ALLEGATO C

ACCORDO PER IL TRATTAMENTO DEI DATI PERSONALI EX ART 28 (3) DEL REGOLAMENTO UE / 2016/679

Tra

Ragione Sociale Indirizzo……

Città Legale Rappresentante

Telefono…… Email……..

Responsabile della Protezione dei dati (DPO)

Nome……Cognome……

Email……..

che interviene in qualità di **Titolare del Trattamento**

e

La Società **Links Management & Technologies S.p.A.**, rappresenta dal dott. Giancarlo Negro in qualità di rappresentante legale, con sede in Lecce, Via Rocco Scotellaro 55, (C.F. 03351210756), il cui Responsabile della Protezione dei dati (DPO) è raggiungibile all'indirizzo email privacy@linksmt.it e che interviene n qualità di **Responsabile del Trattamento**

PREMESSO CHE

- Con D.G.R. 1871 del 14.10.2019 la Regione Puglia ha deliberato di approvare ''Puglia Digitale'', il programma triennale degli interventi finalizzati all' attuazione dell'Agenda Digitale pugliese e della strategia per la Crescita Digitale, in attuazione del Piano Triennale nazionale ICT 2019-2021. In virtù di tale atto la Regione Puglia ha definitivamente deliberato di assumere il ruolo di Soggetto Aggregatore Territoriale per il Digitale (SATD);
- Con Delibera n. 1948 del 30.11.2020 la Giunta Regionale ha approvato lo stanziamento di risorse per complessivi Euro 5.000,000,00 a valere sul POC Puglia 2014 - 2020 - Asse II - Azione 2.3 "Interventi per il potenziamento della domanda di ICT dei cittadini e imprese in termini di utilizzo dei servizi online, inclusione digitale e partecipazione in rete", destinandole alla realizzazione dell'intervento denominato "Innovazione Enti Locali della Regione Puglia";
- Con la stessa Delibera la Giunta Regionale ha approvato la scheda progettuale "Innovazione Enti Locali della Regione Puglia" ed ha delegato il Dirigente della Sezione Infrastrutture energetiche e digitali per tutti gli adempimenti conseguenti alla realizzazione dell'intervento "Innovazione Enti Locali della Regione Puglia";
- con Determinazione Dirigenziale n. 84 del 06.05.2021 la Sezione Infrastrutture energetiche e digitali, ora Sezione Crescita Digitale delle Persone del Territorio e delle Imprese, ha affidato alla società in-house InnovaPuglia S.p.A. la realizzazione del Piano Operativo "Innovazione Enti Locali della Regione Puglia";

