

## NOMINA DEL SUB-RESPONSABILE DEL TRATTAMENTO ESTERNO

ai sensi del Regolamento Generale sulla Protezione dei Dati UE 2016/679

La Società ERAMUS SRL con sede in San Cesareo RM codice fiscale e Partita IVA: **10241261006**  
PEC: [posta@pec.erasmus.it](mailto:posta@pec.erasmus.it), in persona dell'Amministratore Unico Matteo Mauri, in qualità di

### RESPONSABILE DEL TRATTAMENTO DEI DATI PERSONALI

*dei contribuenti\cittadini\imprese del Comune di Tivoli, in virtù del servizio di supporto erogato al medesimo  
Ente Locale*

VISTO il Regolamento UE 2016/679, ad oggetto: "Regolamento europeo in materia di protezione dei dati personali", di seguito GDPR;

VISTO il Decreto Legislativo 30 giugno 2003, n. 196, ad oggetto: "Codice in materia di protezione dei dati personali", come novellato dal D.Lgs. 101/2018;

PRESO ATTO che:

1. L'art. 4 comma 8 del suddetto Regolamento definisce il Responsabile come: *"la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento"*.
2. L'art. 28 del suddetto Regolamento stabilisce che:
  - a. comma 1) *"Qualora un trattamento debba essere effettuato per conto del titolare del trattamento, quest'ultimo ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato"*.
  - b. comma 3) *"I trattamenti da parte di un responsabile del trattamento sono disciplinati da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, che vincoli il responsabile del trattamento al titolare del trattamento e che stipuli la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento"*.

### RICORRE

Per l'esecuzione di specifiche attività di trattamento di dati personali riferibili al servizio di "realizzazione della piattaforma OpenPA 5.0" alla società DATATELLERS S.R.L, Part. IVA 02847840218, giusto contratto sottoscritto tra le parti, in qualità di sub-responsabile del trattamento.

La Società DATATELLERS S.R.L. con sede in Bolzano (BZ), Piazza Fiera, 1 cap 39100, Codice fiscale, partita iva e n.iscr. al Registro Imprese 02847840218, e-mail: [amministrazione@datatellers.info](mailto:amministrazione@datatellers.info), P.E.C.: [datatellers@legalmail.it](mailto:datatellers@legalmail.it), in persona dell'Amministratore Delegato, Riccardo Valletti, è pertanto designata sub-responsabile del trattamento di dati personali, secondo quanto specificato di seguito, per il servizio di "realizzazione della piattaforma OpenPA 5.0", giusto contratto tra le parti.

Il Responsabile del trattamento autorizza il sub-responsabile a trattare i dati personali nel rispetto del Regolamento Generale sulla Protezione dei dati UE 2016/679 e secondo quanto disciplinato all'interno del presente atto, per lo svolgimento dei compiti previsti dal contratto principale e dalle disposizioni vigenti disposte dalla legislazione in materia di settore.

L'ambito e la natura del trattamento autorizzato, le finalità del trattamento da rispettare, le tipologie di dati personali da trattare e le categorie di soggetti interessati coinvolti, nonché tutti gli altri aspetti connessi al trattamento, sono esplicitate nell'Allegato 1.

## **DOVERI E DIRITTI**

Il Titolare del trattamento ha l'obbligo di adempiere a quanto prescritto dal Regolamento UE 2016/679 e di assicurare che il trattamento di dati personali svolto, direttamente o per suo conto dai Responsabili esterni nominati, rispetti i principi sanciti.

Il Titolare del trattamento ha il diritto di vincolare il trattamento dei dati personali svolto dal Responsabile a specifiche istruzioni che lo stesso è tenuto a rispettare.

Il Responsabile ed i sub-responsabili, per quanto di propria competenza, è tenuto al rispetto dei Principi applicabili al trattamento di dati personali, ai sensi dell'art. 5 del Regolamento Generale sulla Protezione dei Dati, anche per i propri dipendenti e collaboratori, degli obblighi di riservatezza, integrità e tutela dei dati, nonché a garantire l'utilizzo dei dati stessi esclusivamente per le finalità espresse nel presente documento e nel contratto sottoscritto tra le parti.

