trattare i Dati personali in conformità alla normativa vigente in materia di privacy e protezione dei dati personali. Le istruzioni fornite dal Titolare devono essere conformi alla Legge Applicabile. Il Titolare sarà l'unico responsabile dell'esattezza, la qualità e la limitazione della conservazione dei Dati Personali raccolti e trattati. Il Titolare dovrà inoltre garantire che i Dati siano raccolti e trattati in maniera lecita, corretta e trasparente.

**4.3** Il Responsabile del Trattamento informa il Titolare nel caso in cui ritenga che le Istruzioni violino la Legge Applicabile e non eseguirà tali Istruzioni finché non saranno riconosciute come legittime.

## 5. OBBLIGHI DEL RESPONSABILE DEL TRATTAMENTO

### 5.1 Riservatezza

**5.1.1** Il Responsabile del Trattamento tratta tutti i Dati personali come informazioni strettamente riservate. I Dati Personali non possono essere copiati, trasferiti o trattati in conflitto con le Istruzioni, a meno che non venga autorizzato a seguito di ulteriori accordi con il Titolare del Trattamento.

**5.1.2** I dipendenti del Responsabile sono soggetti a un obbligo di riservatezza e hanno firmato un'apposita nomina che li autorizza a trattare i Dati in maniera conforme alla Legge Applicabile e alle disposizioni contenute nel presente DPA.

**5.1.3** I Dati personali sono trattati solamente dal personale necessario ai fini dell'erogazione dei Servizi.

**5.1.4**. Il Responsabile del Trattamento assicura, inoltre, che i dipendenti che svolgono operazioni di trattamento sui Dati personali possano trattare solo le categorie di Dati personali in conformità alle Istruzioni.

**5.2 Sicurezza**

**5.2.1** Il Responsabile del Trattamento deve attuare le misure tecniche e organizzative appropriate ai sensi dell'articolo 32 del GDPR. Il Responsabile del Trattamento può aggiornare o modificare le misure di sicurezza di volta in volta a condizione che tali aggiornamenti e modifiche non comportino il peggioramento dei livelli di sicurezza complessiva. Le misure di sicurezza sono elencate nel Sub-Allegato B.

**5.3 Valutazioni d'impatto sulla protezione dei dati e consultazione preventiva**

**5.3.1** Se l'assistenza del Responsabile del Trattamento è necessaria e pertinente, il Responsabile assisterà il Titolare nel predisporre le valutazioni d'impatto sulla protezione dei dati in conformità all'art. 35 del GDPR, insieme a qualsiasi consultazione preventiva ai sensi dell'art. 36 del GDPR.

**5.4 Diritti degli interessati**

**5.4.1** Se il Titolare riceve una richiesta da un interessato per l'esercizio dei propri diritti ai sensi della Legge Applicabile e la risposta corretta e legittima a tale richiesta richiede l'assistenza del Responsabile del Trattamento, il Responsabile assisterà il Titolare fornendo, entro un tempo ragionevole, le informazioni necessarie e la documentazione richiesta dal Titolare. Il Responsabile dovrà assistere il Titolare nel gestire tali richieste in conformità con la Legge Applicabile.

**5.4.2** Se il Responsabile del Trattamento riceve una richiesta da un interessato per l'esercizio dei propri diritti ai sensi della Legge Applicabile e tale richiesta è connessa ai Dati Personali raccolti dal Titolare, il Responsabile dei dati deve immediatamente inoltrare la richiesta al Titolare e deve astenersi dal rispondere direttamente all'interessato.

**5.5 Violazione di Dati personali**

**5.5.1** In caso di violazione di Dati personali ("Data Breach") che possa comportare la distruzione, la perdita, l'alterazione, la divulgazione o l'accesso non autorizzato o accidentale ai Dati personali trattati per conto del Titolare del Trattamento, il Responsabile dovrà dare comunicazione al Titolare entro quarantotto (48) ore dal momento in cui il Data Breach viene rilevato dal Responsabile.

**5.5.2** Il Responsabile del Trattamento dovrà compiere ogni ragionevole sforzo per identificare la causa di tale violazione e adottare le misure che riterrà necessarie per determinarne la causa e per impedire che tale violazione si ripresenti.

**5.6 Documentazione di conformità e diritti di audit**

**5.6.1** Su richiesta del Titolare, il Responsabile del Trattamento dovrà mettere a disposizione del Titolare tutte le informazioni rilevanti necessarie a dimostrare la conformità dei trattamenti svolti secondo i termini del presente DPA.

**5.6.2** Il Responsabile riconosce il diritto del Titolare, con le modalità e nei limiti di seguito indicati, a effettuare audit per verificare la conformità del Responsabile agli obblighi previsti dal presente DPA e dalla normativa. Il Titolare potrà avvalersi, per tali attività, di proprio personale specializzato o di revisori esterni, purché tali soggetti siano previamente vincolati da idonei impegni alla riservatezza.