- Nell'ambito di tali attività il Dirigente della Sezione competente ha chiesto ad InnovaPuglia di predisporre i documenti necessari per l'espletamento della procedura di gara finalizzata alla realizzazione di uno Sportello Telematico per gli Enti Locali e di un portale per il *digital onboarding* dei servizi offerti;
- InnovaPuglia ha trasmesso il Progetto di acquisto, comprensivo di Capitolato tecnico e di tutti gli altri documenti di gara, con nota prot. inpu/AOO_1/PROT/03/06/2021/0004328 e successivi nuovi invii con note prot. inpu/AOO_1/PROT/14/09/2021/0005988 e prot. inpu/AOO_1/PROT/28/09/2021/0006245 della versione definitiva;
- Con Atto Dirigenziale n. 159/DIR/2021/00199 del 11/10/2021 la Sezione Infrastrutture energetiche e digitali (ora Sezione Sezione Crescita Digitale delle Persone del Territorio e delle Imprese) ha avviato la procedura per l'affidamento dell'appalto specifico "Servizi per l'evoluzione del sistema sportello telematico giustizia verso la piattaforma sportello telematico e portale dei servizi per gli enti locali, da erogare in modalità SaaS", a valere sul POC Puglia 2014-2020. Asse II "Migliorare l'accesso, l'impiego e la qualità delle TIC " – Azione 2.3, mediante ricorso all'Accordo Quadro "Servizi di sviluppo, manutenzione, assistenza ed altri servizi in ambito ICT" di InnovaPuglia (Lotto 8 - CIG 7329233268), di cui all'art. 54 del D.Lgs. n. 50/2016, da aggiudicarsi con il criterio dell'offerta economicamente più vantaggiosa di cui all'art. 95 comma 2 del D.Lgs. n. 50/2016, nel rispetto e alle condizioni stabilite nella lettera di invito;
- con Atto DD n. 193/DIR/2022/00014 del 16/03/2022 della Sezione Trasformazione digitale (ora Sezione Sezione Crescita Digitale delle Persone del Territorio e delle Imprese) si è proceduto a disporre l'aggiudicazione dell'appalto al RTI costituito da Links Management and Technology S.p.A. con sede legale in Lecce (Le) alla Via Rocco Scotellaro n. 55 – Codice Fiscale 03351210756 – Partita IVA n. 03351210756 e DEDAGROUP PUBLIC SERVICES con sede legale a Trento (TN) CAP 38121 alla via di Spini n. 50 – Codice Fiscale n. 03188950103 – Partita IVA n. 017278660221;
- con D.G.R. n. 778 del 05/06/2025 la Giunta regionale ha provveduto, tra l'altro, a stanziare risorse complessive pari ad € 3.000.000,00 per dare copertura all'intervento "Innovazione digitale Enti territoriali: Potenziamento Hub di intermediazione digitale" previsto nell'Accordo per la Coesione sottoscritto tra la Presidenza del Consiglio dei Ministri e la Regione Puglia a valere su fondi FSC 2021;
- con D.D. 193/DIR/2025/00267, della Sezione Crescita Digitale delle Persone, del territorio e delle Imprese, si è proceduto a disporre l'affidamento dei "Servizi di gestione ed evoluzione della piattaforma e-Gov della Regione Puglia per gli enti locali", a valere fondi FSC 2021-2027 nell'ambito della Linea di intervento 02.01 - Tecnologie e servizi digitali, mediante adesione all'Accordo Quadro "Servizi Applicativi in ottica Cloud e Servizi di Demand e PMO per le Pubbliche Amministrazioni Locali (PAL) (ed. 3) – ID 2610 – Lotto 1", di cui all'art. 59 comma 4, lettera a) D.Lgs. 36/2023, al RTI composto da Enterprise Services Italia S.r.l., nella sua qualità di impresa mandataria capo-gruppo, e Datamanagement Italia S.p.A., Deda Next S.r.l., DS Tech S.r.l., Ennova Go S.r.l., Etna Hitech S.C.p.A., ICTLAB PA S.r.l., Links Management and Technology S.p.A., Parsec 3.26 S.r.l., Sopra Steria Group S.p.A., in qualità di mandanti;
- nell'ambito del suddetto affidamento permangono, in particolare, a carico della Società Links Management and Technology S.p.A., i servizi di Manutenzione adeguativa/correttiva, gestione del Portafoglio Applicativo e Gestione Operativa delle Piattaforme dello Sportello Telematico Enti Locali;
- InnovaPuglia è stata nominata dalla Regione Puglia quale Responsabile del Trattamento relativamente all'affidamento "Sviluppo dei servizi Cloud per la PA" DGR 1871/2019 e DGR 179/2020. Si precisa che nell'ambito di tale nomina InnovaPuglia, qualificata (QI1 e QC1) nel marketplace dell'Agenzia per la Cybersicurezza Nazionale come Cloud Service Provider (CSP), tratta esclusivamente i dati personali e identificativi dell'utenza che deve amministrare il Sistema Informativo Regionale "Sportello Telematico Enti Locali" sulla piattaforma Cloud, in quanto la gestione dei sistemi virtuali ospitati sul cloud è di esclusiva competenza dei Cloud Service Customer (CSC) e dei relativi fornitori denominati Cloud Service User (CSU).

Per tutto quanto su riportato,

- L'espletamento delle attività previste nell'ambito del contratto comporta il trattamento di dati personali da parte della Società in qualità di Responsabile del trattamento ex art 28 Reg. (UE) 2016/679 (d'ora in poi GDPR), rendendo necessario che tra le parti sia stipulato un accordo che disciplini la natura, la finalità e la durata del trattamento, il tipo di dati personali e le categorie degli interessati oltre che i compiti e responsabilità specifici del Responsabile;
- il Titolare, al fine di utilizzare i sistemi software di cui agli affidamenti su riportati, deve provvedere a sottoscrivere il succitato accordo con la Società aggiudicatrice cui è affidata la gestione della piattaforma "Sportello Telematico Enti Locali" in qualità di Responsabile del trattamento dati;
- il presente accordo stabilisce diritti e obblighi del Titolare e del Responsabile del trattamento riferiti all'appalto aggiudicato;
- il presente Accordo prevale su disposizioni simili contenute in altri accordi tra le parti;
- gli allegati 1, 2 costituiscono parte integrante dell'Accordo;
- il presente accordo **non comporta alcun diritto del Responsabile ad uno specifico compenso e/o indennità e/o rimborso derivante dal medesimo** a meno di specifiche implementazioni richieste che esulano dall'oggetto del contratto principale;

