

### **ALLEGATO 3 - PRIVACY**

Il presente Allegato è redatto in conformità a quanto previsto all'art. 28 del Regolamento (UE) 2016/679 e forma parte integrante e sostanziale del Contratto stipulato tra le Parti.

Il Fornitore, come sotto definito, dichiara, nell'ambito della procedura ad evidenza pubblica, di essere in grado di assicurare idonee ed adeguate garanzie in termini di conoscenza specialistica, affidabilità, risorse, nonché in ordine all'adozione di misure tecniche, logiche ed organizzative per assicurare che i trattamenti dei dati personali siano conformi alle esigenze del Regolamento Europeo. Con la sottoscrizione del Contratto e del presente Allegato, che ne costituisce parte integrante, il Fornitore dichiara altresì di essere consapevole di essere nominato, con la sottoscrizione del presente Allegato, Responsabile del trattamento in funzione della designazione fatta da Inail in qualità di Titolare, nel presente Allegato e nei documenti tecnico – funzionali che verranno eventualmente scambiati tra le Parti e sottoscritti ai fini della rilevanza contrattuale.

Il Titolare e il Fornitore sono di seguito nominati disgiuntamente la Parte e congiuntamente le "Parti".

Il mancato rispetto delle disposizioni di cui al presente Allegato sarà considerato un grave inadempimento del Contratto ai sensi dell'art. 15 S del medesimo.

Ai fini del presente Allegato con il termine "Fornitore" o "Responsabile del trattamento" si individua l'Impresa appaltatrice designata quale Responsabile del trattamento ai sensi del Regolamento (UE) 2016/679 o GDPR in ragione delle prestazioni oggetto del Contratto.

Pertanto, ai fini del presente Allegato e delle sue successive modifiche/integrazioni concordate in forma scritta tra le Parti, le Parti espressamente convengono che il fornitore è di seguito definito come Fornitore o Responsabile del trattamento dei dati, Inail definito come Titolare del trattamento dei Dati Personali.

#### **PREMESSA:**

#### **OGGETTO e DURATA DEL PRESENTE ALLEGATO**

1. Il presente Allegato disciplina le istruzioni che il Fornitore si impegna ad osservare nell'ambito dei trattamenti dei Dati Personali che realizzerà per conto del Titolare nello svolgimento delle attività e dei servizi oggetto del Contratto garantendo il rispetto della normativa vigente in materia di tutela e sicurezza dei Dati Personali.
2. La durata di efficacia del presente Allegato, che è parte integrante del Contratto a cui si riferisce, decorre dalla data della sua sottoscrizione - ovvero *<inserire data>* - e termina alla data di cessazione del Contratto (ossia: *<inserire data>*).
3. Le Parti espressamente convengono che in caso di contrasto tra le disposizioni contenute nel presente Allegato e le Norme in materia di Trattamento dei Dati Personali come sotto definite e le loro successive modifiche/integrazioni, queste ultime si riterranno prevalenti.
4. In caso di contrasto tra le disposizioni contenute nel presente Allegato e qualsiasi disposizione contenuta nel Contratto con riferimento alla Privacy, le norme contenute nel presente Allegato si riterranno prevalenti.

#### **DEFINIZIONI**

- "Dati Personali": i Dati Personali di cui all'art. 4 del Regolamento UE 2016/279 (nonché i dati appartenenti alle categorie particolari di dati personali di cui all'art. 9 e 10 del Regolamento UE 2016/679).
- "Tipo di Dati Personali trattati": Dati comuni (dati anagrafici, dati di contatto, ecc.).
- "Categorie di soggetti interessati": Dipendenti e Collaboratori.

