Allegato B

Data Protection Agreement (tra Titolare-Responsabile)

Clausole Contrattuali Titolare – Responsabile

1. Scopo del Documento

Il presente documento, costituisce parte integrante dell'accordo stipulato ai sensi del DD n.8263/2019, aggiornato ai sensi del Regolamento UE 2016/679, per regolamentare i rapporti tra Titolare e Responsabile nell'ambito dei trattamenti dei dati personali connessi allo sviluppo dei servizi in materia Sistema Toscano dei Servizi alle Imprese , in particolare inerenti i seguenti applicativi:

- STAR – Accettatore istanze telematiche SUAP per l'acquisizione e la gestione delle istanze da parte di cittadini ed imprese;
- BDM – Banca dati management: gestione dei procedimenti locali, della relativa modulistica e configurazione oneri da pagare
- Desktop SUAP: sistema per i referenti dei SUAP che consente loro di monitorare le interazioni sulle singole pratiche, effettuare report per l'individuazione di interazioni non correttamente gestite, effettuare report quantitativi sul numero delle pratiche, gestire i responsabili e gli operatori SUAP
- WFA: sistema di orchestrazione tra gli attori della rete dei SUAP

Definizioni:

Titolare il soggetto titolare delle finalità dei trattamenti e dei dati personali oggetto delle attività disciplinate dal contratto/convenzione

Responsabile il soggetto che effettua trattamenti di dati personali per conto del Titolare

Interessato la persona fisica cui si riferiscono i dati personali trattati

DPO Responsabile trattamento dati personali/Data Protection Officer

GDPR Regolamento Europeo sulla protezione dei dati personali 2016/679 – General Data Protection Regulation

Security IT Manager/CISO la persona o la struttura a cui sono demandate le attività di auditing sulle misure di sicurezza adottate e di incident management

Incident management procedura di gestione degli incidenti IT relativi a dati personali

Responsabile della sicurezza IT la persona o la struttura cui è demandato il compito di definire, impostare e gestire le misure di sicurezza IT

Lock-In con tale termine si intende la diminuzione o perdita da parte del titolare della possibilità di gestire i servizi e relativi dati in autonomia senza dover forzatamente ricorrere al soggetto a cui ne ha ceduto la gestione. La sicurezza dei dati e la continuità del servizio devono sempre essere sotto il controllo del Titolare.

Accordo Data Protection fra Titolare e Responsabile
(Data Protection Agreement)

TRA

Comune di

con sede legale in

in persona del suo legale rappresentante o suo delegato al trattamento dei dati personali

(indicare l'atto di delega)

E

Regione Toscana, con sede legale in Firenze, Piazza del Duomo n. 10, in persona del Direttore Gianluca Vannuccini, responsabile della Direzione Sistemi Informativi, Infrastrutture tecnologiche e Innovazione, in qualità di delegato al trattamento dei dati personali, ex dgr 585/2018

ART. 1 - TRATTAMENTO DEI DATI PERSONALI

Ai sensi e per gli effetti della normativa in materia di protezione dei dati personali (Reg. UE n. 2016/679, di seguito "GDPR"), nonché D. Lgs. 196/2003 da ultimo novellato dal D. Lgs. 101/2018, (di seguito "Codice Privacy") ed in relazione alle operazioni che vengono eseguite per lo svolgimento dei servizi in materia di giustizia civile e penale, in particolare inerenti i seguenti applicativi:

- STAR – Accettatore istanze telematiche SUAP;
- BDM – Banca dati management;
- Desktop SUAP;
- WFA

il Comune di
in qualità di **Titolare**, nomina **Regione Toscana – Giunta Regionale Responsabile** del trattamento, ai sensi dell'articolo 28 GDPR.

Titolare e Responsabile verranno in seguito entrambi indicati congiuntamente "le Parti".