(inserire ragione sociale del Titolare)…… quale Titolare dei dati cui competono le decisioni in ordine alle finalità ed alle modalità del trattamento dei dati personali *(di seguito "Titolare")*, in persona del suo legale rappresentante, individua la società ***LINKS MANAGEMENT AND TECHNOLOGY S.P.A.*** quale Responsabile dei trattamenti dei dati personali *(di seguito "Responsabile")* effettuati in relazione al Servizio oggetto del contratto di cui al punto precedente e fornisce alla medesima istruzioni in merito ai predetti trattamenti.

1 DIRITTI E OBBLIGHI DEL TITOLARE

Il Titolare del trattamento è responsabile di garantire che il trattamento dei dati personali avvenga in conformità con l'articolo 24 del GDPR.

È intenzione del Titolare consentire l'accesso sia al Responsabile che alle persone autorizzate al trattamento per i soli dati personali la cui conoscenza sia necessaria per adempiere ai compiti loro attribuiti.

Il Titolare affida al Responsabile tutte le operazioni di trattamento dei dati personali necessarie per dare piena esecuzione al Servizio innanzi indicato.

Il Titolare si impegna a comunicare per iscritto al Responsabile qualsiasi variazione si dovesse rendere necessaria nelle operazioni di trattamento dei dati.

Il Titolare dichiara, inoltre, che i dati da lui trasmessi al Responsabile:

- sono pertinenti e non eccedenti rispetto alle finalità per le quali sono stati raccolti e successivamente trattati;
- in ogni caso, i dati personali, oggetto delle operazioni di trattamento affidate al Responsabile, sono raccolti e trasmessi rispettando ogni prescrizione della normativa applicabile. Resta inteso che rimane a carico del Titolare l'onere di individuare la base legale del trattamento dei dati personali degli interessati.

Il Titolare ha il diritto e l'obbligo di prendere decisioni riguardo le finalità e i mezzi del trattamento di dati personali.

2 OBBLIGHI DEL RESPONSABILE

Il Responsabile deve procedere al trattamento secondo le istruzioni del Titolare documentate mediante il presente accordo.

Istruzioni successive potranno essere fornite dal Titolare anche durante il trattamento di dati personali purché documentate per iscritto. In ogni caso, qualora le dette istruzioni dovessero comportare implementazioni non previste e/o non prevedibili alla stipula del contratto principale, le stesse dovranno essere concordate di volta in volta in termini di tempi/costi e fattibilità tra le parti.

Il Responsabile del trattamento informa immediatamente il Titolare qualora le istruzioni impartite dallo stesso violino il GDPR o le disposizioni applicabili in materia di protezione dei dati dell'UE o degli Stati membri.

Sarà cura del Responsabile vincolare le persone autorizzate al trattamento alla riservatezza o ad un adeguato obbligo legale di confidenzialità anche per il periodo successivo all'estinzione del rapporto di collaborazione intrattenuto con il Responsabile, in relazione alle operazioni di trattamento da esse eseguite.

Il Responsabile, nel designare per iscritto le persone autorizzate al trattamento, dovrà assicurarsi che esse abbiano accesso ai soli dati personali la cui conoscenza sia strettamente necessaria per adempiere ai compiti loro assegnati. Dovrà inoltre curarne la formazione sui temi relativi alla protezione dei dati personali.

Inoltre, ove applicabile e per quanto concerne i trattamenti effettuati per l'erogazione della fornitura dalle persone autorizzate al trattamento con mansioni di "Amministratore di Sistema", il Responsabile è tenuto altresì al rispetto delle previsioni relative alla disciplina sugli amministratori di sistema contenute nel provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008 modificato in base al provvedimento del 25 giugno 2009.

Il Responsabile, in particolare, si impegna a conservare direttamente e specificamente gli estremi identificativi delle persone fisiche preposte quali amministratori di sistema, e a fornirli prontamente al Titolare su richiesta del medesimo.

In caso di danni derivanti dal trattamento, il Responsabile ne risponderà qualora non abbia adempiuto agli obblighi del GDPR specificatamente diretti ai Responsabili del trattamento o abbia agito in modo difforme o contrario rispetto alle legittime istruzioni del Titolare, a meno che non dimostri che l'evento dannoso non gli sia in alcun modo imputabile.