- “Norme in materia di Trattamento dei Dati Personali”: tutte le leggi, disposizioni e direttive normative applicabili in relazione al trattamento e/o alla protezione dei Dati Personali, così come modificate di volta in volta, ivi incluso, ma non limitatamente, il Regolamento UE 2016/679 (GDPR), la normativa di adeguamento italiana, circolari, pareri e direttive dell’Autorità di Controllo nazionale, le decisioni interpretative adottate dallo European Data Protection Board.
- “Contratto”: si intende il contratto stipulato tra il Titolare e il Fornitore avente ad oggetto l’acquisizione di servizi certificati di firma digitale in modalità SaaS e servizi connessi, con relativi dispositivi, manutenzione e assistenza specialistica
- “Misure di Sicurezza”: le misure di sicurezza di natura fisica, logica, tecnica e organizzativa adeguate a garantire un livello di sicurezza adeguato al rischio, ivi comprese quelle specificate nel Contratto, unitamente ai suoi Allegati.
- “Sub-Responsabile del trattamento”: la persona fisica o giuridica, l’Autorità pubblica, il servizio o altro organismo che svolge l’attività di responsabile del trattamento in forza di contratto scritto con il Responsabile del trattamento. Le Parti convengono che il Responsabile del trattamento non ricorrerà a un altro Responsabile, che opererà in qualità di Sub-responsabile senza previa autorizzazione scritta, specifica o generale, da parte del Titolare del trattamento.
- “Persone autorizzate al trattamento dei dati”: persone che in qualità di dipendenti, collaboratori, amministratori o consulenti del responsabile e/o del sub-responsabile siano state autorizzate al trattamento dei Dati Personali sotto l’autorità diretta del Titolare o del Responsabile.
- “Violazione dei Dati Personali (data breach)”: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l’accesso ai Dati Personali trasmessi, conservati o comunque trattati.
- “Incidente di sicurezza”: la violazione di sicurezza che comporta la perdita, la modifica, la divulgazione non autorizzata o l’accesso a dati e/o informazioni riservate la violazione e/o il malfunzionamento di misure di sicurezza, di strumenti elettronici, hardware o software a protezione dei dati e delle informazioni.
- Per quanto non espressamente ivi richiamato nelle Definizioni di cui al presente Allegato, Le Parti rinviando alle definizioni di cui all’art. 4 del Regolamento (UE) 2016/679.

## **SICUREZZA DEI DATI PERSONALI**

Il Fornitore ottempererà a tutte le norme in materia di Trattamento dei Dati Personali in relazione al Trattamento dei Dati Personali ivi comprese quelle che saranno emanate nel corso della durata del Contratto al fine di assicurare, ciascuno nell’ambito delle proprie attività e competenze specifiche, un adeguato livello di sicurezza dei trattamenti, inclusa la riservatezza e in modo tale da ridurre al minimo i rischi di distruzione o perdita, anche accidentale, modifica, divulgazione non autorizzata, nonché di accesso non autorizzato, anche accidentale o illegale, o di trattamento non consentito o non conforme alle finalità della raccolta.

## **OBBLIGHI E ISTRUZIONI PER IL FORNITORE**

### **I. OBBLIGHI GENERALI DEL FORNITORE**

1. Ai sensi del presente Allegato, il Fornitore è autorizzato a trattare per conto del Titolare i Dati Personali necessari per l’esecuzione delle attività di cui all’oggetto del Contratto.
2. A tal fine il Fornitore si impegna a:
  - non determinare o favorire mediante azioni e/o omissioni, direttamente o indirettamente, la violazione da parte del Titolare del trattamento delle Norme in materia di Trattamento dei Dati Personali;
  - trattare i Dati Personali esclusivamente in conformità al presente Allegato, e pertanto nella misura ragionevolmente necessaria all’esecuzione del Contratto, e in conformità alle Norme in materia di Trattamento dei Dati Personali;
  - adottare, Misure di sicurezza come di seguito previste e in ogni caso adeguate a garantire la protezione e la sicurezza dei Dati Personali al fine di prevenire a titolo indicativo e non esaustivo:
    - incidenti di sicurezza; violazioni dei Dati Personali (Data Breach);