Il sub-responsabile risponde direttamente in caso di eventuali violazioni derivanti da una sua condotta illecita o scorretta o in contrasto con i principi del Regolamento o le istruzioni impartite dal Responsabile. A tale scopo, il sub-responsabile deve collaborare con il Responsabile ed assisterlo nei casi in cui l'interessato eserciti i propri diritti, elencati nel Regolamento, adottando opportune misure organizzative e tecniche, nonché nei casi di evento di "data breach" o di necessaria valutazione d'impatto.

Il sub-responsabile, inoltre, si impegna a mantenere indenne il Responsabile del trattamento per qualsiasi sanzione, richiesta e/o danno o spesa, incluse quelle legali, che possano derivare da un mancato rispetto della normativa in materia di protezione dei dati personali allo stesso imputabile, ivi compresi eventuali risarcimenti danni avanzati dai soggetti Interessati, fatto salvo il mancato rispetto della normativa in materia di protezione dei dati personali sia imputabile al Responsabile del trattamento ed il sub-responsabile abbia agito in fede ai requisiti contrattuali.

## **SICUREZZA DEL TRATTAMENTO**

Per i trattamenti operati attraverso la propria organizzazione, il sub-responsabile, prestatore di servizi, deve garantire l'adozione di un sistema di misure di sicurezza di tipo tecnico ed organizzativo, ritenuto adeguato rispetto ai trattamenti da effettuare ed ai livelli di rischio presenti secondo i principi espressi all'art. 32 del Regolamento. A tal fine, il sub-responsabile, in considerazione dello stato dell'arte, dei costi di attuazione, della natura, dell'oggetto, del contesto e delle finalità del trattamento, nonché dei rischi derivanti, in particolare, dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trattati, si impegna a mettere in atto le misure tecniche e organizzative descritte Allegato 2 alla presente lettera.

## **COMPROVA DELLA CONFORMITÀ**

Il sub-responsabile del Trattamento è tenuto a dimostrare il rispetto dei principi espressi dal Regolamento durante lo svolgimento delle attività di trattamento, inclusa l'adeguatezza e l'efficacia delle misure adottate.

Il sub-responsabile, se richiesto o necessario, mette a disposizione le informazioni e la documentazione atta a dimostrare tale conformità, oltre a contribuire in caso di attività di verifica dell'adempimento delle presenti disposizioni svolta da parte del Responsabile o dell'Autorità di controllo preposta.

A tal riguardo il sub-responsabile:

- consente l'accesso alla propria sede o a qualsiasi altro locale ove si svolgono le attività di trattamento dei dati;
- garantisce la possibilità di intervistare i soggetti autorizzati al trattamento;
- permette l'accesso ai sistemi informativi e strumenti informatici ove avvengono le operazioni di trattamento.

## **NOTIFICA DI VIOLAZIONE**

Il sub-responsabile ha l'obbligo di informare il Titolare nel caso in cui si verifichi una violazione dei dati personali, senza ingiustificato ritardo e, in ogni caso, entro e non oltre 36 ore dal momento in cui ne è venuto a conoscenza. In tal modo il Responsabile, opportunamente avvertito, avrà il tempo necessario per notificare la violazione all'autorità di controllo e, ove necessario, agli Interessati.

Il sub-responsabile, al momento della dichiarazione di violazione, dovrà fornire le seguenti informazioni in merito:

- alla natura della violazione dei dati personali, alle categorie e al numero approssimativo dei soggetti interessati coinvolti;
- alle probabili conseguenze della violazione dei dati personali;
- alle misure adottate o che intende adottare per porre rimedio alla violazione dei dati personali e, eventualmente, per attenuarne i possibili effetti negativi.

Il sub-responsabile deve, inoltre, essere a conoscenza del fatto che per la violazione delle disposizioni in materia di trattamento dei dati personali sono anche previste sanzioni di natura penale.