3 SICUREZZA DEL TRATTAMENTO

Tenendo conto dello stato dell'arte, dei costi di implementazione e della natura, ambito, contesto e finalità del trattamento, come anche della probabilità e severità del rischio per i diritti e le libertà delle persone fisiche, il Titolare ed il Responsabile implementano appropriate misure tecniche ed organizzative per assicurare un livello di sicurezza adeguato al rischio.

Il Titolare valuta i rischi inerenti al trattamento per i diritti e le libertà degli interessati, ed implementa le misure idonee a mitigarli. A seconda della loro rilevanza, tali misure posso includere le seguenti:

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.

Il Responsabile assiste il Titolare nel garantire il rispetto degli obblighi relativi alle misure tecniche-organizzative di cui all'art. 32 GDPR, fornendo a quest'ultimo il dettaglio delle misure di sicurezza implementate per le operazioni del trattamento eseguite presso le proprie sedi e con i propri mezzi tecnico-organizzativi, insieme a tutte le altre informazioni necessarie al Titolare per ottemperare ai propri obblighi normativi.

Le misure di sicurezza tecnico-organizzative attuate dal Responsabile del trattamento sono elencate nell'**Allegato 1**, parte integrante del presente accordo.

4 SUB-RESPONSABILI

Il Responsabile del trattamento deve soddisfare i requisiti di cui all'articolo 28, paragrafi 2 e 4 del GDPR quando ricorre ad altro responsabile (altrimenti detto sub-responsabile).

Il Titolare concede al Responsabile preventiva autorizzazione generale per il ricorso a Sub-Responsabili. Il Responsabile informa per iscritto il Titolare di eventuali modifiche relative ad aggiunta o sostituzione di sub-responsabili con almeno 10 giorni di preavviso, dando in tal modo al Titolare modo di opporsi a tali cambiamenti prima che tali sub-responsabili vengano ingaggiati. All'informazione è allegata la dichiarazione da parte del sub responsabile di accettazione delle medesime obbligazioni oggetto del presente accordo.

Quando il Responsabile coinvolga un sub-responsabile per l'esecuzione di specifiche attività del trattamento operato per conto del Titolare, sullo stesso sub-responsabile devono essere imposte mediante un contratto o altro atto giuridico le stesse obbligazioni relative alla protezione dei dati contenute nel presente accordo, in particolare prevedendo sufficienti garanzie per quanto attiene all'adozione di appropriate misure tecniche ed organizzative tali da rendere il trattamento conforme ai requisiti del presente accordo e del GDPR.

Il Responsabile del trattamento è tenuto a richiedere che il sub-responsabile soddisfi almeno gli obblighi cui è esso stesso soggetto ai sensi del presente accordo e del GDPR, e che in questa prospettiva l'organizzazione interna del sub responsabile sia correttamente adeguata.

5 TRASFERIMENTO DEI DATI IN UN PAESE TERZO

Qualsiasi trasferimento di dati personali verso paesi terzi o organizzazioni internazionali da parte del responsabile del trattamento dei dati deve avvenire esclusivamente sulla base di istruzioni documentate da parte del Titolare e deve sempre avvenire in conformità al Capitolo V del GDPR.

Nel caso di trasferimenti verso paesi terzi o organizzazioni internazionali, richiesti dalla legislazione dell'UE o degli Stati membri a cui è soggetto il Responsabile del trattamento, e che non siano stati richiesti dal Titolare del trattamento con specifica istruzione, il Responsabile del trattamento chiede al Titolare l'autorizzazione al trattamento con queste modalità.

6 ASSISTENZA AL TITOLARE

Il Responsabile del trattamento dei dati deve inoltre, tenendo conto della natura del trattamento e delle informazioni disponibili fornire supporto al Titolare affinché possa ottemperare:

- all'obbligo del Titolare a effettuare senza indebito ritardo e, ove possibile, entro e non oltre 72 ore dalla sua conoscenza, la comunicazione circa una violazione dei dati personali all'Autorità per la Protezione dei Dati Personali a meno che non sia è improbabile che comporti un rischio per i diritti e le libertà delle persone fisiche;

- all'obbligo del Titolare di effettuare una valutazione dell'impatto delle operazioni di trattamento previste sulla protezione dei dati personali (una valutazione d'impatto sulla protezione dei dati);

- all'obbligo del Titolare del trattamento di consultare l'Autorità per la Protezione dei Dati personali prima di porre in essere un trattamento qualora una valutazione d'impatto indicasse che il trattamento comporterebbe un rischio elevato (in assenza di misure adottate dal Titolare di mitigazione del rischio).