- ogni violazione delle misure di sicurezza;
  - tutte le altre forme di Trattamento dei dati non autorizzate o illecite.
3. Il Fornitore si impegna a designare il Responsabile della protezione dei dati di cui all'art. 37 GDPR e a comunicarne i dati e i contatti di riferimento tempestivamente al Titolare in ragione dell'attività svolta.
4. Ai sensi dell'articolo 28 del GDPR, comma 2 e 4, il Responsabile del trattamento può ricorrere ad altri Responsabili del trattamento, al fine di svolgere specifiche attività di trattamento. Le Parti espressamente convengono che, su tali altri Responsabili del trattamento, secondo quanto disposto dal GDPR, sono imposti mediante contratto o altro atto giuridico, i medesimi obblighi contrattuali in vigore tra il Titolare e il Responsabile iniziale, prevedendo in particolare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del regolamento (UE) 2016/679. In ogni caso il Responsabile iniziale conserva nei confronti del Titolare l'intera responsabilità dell'adempimento degli obblighi dell'altro Responsabile.

[CASO AUTORIZZAZIONE GENERALE: il Responsabile del trattamento comunica in forma scritta al Titolare del trattamento *entro X mesi* precedenti alla relativa modifica - eventuali modifiche previste riguardanti l'aggiunta o la sostituzione di altri responsabili del trattamento, dando così al Titolare del trattamento l'opportunità di opporsi a tali modifiche].

## **II. ISTRUZIONI PER IL FORNITORE**

### **II.A) Elementi essenziali delle istruzioni**

Gli elementi essenziali del trattamento sono contenuti nel presente Allegato, nel Contratto e nei suoi allegati che ne costituiscono parte integrante, nonché nei documenti tecnico – funzionali che saranno eventualmente scambiati tra le Parti e che il Responsabile del trattamento sottoscrivere ai fini di efficacia contrattuale.

### **II.B) Obblighi del Fornitore nei confronti del Titolare**

Il Fornitore si impegna a:

1. Trattare i dati solo per l'esecuzione delle attività di cui all'oggetto del Contratto.
2. Trattare i dati conformemente alle istruzioni documentate impartite dal Titolare del trattamento (con il presente Allegato e con eventuali ulteriori integrazioni al presente Allegato, in ogni caso sottoscritte dalle Parti).
3. Qualora il Fornitore reputi che un'istruzione sia, o possa essere, contraria alla Normativa in materia di protezione dei dati, ivi incluso il GDPR, deve informarne immediatamente il Titolare del Trattamento.
4. Trattare i dati conformemente al presente Allegato anche nei casi di trasferimento dei dati verso un paese terzo o un'organizzazione internazionale, e in ogni caso come previsto dall'art. 28 paragrafo 3 del GDPR.
5. Garantire che il trattamento dei Dati Personali sia effettuato in modo lecito, corretto, adeguato, pertinente e avvenga nel rispetto dei principi di cui all'artt. 5 e ss. del GDPR.
6. Garantire la riservatezza dei Dati Personali trattati per l'esecuzione delle attività del Contratto.
7. Garantire che le Persone autorizzate a trattare i Dati Personali in virtù del presente Contratto: *i)* si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza; *ii)* abbiano ricevuto, e ricevano, da parte del Fornitore la formazione necessaria in materia di protezione dei Dati Personali; *iii)* accedano e trattino i Dati Personali osservando le istruzioni impartite dal Titolare del trattamento, in ogni caso conformemente alle disposizioni di cui al presente Allegato.
8. Tenere conto nell'esecuzione delle attività contrattuali dei principi della protezione dei dati fin dalla progettazione e protezione per impostazione predefinita (privacy by design e by default) anche mediante l'ausilio delle istruzioni documentate impartite dal Titolare del trattamento.