In ogni caso la responsabilità penale per eventuale uso non corretto dei dati oggetto di tutela resta a carico della singola persona cui l'uso illegittimo degli stessi sia imputabile.

In merito alla responsabilità civile, si fa rinvio all'art. 154 del Codice di Procedura Civile, che dispone relativamente ai danni cagionati per effetto del trattamento ed ai conseguenti obblighi di risarcimento, implicando, a livello pratico, che, per evitare ogni responsabilità, l'operatore è tenuto a fornire la prova di avere applicato le misure tecniche di sicurezza più idonee a garantire appunto la sicurezza dei dati detenuti.

## **ISTRUZIONI PER IL SUB-RESPONSABILE**



Il sub-responsabile del Trattamento si impegna ad impartire per iscritto, ai propri collaboratori autorizzati al trattamento, istruzioni in merito alle operazioni di trattamento dei dati personali ed a vigilare sulla loro puntuale applicazione in accordo del considerando art. 28 del Regolamento UE 679/2016.

Tutti i dati personali devono essere conservati sotto la esclusiva e diretta responsabilità del sub-responsabile del Trattamento mediante le attività e le relative procedure adottate dallo stesso.

Il sub-responsabile del Trattamento dovrà garantire alla specifica categoria di interessati i diritti previsti dal Regolamento 2016/679 e i diritti di informazione previsti dalle norme che disciplinano la materia di riferimento.

Pertanto:

- i dati devono essere trattati solo per l'erogazione dei servizi espressi all'interno del contratto e/o secondo quanto stabilito in altri atti documentabili, tra cui la presente lettera. Non è consentito effettuare ulteriori trattamenti che possano differire da tali finalità, salvo che non sia espressamente richiesto dal responsabile del trattamento o derivi da obblighi di legge.
- il sub-responsabile del trattamento non deve comunicare a terzi o diffondere i dati personali dei soggetti Interessati, se non previa autorizzazione del responsabile del trattamento.
- il sub-responsabile è tenuto ad adottare tutte le misure adeguate al trattamento, richieste ai sensi dell'articolo 32 del Regolamento e, ove previsto, dal responsabile.
- è onere del sub-responsabile avvertire il responsabile qualora si configuri un qualsiasi rischio derivante dal trattamento di dati per la gestione dei servizi affidati o ad essi conseguenti.
- il sub-responsabile si impegna ad individuare gli addetti da destinare al servizio e a designarli quali persone autorizzate al Trattamento;
- il sub-responsabile deve garantire che le persone autorizzate al trattamento dei dati personali sotto la sua autorità si siano impegnate alla riservatezza e siano adeguatamente istruite affinché svolgano il trattamento di dati personali nel rispetto del Regolamento e delle istruzioni impartite dal responsabile.
- il sub-responsabile è tenuto a collaborare con il responsabile del trattamento, tramite adeguate misure tecniche e organizzative, affinché sia garantito un corretto riscontro in caso di richieste pervenute dagli Interessati per l'esercizio dei propri diritti, ivi compreso il diritto all'oblio e alla portabilità ove applicabili.
- il sub-responsabile assiste il responsabile nell'adozione di adeguate misure di sicurezza.
- Il sub-responsabile deve redigere il registro delle attività di trattamento in conformità ai requisiti previsti all'art. 30, comma 2 del GDPR.

Il sub-responsabile si impegna ad osservare la massima riservatezza nel trattamento dei dati ed in particolar modo si impegna a rispettare il divieto di comunicazione a terzi e di diffusione dei dati personali trattati; questi rimangono di proprietà del Titolare.

#### **TERMINE DELLA PRESTAZIONE**

La presente designazione avrà la medesima durata del Contratto. Qualora questo venisse meno o perdesse efficacia e per qualsiasi motivo, anche la presente nomina verrà automaticamente meno senza bisogno di comunicazioni o revoche, ed il sub-responsabile non sarà più legittimato a trattare i dati qui considerati.