I trattamenti affidati dal **Titolare** al **Responsabile** riguardano:

Per l'applicativo *STAR*

- le operazioni di trattamento affidate al Responsabile sono riconducibili alle funzioni ascrivibili all'amministratore di sistema e sono le seguenti: inserimento, modifica, cancellazione utenti e monitoraggio sistema;
- le categorie di interessati sono: cittadini;
- la tipologia di dati trattati sono: dati comuni (dati anagrafici e di contatto); si segnala che il sistema acquisisce anche documenti non strutturati che potrebbero contenere dati

Per l'applicativo *BDM*

- le operazioni di trattamento affidate al Responsabile sono riconducibili alle funzioni ascrivibili all'amministratore di sistema e sono le seguenti: inserimento, modifica, cancellazione utenti e monitoraggio sistema;
- le categorie di interessati sono: operatori degli enti regionali e locali;
- la tipologia di dati trattati sono: dati comuni (dati anagrafici e di contatto)

Per l'applicativo *Desktop SUAP*

- le operazioni di trattamento affidate al Responsabile sono riconducibili alle funzioni ascrivibili all'amministratore di sistema e sono le seguenti: inserimento, modifica, cancellazione utenti e monitoraggio sistema;
- le categorie di interessati sono: cittadini e operatori degli enti locali;
- la tipologia di dati trattati sono: dati comuni (dati anagrafici e di contatto)

Per l'applicativo *WFA*

- le operazioni di trattamento affidate al Responsabile sono riconducibili alle funzioni ascrivibili all'amministratore di sistema e sono le seguenti: monitoraggio sistema;
- le categorie di interessati sono: cittadini;
- la tipologia di dati trattati sono: dati comuni (dati anagrafici e di contatto)

I trattamenti effettuati per conto del Titolare dal Responsabile cesseranno al completamento del contratto/convenzione ovvero in caso di sua risoluzione, per qualsiasi altro motivo.
Se una disposizione del presente articolo è o diventa invalida o inapplicabile, la validità e l'applicabilità delle altre disposizioni del medesimo rimangono inalterate. In questo caso, Titolare e Responsabile concordano di adottare una disposizione che corrisponda al meglio allo scopo previsto nella disposizione non valida o agli interessi comuni.

Regione Toscana – Giunta Regionale, in quanto **Responsabile**, fornisce garanzie sufficienti, in particolare in termini di conoscenze specialistiche, affidabilità e risorse, per attuare misure tecniche e organizzative che soddisfino i requisiti normativi sanciti dal GDPR, dal Codice Privacy e da qualsiasi altra norma connessa inerente al trattamento dei dati personali, comprese le misure di sicurezza del trattamento, per garantire la riservatezza e la protezione dei diritti degli interessati.

Regione Toscana – Giunta Regionale, in quanto **Responsabile**, è tenuto ad assicurare e far assicurare ai propri dipendenti, collaboratori e responsabili ulteriori, la riservatezza ed il corretto trattamento delle informazioni, dei documenti e degli atti amministrativi, dei quali venga a conoscenza durante l'esecuzione della prestazione.

In tal senso il **Responsabile**, si impegna a consegnare, alla firma del presente accordo, al Titolare e al suo DPO, se nominato, le istruzioni impartite agli autorizzati coinvolti nell'esecuzione dei trattamenti svolti per conto del Titolare.

In particolare, ai sensi dell'art. 28 GDPR, Regione Toscana – Giunta Regionale si impegna a:

- adottare e mantenere aggiornato un proprio registro dei trattamenti;
- non mettere in atto, per nessun motivo, trattamenti di dati diversi da quelli autorizzati dal Titolare oggetto del presente accordo e presenti, nel registro dei trattamenti. In tal senso renderà accessibile al Titolare il registro dei trattamenti, consentendo operazioni di consultazione, approvazione e diniego in relazione a singoli o gruppi di trattamenti;
- fornire per iscritto agli autorizzati al trattamento le necessarie istruzioni in tema;
- nominare gli autorizzati che svolgono le funzioni di "Amministratore di sistema", ai sensi dei provvedimenti del Garante italiano per la protezione dei dati personali del 27/11/2008 e del 25/6/2009, conservando i relativi estremi identificativi, definendo gli ambiti di operatività ai medesimi consentiti e comunicandone al titolare l'elenco nominativo con i relativi ambiti di operatività. A tal fine si precisa che gli Amministratori di sistema sono quelle figura professionali preposte ad attività finalizzate a garantire la sicurezza, la gestione e la manutenzione delle applicazioni, delle banche dati, dei sistemi e delle infrastrutture tecnologiche, svolgendo attività tecniche al fine di assicurare l'erogazione e la continuità dei servizi in sicurezza, sulla base delle indicazioni ricevute dal Responsabile, dei mezzi e degli strumenti a disposizione;
- predisporre e trasmettere, ogni qualvolta ciò appaia necessario, al Titolare una relazione in merito agli adempimenti eseguiti e alle misure di sicurezza adottate al fine di renderle e mantenerle sempre adeguate ed aggiornate rispetto alla evoluzione delle minacce e sulla base dei riscontri derivanti dalla registrazione continua e puntuale degli incidenti eventualmente occorsi;
- assistere e garantire il Titolare del trattamento nell'evasione delle richieste e del rispetto dei tempi previsti, nei rapporti con l'Autorità Garante per la protezione dei dati personali;
- assistere il Titolare al fine di dare seguito alle richieste per l'esercizio dei diritti degli interessati ai sensi degli artt. 15 a 22 del Regolamento UE; qualora gli interessati esercitino tale diritto verso il Responsabile, quest'ultimo è tenuto ad inoltrare tempestivamente e comunque nel più breve tempo possibile, le istanze al Titolare, supportando quest'ultimo al fine di fornire adeguato riscontro agli interessati nei tempi prescritti;
- assistere ed assicurare la piena, fattiva e puntuale collaborazione al Titolare del trattamento, nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36 del GDPR, tenendo conto della natura del trattamento, della tipologia di dati trattati, delle categorie e numerosità degli interessati;
- garantire al Titolare, su richiesta, l'accesso e la disponibilità permanente ai dati, su formati e strumenti di uso comune che ne garantiscano la fruizione da parte del Titolare, consentendo in tal modo la piena continuità dei servizi oggetto del presente appalto e in modo che mai si configuri una situazione di lock in. Il Titolare deve essere sempre messo in condizione di poter garantire la continuità del servizio, ferma restando l'interruzione/sospensione del servizio non imputabile al Responsabile;
- Tenuto conto della natura, dell'oggetto, del contesto e delle finalità del trattamento, il Responsabile del trattamento deve mettere in atto misure tecniche ed organizzative adeguate per garantire un livello di sicurezza adeguato al rischio e per garantire il rispetto

degli obblighi di cui all'art. 32 del Regolamento UE. Tali misure, individuate nell'Allegato 1) al presente accordo , comprendono tra le altre, se del caso:

- la capacità di assicurare, su base permanente, la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi che trattano i dati personali;
- la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico;
- una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento;

A tal fine si impegna ad assistere ed assicurare la piena, fattiva e puntuale collaborazione al titolare del trattamento.