**5.6.3** Il Responsabile può opporsi per iscritto alla nomina da parte del Titolare di eventuali revisori esterni che siano, ad insindacabile giudizio del Responsabile, non adeguatamente qualificati o indipendenti, siano concorrenti del Responsabile o che siano evidentemente inadeguati. In tali circostanze, il Titolare sarà tenuto a nominare altri revisori o a condurre le verifiche in proprio.

**5.6.4** Il Responsabile risponderà alle richieste di documentazione aggiuntiva o di programmazione di audit inoltrate dal Titolare entro trenta (30) giorni dalla data di ricezione della richiesta.

**5.7 Trasferimento dei Dati**

**5.7.1** In via ordinaria, il Responsabile del Trattamento non trasferirà i Dati in Paesi non appartenenti allo Spazio Economico Europeo (SEE).

**5.7.2.** A fini dell'erogazione dei Servizi, il Responsabile tratterà i dati nei seguenti luoghi:

- **C.so Unione Sovietica 612/15 B - 10135 Torino (TO) – Italia** [Sede del Responsabile del Trattamento]
- **Torino – Vercelli** [Sede dei datacenter del Sub-Responsabile del Trattamento]

**5.7.3.** Qualora si rendesse necessario, per svolgere alcune tipologie di trattamenti (a titolo esemplificativo: backup, hosting, ecc.), il trasferimento dei Dati al di fuori dello Spazio economico europeo (SEE), i Dati saranno trasferiti solamente a Sub-Responsabili che abbiano adottato le adeguate garanzie previste dagli artt. 44-50 del GDPR (a titolo esemplificativo: Privacy Shield Framework, Decisioni di adeguatezza della Commissione Europea, Clausole Contrattuali Standard). L'elenco aggiornato dei Sub-Responsabili è disponibile nel Sub-Allegato C del presente DPA.

**6. AUTORIZZAZIONE GENERALE ALLA NOMINA DI SUB-RESPONSABILI**

**6.1** Al Responsabile del Trattamento viene conferita l'autorizzazione generale a nominare terze parti ("Sub-responsabili") per il trattamento dei Dati personali senza che siano necessarie ulteriori autorizzazioni scritte e specifiche dal Titolare del Trattamento.

**6.2** Il Responsabile avvisa il Titolare prima che vengano stipulati accordi con un nuovo potenziale Sub-responsabile e prima che il Sub-responsabile tratti i Dati personali raccolti dal Titolare. Se il Titolare del Trattamento desidera opporsi alla nomina di un nuovo Sub-responsabile, il Titolare deve notificare tale opposizione al Responsabile per iscritto entro dieci (10) giorni lavorativi dal ricevimento della notifica da parte del Responsabile del Trattamento. L'assenza di eventuali obiezioni da parte del Titolare del Trattamento è da intendersi come consenso per la nomina di un nuovo Sub-responsabile.

**6.3** Nel caso in cui il Titolare del Trattamento si opponga a un nuovo Sub-responsabile e il Responsabile non possa accogliere l'obiezione del Titolare, il Titolare del Trattamento può richiedere l'interruzione dei Servizi fornendo comunicazione scritta al Responsabile.

**6.4** Il Responsabile del Trattamento deve firmare un apposito DPA con ogni nuovo Sub-responsabile. Tale accordo deve prevedere come minimo gli stessi obblighi di protezione dei dati applicabili al Responsabile del Trattamento, compresi gli obblighi previsti dal presente DPA.

Il Responsabile del Trattamento monitorerà e verificherà periodicamente la conformità dei suoi Sub-responsabili alla Legge Applicabile. La documentazione di tale monitoraggio deve essere fornita al Titolare del Trattamento se richiesto per iscritto.

**6.5** Il Responsabile del Trattamento, al momento dell'introduzione del presente DPA, impiega i Sub-responsabili elencati nel Sub-Allegato C. Se il Responsabile sigla un contratto con un nuovo Sub-responsabile, tale nuovo Sub-responsabile deve essere aggiunto alla lista dei Sub-Responsabili del Sub-Allegato C.

## 7. CANCELLAZIONE DEI DATI

**7.1** Dopo la scadenza o la risoluzione della fornitura del servizio, il Responsabile del Trattamento cancellerà o restituirà al Titolare tutti i Dati Personali in suo possesso, eccetto nel caso in cui sia richiesto dalla Legge Applicabile al Responsabile del Trattamento di conservare alcuni o tutti i Dati personali (in quel caso il Responsabile archivierà i dati e attuerà misure ragionevoli per impedire che i Dati personali vengano ulteriormente trattati). I termini di questo DPA continueranno ad applicarsi a tali Dati personali.