- agli obblighi del Titolare nei confronti delle richieste di esercizio dei diritti dell'interessato stabilite nel capitolo III GDPR per quanto applicabile.

Il Responsabile sarà, inoltre, tenuto a comunicare tempestivamente al Titolare eventuali istanze degli interessati, contestazioni, ispezioni o richieste dell'Autorità di Controllo e dalle Autorità Giudiziarie, ed ogni altra notizia rilevante in relazione al trattamento dei dati personali oggetto del contratto.

Il Responsabile, in virtù delle attività svolte, è tenuto altresì a rispettare le previsioni vigenti in tema di amministratori di sistema, tra cui quelle contenute nel Provvedimento emanato il 27 novembre 2008 dall'Autorità Garante per la protezione dei dati personali, recante "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema", così come integrato dal successivo provvedimento datato 29 giugno 2009.
Nello specifico, il Responsabile dovrà:

1. predisporre, aggiornare e conservare l'elenco contenente gli estremi identificativi delle persone fisiche preposte quali amministratori di sistema;
2. comunicare a Regione Puglia l'elenco aggiornato contenente gli estremi identificativi delle persone fisiche preposte quali amministratori di sistema, specificando quali siano gli amministratori di sistema che nell'ambito delle proprie funzioni e mansioni abbiano la possibilità di intervenire sui dati personali di pertinenza o comunque in possesso del Titolare. In particolare, deve essere specificato quali Amministratori di sistema possano effettuare sul database ricerche nominative o sulla base di altri parametri tra quelli utilizzati per l'accesso allo Sportello telematico. Il suddetto elenco dovrà essere comunicato a Regione Puglia:
    a. ogniqualvolta quest'ultimo ne faccia richiesta;
    b. ogniqualvolta sia inserita una nuova persona fisica preposta quale amministratore di sistema (con l'elenco delle funzioni ad essi attribuite);
    c. comunque, con periodicità almeno trimestrale.
3. verificare annualmente l'operato degli amministratori di sistema in modo da controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza riguardanti i trattamenti dei dati personali previste dalle norme vigenti;
4. adottare sistemi idonei alla registrazione degli accessi logici (c.d. autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte degli amministratori di sistema. Tali registrazioni (access log) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo per cui sono richieste. Esse

devono altresì comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate. In particolare, nell'ipotesi in cui sia stata effettuata una ricerca nominativa o una ricerca basata sugli altri parametri utilizzati per l'accesso allo Sportello telematico, devono essere indicati nel registro i seguenti dati:

- amministratore di sistema che ha effettuato la ricerca,
- data e orario della ricerca,
- query,
- motivazioni della ricerca.

Le summenzionate registrazioni, inoltre, devono essere conservate per un periodo congruo, non inferiore a 1 (uno) anno, durante il quale devono essere rese disponibili a Regione Puglia ogniqualvolta il medesimo ne faccia richiesta e, comunque, ogni sei mesi.
Il Titolare potrà chiedere a Regione Puglia di visionare tale documentazione.

7 NOTIFICA DEL DATA BREACH

In caso di violazione dei dati personali, il Responsabile del trattamento deve informare il Titolare della violazione (o presunta violazione) entro 48 dopo che il Responsabile ne è venuto a conoscenza per consentire al Titolare la notifica della violazione dei dati personali all'autorità di controllo competente così come previsto dall'Articolo 33 del GDPR. Di tale eventuale violazione e delle azioni conseguenti, deve essere resa edotta anche Regione Puglia.

Le parti definiscono nell'**Allegato 2** tutti gli elementi che devono essere forniti dal responsabile al Titolare del trattamento nella notifica di una violazione dei dati personali.

8 CANCELLAZIONE E RESTITUZIONE DEI DATI

Al termine delle operazioni di trattamento affidate, nonché all'atto della cessazione per qualsiasi causa del trattamento da parte del Responsabile, lo stesso sarà tenuto a restituire al Titolare i dati personali oggetti del trattamento, con contestuale integrale distruzione comunicando se e quali dati debbano essere conservati in quanto sia richiesto da norme di legge od altri fini (contabili, fiscali, ecc.).

Il Responsabile provvederà a rilasciare al Titolare apposita dichiarazione per iscritto contenente l'attestazione che presso il Responsabile non esista alcuna copia dei dati personali e delle informazioni di titolarità del Titolare.