- Restituire tutti i dati personali di pertinenza del Titolare, dopo che è terminata la prestazione dei servizi relativi al trattamento, cancellando le copie esistenti in proprio possesso, salvo che il diritto dell'Unione o degli Stati membri preveda la conservazione dei dati;
- il Responsabile informa tempestivamente e, in ogni caso senza ingiustificato ritardo dall'avvenuta conoscenza, il Titolare di ogni violazione di dati personali (cd. data breach); tale notifica è accompagnata da ogni documentazione utile, ai sensi degli artt. 33 e 34 del Regolamento UE, per permettere al Titolare del trattamento, ove ritenuto necessario, di notificare questa violazione all'Autorità Garante per la protezione dei dati personali, entro il termine di 72 ore da quanto il Titolare ne viene a conoscenza; nel caso in cui il Titolare debba fornire informazioni aggiuntive all'Autorità di controllo, il Responsabile supporterà il Titolare nella misura in cui le informazioni richieste e/o necessarie per l'Autorità di controllo siano esclusivamente in possesso del Responsabile e/o di suoi sub-Responsabili;
- sarà obbligo del Titolare del trattamento vigilare durante tutta la durata del trattamento, sul rispetto degli obblighi previsti dalle presenti istruzioni e dal Regolamento UE sulla protezione dei dati da parte del Responsabile del trattamento, nonché supervisionare l'attività di trattamento dei dati personali effettuando, ove necessario, audit, ispezioni e verifiche periodiche sull'attività posta in essere dal Responsabile. A tal fine il Responsabile del trattamento metterà a disposizione, su richiesta del titolare del trattamento, che deve pervenire al Responsabile con un preavviso di almeno 15 giorni, tutte le informazioni necessarie per dimostrare il rispetto degli obblighi derivanti dal regolamento UE, agevolando il contributo alle attività di revisione, comprese le ispezioni, realizzate dal Titolare del trattamento o da un altro soggetto da questi incaricato, ivi compresa, se necessario, l'attività di monitoraggio e controllo da parte del DPO, sulle misure di sicurezza attuate e sulla loro efficacia fornendo tutta la documentazione che sarà richiesta e collaborando attivamente alle attività di rilevazione e misura;
- comunicare al Titolare il nome ed i dati del proprio "Responsabile della protezione dei dati" (DPO), designato ai sensi dell'articolo 37 del Regolamento UE; il Responsabile della protezione dei dati personali (DPO) del Responsabile collabora e si tiene in costante contatto con il Responsabile della protezione dei dati (DPO) del Titolare;
- comunicare al Titolare, al DPO il nome e i riferimenti di contatto del proprio Responsabile della sicurezza IT;
- mettere in atto gli interventi necessari qualora l'attività di monitoraggio e controllo mettesse in evidenza punti di debolezza nelle misure e nelle tecniche adottate o qualora durante l'esecuzione dei trattamenti, la normativa in materia di Trattamento dei Dati Personali generi nuovi requisiti (ivi incluse nuove misure di natura fisica, logica, tecnica, organizzativa, in materia di sicurezza o trattamento dei dati personali), il Responsabile del

trattamento si impegna a collaborare - nei limiti delle proprie competenze tecniche, organizzative e delle proprie risorse - con il Titolare affinché siano sviluppate, adottate e implementate misure correttive di adeguamento ai nuovi requisiti;

- al fine dello svolgimento della valutazione dei rischi in fase di DPIA, il Responsabile si impegna a collaborare con il Titolare, assicurando una piena, fattiva e puntuale informazione sugli asset coinvolti nel trattamento, in particolare sulle minacce e sulle misure di sicurezza adottate e sulle loro correlazioni;
- non trasferire i dati personali di cui al presente accordo verso un paese terzo o un'organizzazione internazionale se non su istruzione documentata del Titolare o per adempiere a una norma del diritto dell'Unione o dello Stato membro cui è soggetto il Responsabile del trattamento.

Nel caso in cui per le prestazioni affidate dal Titolare al Responsabile, quest'ultimo ritenga di avvalersi di ulteriori soggetti, è autorizzato sin d'ora, alla nomina di altri responsabili del trattamento (d'ora in poi "sub-responsabili"), previa informazione al Titolare. Il Responsabile del trattamento si impegna a fornire l'elenco dei sub-responsabili sino d'ora incaricati, e, in caso di sostituzione o aggiunta di nuovi sub-responsabili, prima della stipula dei relativi contratti di esternalizzazione di servizi, a trasmettere al Titolare l'identità ed i dati di contatto del nuovo sub-responsabile, con le relative attività di trattamento delegate. Se entro 15 giorni dal ricevimento delle suddette informazioni il Titolare non si oppone, il contratto di esternalizzazione con il nuovo sub-responsabile può essere stipulato.