## 8. DATI DI CONTATTO

**8.1** I dati di contatto del Responsabile del Trattamento sono i seguenti:

**STESEI SNC**
Indirizzo: C.so Unione Sovietica 612/15 B - 10135 Torino
Mail: stesei@stesei.it - Tel: +39 011 347 36 20

# Sub-Allegato A - Dati personali

## 1. Dati personali

**1.1** Il Responsabile del Trattamento tratta i seguenti tipi di Dati personali necessari all'erogazione dei Servizi:

***a. Nome, Cognome, Codice Fiscale;***
***b. Telefono***
***c. Indirizzo e-mail***
***d. Ufficio di appartenenza***
***c. Log con dati relativi all'accesso dell'utente alla piattaforma e alle azioni compiute all'interno della stessa;***

## 2. Categorie di Soggetti Interessati

**2.1** Il Responsabile del Trattamento tratta per conto del Titolare i Dati personali relativi alle seguenti categorie di soggetti interessati:

***a. Dipendenti del Titolare del Trattamento***
***b. Operatori autorizzati dal Titolare del Trattamento***

## 3. Finalità del Trattamento

**3.1** Il Responsabile del Trattamento tratterà i Dati Personali dei Soggetti interessati per le seguenti finalità:

***a. Erogazione dei servizi digitali della piattaforma Indagor***

# Sub-Allegato B
# Misure tecnico-organizzative e di sicurezza

**1. Nomina dei soggetti autorizzati**
Il Responsabile del Trattamento ha nominato con apposito atto tutti i soggetti autorizzati all'accesso ai dati personali, vincolandoli a un obbligo di riservatezza.

**2. Sub-Responsabili e Accordi per la protezione dei dati personali**
Il Responsabile del Trattamento impiega esclusivamente Sub-Responsabili del Trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che i trattamenti soddisfino i requisiti del GDPR e garantiscano la tutela dei diritti dell'interessato.
Al momento l'unico sub-responsabile utilizzato da Stesei è CSI PIEMONTE (Sub-Responsabile del trattamento presso il quale vengono conservati i Dati).
CSI PIEMONTE dispone delle certificazioni elencate in https://www.csipiemonte.it/web/it/certificazioni.
L'infrastruttura cloud è inoltre Qualifica AGID.

**3. Misure di sicurezza per i database**
L'accesso ai database di servizio è consentito esclusivamente all'amministratore di sistema che ha adottato tutte le contromisure per limitare le possibilità di accesso fraudolento.
Il Sub-Responsabile del Trattamento (CSI PIEMONTE) presso il quale saranno conservati i Dati ha altresì adottato le misure di sicurezza tecniche e organizzative elencate nel dettaglio al seguente link: https://nivola-userguide.readthedocs.io/it/latest/index.html.

**4. Cifratura dei dati**
Ai sensi dell'art.32, paragrafo 1, comma (a) del GDPR, STESEI ha proceduto a cifrare i dati personali contenuti nei database utilizzando l'algoritmo AES (Advanced Encryption Standard).

La cifratura è stata predisposta per i dati identificativi dell'utente (Nome e Cognome, Codice Fiscale, Indirizzo mail, Telefono) e per i dati identificativi del soggetto per il quale è stata emessa un'interrogazione (Generalità, Codice Fiscale).

Inoltre, la società ha predisposto la cifratura di tutti gli strumenti necessari alla connessione con gli Enti Erogatori attestati sulla piattaforma PDND.

Infine, sono state cifrate le credenziali di accesso (Username e Password) alla piattaforma degli utenti.

**5. Misure di sicurezza ambientali**
I locali operativi di STESEI SNC sono protetti da impianto antiincendio e segnali di evacuazione.
L'accesso all'edificio principale è sorvegliato da un impianto di videosorveglianza e gli spazi sono protetti da allarme.
L'accesso al comprensorio dove ha sede Stesei è sorvegliato da un servizio di vigilanza.
Ordinariamente, i Dati Personali degli Interessati non verranno stampati su supporti cartacei.
Qualora fosse necessario trattare i dati su documenti cartacei, questi verranno riposti in appositi archivi chiusi a chiave alla fine della sessione di lavoro.

**6. Capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento**

L'azienda ha predisposto il backup dei dati con frequenza giornaliera.
Il trattamento dei dati è consentito solo dopo il superamento di una procedura di autenticazione univocamente associata all'addetto e relativa ad uno specifico trattamento o ad un insieme di trattamenti. Inoltre, il codice di identificazione, quando utilizzato, non viene mai assegnato ad altri addetti, nemmeno in tempi diversi.

**7. Password e procedure di autenticazione**

Le password degli utenti devono avere obbligatoriamente un minimo 10 caratteri, dei quali una lettera maiuscola, un numero e un carattere speciale.

**8. Capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico**

Sono state adottate idonee misure per garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati e non superiori alle 48 ore.
L'azienda ha inoltre introdotto una policy per la rapida individuazione e segnalazione dei Data Breach al Titolare del trattamento e al Garante per la Protezione dei Dati Personali, ove applicabile.

**9. Procedure per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento**

Periodicamente, con cadenza almeno annuale, sono aggiornati gli ambiti del trattamento consentito agli addetti ed ai responsabili della gestione o manutenzione dei sistemi elettronici e aggiornate le misure di sicurezza allo stato dell'arte a seguito di periodiche analisi dei rischi.

# Sub-Allegato C
# Sub-responsabili approvati

| Nome | Indirizzo | Riferimenti |
|---|---|---|
| CSI PIEMONTE (società in-house della regione Piemonte) | C.so Unione Sovietica 216 - Torino | Fornitore dei servizi di cloud |