9 AUDIT E ISPEZIONI

Il responsabile del trattamento mette a disposizione del Titolare tutte le informazioni necessarie per dimostrare la conformità agli obblighi di cui all'articolo 28 GDPR e si rende disponibile per le attività di audit, comprese le ispezioni, condotte dal Titolare del trattamento, o da un altro revisore dallo stesso incaricato.

A tal scopo, il Responsabile riconosce al Titolare, ed agli incaricati del medesimo, il diritto di richiedere evidenza delle certificazioni più recenti emesse da terze parti accreditate. In subordine, qualora il Titolare abbia bisogno di ulteriori informazioni per adempiere ai propri obblighi di audit, avrà la facoltà di richiedere al Responsabile ulteriori evidenze, e, se del caso, previo congruo preavviso di 5 giorni lavorativi, di accedere ai locali del fornitore presso i quali si svolgono le operazioni di trattamento.

In ogni caso, il Titolare si impegna per sé e per i terzi incaricati da quest'ultimo, a che le informazioni raccolte durante le operazioni di verifica siano utilizzate solo per finalità di audit, e che le operazioni di verifica si svolgano in modo tale da non interferire con la normale attività produttiva del Responsabile.

10 CESSAZIONE DELL'ACCORDO

La presente nomina avrà efficacia fintanto che venga erogato il Servizio e finché il responsabile comunque disponga, anche in fatto e indirettamente, dei dati. Qualora il Servizio comporti un'esecuzione periodica e/o continuativa, rinnovata di volta in volta con specifici contratti, la presente nomina si intende efficace per la durata complessiva del Servizio.

11 COMUNICAZIONI TRA LE PARTI

Le comunicazioni tra le parti, ai fini del presente incarico, dovranno essere indirizzate:

- per il Responsabile del trattamento: Links Management and Technology SpA, Via Rocco Scotellaro 55, Lecce, links@legalmail.it.
- per il Titolare del trattamento *(ragione sociale azienda Cliente, sede legale, PEC)*.

Per conto del Titolare	**Per conto del Responsabile**
_____	_____

Allegato 1 Misure di sicurezza
Allegato 2 Scheda evento Data Breach

Allegato 1 – Caratteristiche del trattamento e Misure tecniche e organizzative

Dettagli Trattamento

☒Application Maintenance Management

☒Funzioni di Amministratore Di Sistema

☒Customer Support

☒Sviluppo Prodotto

Categorie di Interessati

I Dati Personali trattati riguardano le seguenti categorie di Interessati:

☒Dipendenti ☒Altro (specificare) Cittadini e Imprese

Tipologia di Dati Personali

I Dati Personali trattati dall'Appaltatore per conto del Titolare del Trattamento riguardano le seguenti categorie di Dati Personali:

☒Dati personali comuni (es. dati anagrafici, di contatto, relativi all'istruzione, stato civile/familiare, esperienza professionale)

☒Dati Finanziari (es. reddito, transazioni finanziarie, investimenti, carte di credito, fatture, ecc.)

☐Dati Particolari (es. sulla salute, genetici, biometrici, opinioni politiche, vita sessuale, ecc.)

☐Dati Giudiziari (es. dati relativi a condanne penali, ecc.)

Caratteristiche del Trattamento

☒I trattamento avviene (in parte)[1] presso la sede del Responsabile
☒I Responsabile svolge anche o solo attività di Amministratore di Sistema e/o gli accessi sono gestiti dal Responsabile
☐ dati (o parte di essi) sono conservati solo o anche dal Responsabile (ovvero il Responsabile ne conserva una copia)
☐ dati (o parte di essi) sono trattati tramite applicazioni deployate sui server del Responsabile
☒ desktop/laptop/mobile devices (o alcuni di essi) utilizzati per il trattamento sono forniti dal Responsabile
☒I software/applicazione/ecc. utilizzato per il trattamento è fornito e/o manutenuto dal Responsabile

Misure di Sicurezza

Il Responsabile e/o Sub-Responsabile e/o suoi ulteriori Responsabili adotteranno le seguenti misure di sicurezza al fine di garantire un livello di sicurezza adeguato al rischio relativo alle attività che ricadono nella loro diretta responsabilità.

[1] Il trattamento avviene dalla sede del responsabile da remoto sul Datacenter Regionale con strumenti e connessioni sicure per le consequenziali attività di verifica e per la conduzione operativa della infrastruttura.