Il Responsabile, prima di procedere alla nomina di un soggetto terzo quale sub-responsabile del trattamento, è tenuto ad assicurarsi che lo stesso presenti garanzie sufficienti in termini di competenza e conoscenza specialistica, affidabilità e risorse per l'adozione di misure tecniche e organizzative appropriate di modo che il trattamento dei dati risponda ai principi e alle esigenze del GDPR, e deve:

- far rispettare obblighi analoghi a quelli forniti dal Titolare al Responsabile del trattamento, riportati in uno specifico contratto o atto di nomina. Qualora il sub-responsabile ometta di adempiere ai propri obblighi in materia di protezione dei dati, il Responsabile conserva nei confronti del Titolare l'intera responsabilità dell'adempimento degli obblighi del sub-responsabile
- far adottare agli eventuali sub-responsabili, idonee e preventive misure di sicurezza tecniche ed organizzative appropriate, atte ad eliminare o, comunque, a ridurre al minimo qualsiasi violazione, rischio di distruzione o perdita, anche accidentale, dei dati personali trattati, di accesso non autorizzato o di trattamento non consentito o non conforme, nel rispetto delle disposizioni contenute nell'articolo 32 del GDPR;

I sub responsabili di cui si avvale attualmente Regione Toscana sono i seguenti:

- **Engineering S.p.A.** che svolge l'attività di assistenza all'utenza dei sistemi oggetto nel presente documento;
- **R.T.I. con società capogruppo Telecom Italia S.p.A. (TIM SpA) e con le società mandanti, Enterprise Services Italia s.r.l. (DXC), IBM Italia S.p.A., Lutech S.p.A., Dedalus S.p.A. e Kyndryl Italia SpA** che gestisce gli ambienti e le macchine dove sono dispiegati i sistemi;
- **R.T.I. Almaviva - The Italian Innovation Company S.p.A. in breve Almaviva S.p.A. (capogruppo), Almawave s.r.l., Indra Italia S.p.A. e Pricewaterhouse-Coopers Advisory S.p.A.** che gestisce il sistema di cooperazione di Regione Toscana

I trattamenti affidati dal Responsabile ai sub responsabili riguardano le funzioni ascrivibili all'amministratore di sistema sopra elencate e quelle di amministratori dei DB e degli ambienti degli applicativi citati.

ALLEGATO 1

Misure tecniche e organizzative, comprese misure tecniche e organizzative per garantire la sicurezza dei dati

Gli applicativi. oggetto del presente Data Protection Agreement. sono locati sulle infrastrutture di SCT (Sistema Cloud della Toscana), i cui servizi di gestione dell'infrastruttura fisica e informatica, backup, disaster recovery, e gestione e monitoraggio dei sistemi e della rete, sono soggetti a controllo per la certificazione in essere del Gestore ISO/27001.

In virtù di tale certificazione sono quindi attive anche misure per:

- ripristino tempestivo per la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
- assicurazione su base permanente della riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
- testing, verifica e valutazione per l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento;
- identificazione, autorizzazione e accessi fisici degli utenti;
- protezione dei dati durante la trasmissione verso l'utenza degli applicativi (ad esempio canali cifrati);
- garantire la sicurezza fisica dei luoghi in cui i dati personali sono trattati;
- garantire la registrazione degli eventi relativi agli accessi degli amministratori di sistema e database administrator;
- consentire la portabilità dei dati e/o garantire la cancellazione~~;~~

Gli applicativi, nella loro forma di codice sorgente, sono soggetti a processi di continuous integration e continuous delivery automatici, allo scopo di garantirne la qualità.

Nella loro forma di codice eseguibile sono invece soggetti a processi di vulnerability assessment, tesi a rilevare eventuali vulnerabilità presenti e sulle quali vengono attivati processi di remediation.

Il presente documento è firmato con firma digitale.

Per la Regione Toscana	Gianluca Vannuccini	firma digitale
Per il Comune/Unione		firma digitale