9. Concordare con il Titolare i contenuti delle informative e le modalità per fornire le informazioni agli interessati, per i trattamenti basati sul consenso, le modalità di acquisizione e revoca del consenso.
10. Qualora richiesto dalle Norme in materia di Trattamento dei Dati Personali, il Titolare e il Fornitore convengono di sottoscrivere un accordo aggiuntivo, di modifica o di aggiornamento che potrà essere necessario in ogni caso conformemente alle Norme sul Trattamento dei Dati Personali.
11. In conformità a quanto disposto dall'art. 28 comma 3 lettera d) del GDPR, rispettare le condizioni di cui ai paragrafi 2 e 4 per ricorrere ad un altro responsabile del trattamento.

#### **II.C) Obblighi del Fornitore nell'ambito dei diritti esercitati dagli Interessati nei confronti del Titolare**

1. Il Fornitore collabora nella misura in cui questo sia possibile e per quanto di sua competenza alle istanze trasmesse dagli Interessati nell'esercizio dei diritti previsti dagli artt. 15-22 del GDPR;
2. Il Fornitore, tenuto conto della natura del trattamento, assiste il Titolare del trattamento con misure tecniche e organizzative adeguate, nella misura in cui questo sia possibile, al fine di soddisfare l'obbligo del Titolare del trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato;
3. il Fornitore adotta e aggiorna un registro di tutte le attività di trattamento eseguite per conto del Titolare e completo di tutte le informazioni previste all'art. 30 del GDPR;
4. Qualora il Fornitore riceva una comunicazione inerente l'esercizio dei diritti dell'interessato, che dovrebbe essere in ogni caso rivolta al Titolare, il Fornitore, si impegna ad inoltrarla tempestivamente, e comunque *entro e non oltre X* giorni dalla ricezione, per posta elettronica al Titolare del trattamento.

#### **II.D) Obblighi del Responsabile che ricorre a Persone Autorizzate al trattamento dei Dati Personali**

Ai sensi dell'art. 28 GDPR, paragrafo 3, b) il Fornitore si obbliga ai sensi del presente Allegato a garantire che le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del Fornitore ovvero Responsabile del trattamento si siano impeginate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza.

### **III. IL REGISTRO DEI TRATTAMENTI DEL RESPONSABILE**

1. Il Fornitore predispone, un registro, in formato elettronico di tutte le categorie di attività relative ai trattamenti svolti per conto del Titolare del Trattamento, come prevede l'art. 30, comma 2, del GDPR.
2. In particolare, il Registro dei trattamenti del Fornitore relativo ai trattamenti eseguiti per conto del Titolare deve contenere:
  - i) il nome e i dati di contatto del Fornitore in qualità di Responsabile del trattamento, di ogni Titolare del trattamento per conto del quale il Responsabile agisce, del rappresentante (eventuale) del Fornitore o del Titolare del trattamento nonché del Responsabile della protezione dei dati (DPO);
  - ii) le categorie dei trattamenti effettuati per conto di ogni Titolare del trattamento;
  - iii) ove applicabile, i trasferimenti di Dati Personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49 del GDPR, la documentazione delle garanzie adeguate;
  - iv) una descrizione generale delle misure di sicurezza tecniche e organizzative messe in atto per un trattamento corretto e sicuro ai sensi dell'articolo 32 del GDPR.

### **IV. COLLABORAZIONE DEL FORNITORE NELL'ADEMPIMENTO DEGLI OBBLIGHI DEL TITOLARE**

Il Fornitore assiste il Titolare nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36 del GDPR tenendo conto della natura del trattamento e delle informazioni a disposizione del Responsabile del trattamento.