Il Cliente, in considerazione dei rischi associati al Trattamento dei Dati Personali, conferma che le Misure di Sicurezza adottate dal Responsabile e/o Sub-Responsabile e/o suoi ulteriori Responsabili sono idonee a fornire un adeguato livello di protezione dei Dati Personali trattati per conto dello stesso.

Nel caso in cui il Cliente operasse per conto di un Titolare terzo, il Cliente si riserverà di integrare e/o modificare le misure di sicurezza come richiesto dallo stesso Titolare.

Risk Level	Categoria	ID	Descrizione
B	**Security Policy e procedure per la protezione dei dati personali**	**A.1**	L'organizzazione documenta la propria politica in merito all'elaborazione dei dati personali come parte della sua politica di sicurezza delle informazioni.
B	**Security Policy e procedure per la protezione dei dati personali**	**A.2**	La politica di sicurezza è riesaminata e aggiornata, se necessario, su base annuale.
B	**Ruoli e responsabilità**	**B.1**	I ruoli e le responsabilità relativi al trattamento dei dati personali sono chiaramente definiti e assegnati in conformità con la politica di sicurezza.
B	**Ruoli e responsabilità**	**B.2**	Durante le riorganizzazioni interne o le cessazioni e il cambio di impiego, sono chiaramente definite le modalità di revoca dei diritti e delle responsabilità con le rispettive procedure di passaggio di consegne.
B	**Gestione degli asset/risorse**	**D.1**	L'organizzazione dispone di un registro delle risorse IT utilizzate per il trattamento dei dati personali (hardware, software e rete). Il registro include almeno le seguenti informazioni: risorsa IT, tipo (ad es. server, workstation), posizione (fisica o elettronica). Ad una persona specifica è assegnato il compito di mantenere e aggiornare il registro (ad esempio, il responsabile IT).
B	**Gestione degli asset/risorse**	**D.2**	Le risorse IT sono riesaminate e aggiornate regolarmente.
B	**Gestione del cambiamento**	**E.2**	Lo sviluppo del software è eseguito in un ambiente speciale, non collegato al sistema IT utilizzato per il trattamento dei dati personali. Quando è necessario eseguire l test, sono utilizzati dati fittizi (non dati reali). Nei casi in cui ciò non è possibile, sono previste procedure specifiche per la protezione dei dati personali utilizzati nei test.
B	**Gestione degli incidenti / Data Breaches**	**G.1**	È definito un piano di risposta agli incidenti con procedure dettagliate per garantire una risposta efficace e ordinata agli incidenti relativi ai dati personali.
B	**Gestione degli incidenti / Data Breaches**	**G.2**	Le violazioni dei dati personali sono segnalate immediatamente alla Direzione. Sono in atto procedure di notifica per la segnalazione delle violazioni alle autorità competenti e agli interessati, ai sensi dell'art. 33 e 34 GDPR.
B	**Business Continuity**	**H.1**	L'organizzazione stabilisce le procedure e i controlli principali da seguire al fine di garantire il livello richiesto di continuità e disponibilità del sistema informatico che elabora i dati personali (in caso di incidente / violazione dei dati personali).
B	**Riservatezza del personale**	**I.1**	L'organizzazione garantisce che tutto il personale comprenda le proprie responsabilità e gli obblighi relativi al trattamento dei dati personali. I ruoli e le responsabilità sono chiaramente comunicati durante il processo di pre-assunzione e / o inserimento.
B	**Formazione**	**J.1**	L'organizzazione garantisce che tutto il personale sia adeguatamente informato sui controlli di sicurezza del sistema informatico relativi al suo lavoro quotidiano. Il personale coinvolto nel trattamento dei dati personali è inoltre adeguatamente informato in merito ai requisiti in materia di protezione dei dati e agli obblighi legali attraverso regolari