#### **IV.A) Misure di sicurezza.**

1. Il Titolare e il Fornitore mettono in atto misure tecniche ed organizzative adeguate per garantire un livello di sicurezza adeguato al rischio e garantire il rispetto degli obblighi di cui all'art. 32 del GDPR. Tali misure comprendono tra le altre:
  - a) la pseudonimizzazione e la cifratura dei Dati Personali;
  - b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
  - c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei Dati Personali in caso di incidente fisico o tecnico;
  - d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento;
  - e) la redazione del Piano di Sicurezza e l'implementazione delle relative contromisure, conformemente al principio di privacy by design ex art. 25 GDPR;
  - f) i controlli previsti dal Sistema di Gestione della Sicurezza delle Informazioni (SGSI) del Titolare del trattamento, certificato secondo lo Standard ISO 27001, nel rispetto delle policy definite nel SGSI;
  - g) nel caso di utilizzo di sistemi cloud per la fornitura oggetto del Contratto stipulato tra le parti, tali sistemi devono garantire un livello di sicurezza analogo a quello che verrebbe implementato all'interno dell'Istituto. A titolo esemplificativo tali sistemi dovranno essere protetti da Antivirus, Autenticazione, IPS, Network Firewall, WAF, ecc.

*[Le misure di sicurezza sopra elencate, in considerazione della rapidità con cui si evolvono le minacce nel settore della sicurezza informatica, sono considerate adeguate al momento, tuttavia le stesse potranno essere oggetto di futuro accordo tra le Parti per integrazioni che si dovessero rendere necessarie sulla base di valutazioni di adeguatezza da parte del Titolare e/o del Responsabile]*
2. Nel valutare l'adeguatezza del livello di sicurezza si tiene conto in special modo dei rischi presentati dal trattamento (o dai trattamenti), che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, ai Dati Personali trasmessi, conservati o comunque trattati.
3. All'esito dell'analisi dei rischi, le misure di sicurezza adeguate ai sensi dell'art. 32 del GDPR devono essere condivise ed approvate dal Titolare
4. L'attività di identificazione dei Dati Personali oggetto del trattamento dovrà seguire i criteri di privacy by default di cui all'art. 25 del GDPR.
5. Ai sensi dell'art. 32, comma 4, GDPR il Fornitore, in qualità di Responsabile del trattamento e il Titolare del trattamento garantiscono che chiunque agisca sotto la loro autorità e abbia accesso ai Dati Personali non tratti tali dati se non debitamente istruito dal Titolare, salvo che lo richieda il diritto dell'Unione o degli Stati membri.

#### **IV.B) Data breach**

1. Il Fornitore collabora con il Titolare del trattamento, nelle attività di adempimento di cui agli articoli 33 e 34 del GDPR in materia di violazioni di Dati Personali, ovvero di data breach.
2. In particolare, il Fornitore, in qualità di Responsabile del trattamento deve:
  - informare il Titolare del trattamento tempestivamente e in ogni caso senza giustificato ritardo, dopo essere venuto a conoscenza della violazione.
  - nel caso in cui il Titolare sia tenuto a fornire informazioni il Fornitore supporterà il Titolare fornendo le informazioni di cui ha disponibilità.

#### **V. ULTERIORI OBBLIGHI DI GARANZIA DEL FORNITORE**

Il Fornitore si impegna a:

1. mettere a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al presente articolo e consenta e contribuisca alle attività di revisione, comprese le ispezioni, realizzati dal titolare del trattamento o da un altro soggetto da questi incaricato.  
Inoltre il Responsabile del trattamento informa immediatamente il titolare del trattamento qualora, a suo parere, un'istruzione violi il presente regolamento o altre disposizioni, nazionali o dell'Unione, relative alla protezione dei dati.
2. Trattare i Dati Personali soltanto su istruzione documentata del Titolare del trattamento, anche in caso di trasferimento dei Dati Personali verso un paese terzo o un'organizzazione internazionale, salvo che lo richieda il diritto dell'Unione o Nazionale cui è soggetto il Responsabile del trattamento. In Tale caso il Responsabile del trattamento informa il Titolare di tale obbligo giuridico prima del trattamento, a meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico.
3. Il Fornitore si impegna a notificare tempestivamente al Titolare ogni provvedimento di un'Autorità di controllo, o dell'Autorità giudiziaria relativo ai *Dati Personali del Titolare* salvo il caso in cui tale comunicazione non sia vietata dal provvedimento o dalla legge. 4) In simili circostanze, e in ogni caso conformemente a quanto previsto dal GDPR e dalla normativa applicabile, il Fornitore deve: *i)* informare il Titolare tempestivamente; *ii)* collaborare con il Titolare, *iii)* garantire il trattamento riservato di tali informazioni.
4. Il Fornitore prende atto e riconosce che, nell'eventualità di una violazione delle norme in materia di Trattamento dei Dati Personali nonché delle disposizioni di cui al presente Allegato, oltre all'applicazione delle clausole di risoluzione del contratto e delle penali oltre all'eventuale risarcimento del maggior danno, il Titolare avrà la facoltà di ricorrere a provvedimenti cautelari, ingiuntivi e sommari o ad altro rimedio equitativo, allo scopo di interrompere immediatamente, impedire o limitare il trattamento, l'utilizzo o la divulgazione dei Dati Personali.
5. Il Fornitore si impegna a tenere indenne il Titolare per qualsiasi responsabilità connessa ad eventuali inadempimenti della normativa GDPR e relativa alla sicurezza informatica da parte del Fornitore.
6. Il Titolare si impegna a tenere indenne il Fornitore per qualsiasi responsabilità connessa ad eventuali inadempimenti della normativa GDPR e relativa alla sicurezza informatica da parte del Titolare del trattamento.

#### **VI. OBBLIGHI DEL FORNITORE AL TERMINE DEL CONTRATTO.**

1. Il Responsabile si impegna a non conservare - nonché a garantire che le Persone Autorizzate al trattamento non conservino - i Dati Personali per un periodo di tempo ulteriore al limite di durata strettamente necessario per l'esecuzione dei servizi e/o l'adempimento degli obblighi di cui al Contratto, in ogni caso per un periodo non maggiore di <X> anni, e in ogni caso come disciplinato dalla legge applicabile in materia.
2. Al termine del Contratto il Fornitore si impegna a cancellare o restituire al Titolare tutti i Dati Personali e tutte le relative copie esistenti, fatto salvo quanto diversamente disposto dalle Norme in materia di Trattamento dei Dati Personali.
3. Il Fornitore deve documentare per iscritto al Titolare tale cancellazione.

#### **VII. MODIFICHE DELLE LEGGI IN MATERIA DI TRATTAMENTO DEI DATI PERSONALI**

In caso di modifica delle Norme in materia di Trattamento dei Dati Personali applicabili al trattamento dei Dati Personali, il Fornitore e il Titolare collaboreranno, per quanto di propria competenza, affinché siano sviluppate, adottate e implementate misure di adeguamento al GDPR e alle sue successive modifiche e integrazioni durante il periodo di efficacia del Contratto.

#### **VIII. DISPOSIZIONI FINALI**

1. Le Parti convengono che le disposizioni di cui al presente Allegato costituiscono l'intera contrattazione tra le Parti in relazione al suo oggetto.
2. Le Parti convengono che qualsiasi modifica al presente Allegato sarà efficace e vincolante tra le Parti solo se definita di comune accordo tra le Parti e in forma scritta.
3. Nessuna delle Parti assumerà obbligazioni per conto dell'altra. Le Parti convengono di essere soggetti giuridici indipendenti.
4. La nullità di una singola clausola non comporta la nullità dell'intero Allegato.
5. Le Parti si danno reciprocamente atto che le disposizioni di cui al presente Allegato, costituiscono la sostanziale volontà tra le Parti, è stato in ogni caso oggetto di trattative tra le Parti.

Luogo, Data

Il Fornitore

Inail, in qualità di Titolare del trattamento

Firma del legale rappresentante

Firma del legale rappresentante