Risk Level	Categoria	ID	Descrizione
			campagne di sensibilizzazione.
B	**Controllo degli accessi ed autenticazione**	**K.2**	L'uso di account generici (non personali) è evitato. Nei casi in cui ciò è necessario, si garantisce che tutti gli utenti che usano l'account generico abbiano gli stessi ruoli e responsabilità.
B	**Controllo degli accessi ed autenticazione**	**K.3**	E' presente un meccanismo di autenticazione che consenta l'accesso al sistema IT (basato sulla politica e sul sistema di controllo degli accessi). Come minimo è utilizzata una combinazione di user-id e password. Le password rispettano un certo livello (configurabile) di complessità.
B	**Logging e monitoraggio**	**L.1**	I log sono attivati per ogni sistema / applicazione utilizzata per il trattamento dei dati personali. Includono tutti i tipi di accesso ai dati (visualizzazione, modifica, cancellazione).
B	**Logging e monitoraggio**	**L.2**	I log sono registrati con marcatura temporale (timestamp) e adeguatamente protetti da manomissioni e accessi non autorizzati. Gli orologi sono sincronizzati con un'unica fonte temporale di riferimento.
B	**Sicurezza desktop/laptop/mobile**	**N.1**	Gli utenti non sono in grado di disattivare o aggirare le impostazioni di sicurezza.
B	**Sicurezza desktop/laptop/mobile**	**N.3**	Gli utenti non hanno i privilegi per installare o disattivare applicazioni software non autorizzate.
B	**Sicurezza desktop/laptop/mobile**	**N.4**	Il sistema ha timeout di sessione quando l'utente non è stato attivo per un certo periodo di tempo.
B	**Sicurezza desktop/laptop/mobile**	**N.5**	Gli aggiornamenti critici di sicurezza rilasciati dallo sviluppatore del sistema sono installati regolarmente.
B	**Network/Communication security**	**O.1**	Ogni volta che l'accesso viene eseguito tramite Internet, la comunicazione è crittografata tramite protocolli crittografici (TLS / SSL).
B	**Sicurezza del ciclo di vita del software**	**R.1**	Durante il ciclo di vita dello sviluppo si seguono le migliori pratiche, lo stato dell'arte e pratiche, framework o standard di sicurezza ben noti.
B	**Sicurezza del ciclo di vita del software**	**R.2**	Specifici requisiti di sicurezza sono definiti durante le prime fasi del ciclo di vita dello sviluppo.
B	**Sicurezza del ciclo di vita del software**	**R.5**	Durante lo sviluppo, sono eseguiti test e convalida rispetto all'implementazione dei requisiti di sicurezza iniziali.

ALLEGATO 2 – SCHEDA EVENTO DATA BREACH

Denominazione della Banca Dati oggetto di incidente e breve descrizione della violazione

_____

_____

Quando si è verificata la violazione dei dati personali nell'ambito della Banca dati?

☐Il __/__/____

☐Tra il __/__/____ e __/__/____

☐In un periodo non ancora determinato

☐E' possibile sia ancora in corso

Dove è avvenuta la violazione?

(specificare se avvenuta a seguito di smarrimento dispositivo o di supporto portatile)

_____

_____

Tipo Violazione

☐Riservatezza (divulgazione dei dati, accesso agli stessi non autorizzati o accidentali)
☐Integrità (modifica non autorizzata o accidentale dei dati)
☐Disponibilità (perdita, accesso o distruzione accidentali o non autorizzati di dati)
☐Lettura (i dati probabilmente non sono stati copiati)
☐Copia (i dati sono ancora presenti sui sistemi del Titolare)
☐Alterazione (i dati sono presenti nei sistemi ma sono stati alterati)
☐Cancellazione (i dati non sono più nella disponibilità del Titolare o di terzi)
☐Furto
☐Altro:

_____

_____

Dispositivo oggetto della violazione

☐Computer
☐Rete
☐Dispositivo mobile
☐Strumento di Backup:
☐Documento Cartaceo
☐Altro:

_____

_____

Sintetica descrizione dei sistemi di elaborazione e/o memorizzazione dati coinvolti

_____

_____

Ubicazione: _____

Quante persone sono state colpite dalla violazione

☐N°_____ persone
☐Circa _____
☐N° non ancora conosciuto:

Tipologia Dati Oggetto Di Violazione

☐Dati anagrafici
☐Dati di accesso/ identificazione
☐Dati relativi a minori
☐Dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche ecc
☐Dati personali idonei a rivelare lo stato di salute e la vita sessuale
☐Dati Giudiziari
☐Copia immagini documenti digitali
☐Ancora sconosciuto
☐Altro

Misure tecniche ed organizzative applicate ai dati oggetto di violazione

(indicare le misure di sicurezza implementate prima del verificarsi dell'evento che dovrebbero coincidere con quelle riportate nell'apposito accordo per il trattamento dei dati)

_____

_____

Quali misure tecnologiche ed organizzative sono state assunte o saranno assunte per contenere la violazione dei dati e/o prevenire simili violazioni

(indicare le misure di sicurezza adottate per arginare gli effetti della gli effetti della violazione e/o impedirne il perpetrarsi o il ripersi della stessa)

_____

_____