Nella conclusione del servizio oggetto dell'accordo, la presente nomina si intenderà revocata e il sub-responsabile dovrà consegnare al responsabile, se espressamente richiesto, gli archivi informatici e cartacei contenenti i dati personali oggetto della presente lettera.

Per tutto quanto non espressamente previsto nel presente atto, si rinvia alle disposizioni generali vigenti in materia di protezione dei dati personali e in aderenza alla specifica materia di riferimento

Una copia del presente atto di nomina viene restituita al responsabile, debitamente firmata per accettazione.

San Cesareo li, 11/11/2024

Sub-Responsabile del Trattamento  
(Per accettazione dell'incarico)

**DATATELLERS S.R.L.**

L'Amministratore Delegato  
Riccardo Valletti




**Responsabile Del Trattamento**

ERAMUS SRL

L'Amministratore Unico

Matteo Mauri



**PARTE I - DESCRIZIONE SERVIZIO**

**Descrizione del servizio:**

servizio di "realizzazione della piattaforma OpenPA 5.0" giusto contratto sottoscritto tra le parti;

**Descrizione delle finalità:**

realizzazione della piattaforma OpenPA 5.0 giusto contratto sottoscritto tra le parti;

**PARTE II – DESCRIZIONE DEL TRATTAMENTO E TIPOLOGIA DI DATI**

<b>1 – Soggetti Interessato</b>														
<p>Nell'esecuzione del Contratto, il sub-responsabile del trattamento può trattare Dati Personali relativi alle seguenti categorie di Interessati:</p> <p>X <input type="checkbox"/> Cittadini                      X <input type="checkbox"/> Contribuenti  <input type="checkbox"/> Dipendenti  <input type="checkbox"/> Collaboratori  <input type="checkbox"/> Altro                      [SPECIFICARE _____ ]</p> <p>Volume di Interessati:</p> <input type="checkbox"/> 0 – 1.000 <input type="checkbox"/> 1.000 – 10.000 X <input type="checkbox"/> 10.000 – 100.000 <input type="checkbox"/> 100.000 – 1M														
<b>3 – Tipologia e finalità del trattamento dei Dati Personali</b>														
<p>Il sub-responsabile del trattamento tratta i dati personali affidati dal responsabile ove ciò sia strettamente necessario per le finalità delle prestazioni identificate nel Contratto.</p> <p><b>Natura del trattamento dei Dati Personali</b></p> <table border="1"> <thead> <tr> <th>Modalità di Trattamento</th> <th>Server responsabile</th> <th>Server/Cloud sub-responsabile</th> </tr> </thead> <tbody> <tr> <td><b>Modifica</b> (il dato personale subisce una modifica)</td> <td>X</td> <td></td> </tr> <tr> <td><b>Cancellazione</b> (eliminazione di dati tramite l'utilizzo di strumenti elettronici)</td> <td>X</td> <td></td> </tr> <tr> <td><b>Conservazione</b> (mantenere memorizzate le informazioni su un qualsiasi supporto)</td> <td></td> <td>X</td> </tr> </tbody> </table>			Modalità di Trattamento	Server responsabile	Server/Cloud sub-responsabile	<b>Modifica</b> (il dato personale subisce una modifica)	X		<b>Cancellazione</b> (eliminazione di dati tramite l'utilizzo di strumenti elettronici)	X		<b>Conservazione</b> (mantenere memorizzate le informazioni su un qualsiasi supporto)		X
Modalità di Trattamento	Server responsabile	Server/Cloud sub-responsabile												
<b>Modifica</b> (il dato personale subisce una modifica)	X													
<b>Cancellazione</b> (eliminazione di dati tramite l'utilizzo di strumenti elettronici)	X													
<b>Conservazione</b> (mantenere memorizzate le informazioni su un qualsiasi supporto)		X												

<b>Consultazione</b> (semplice visualizzazione dei dati)		<b>X</b>
<b>Comunicazione</b> (il dato viene trasferito a terzi determinati)	<b>N.A.</b>	<b>N.A.</b>
<b>Diffusione</b> (dare conoscenza dei dati a soggetti indeterminati, ad es. pubblicazione online)	<b>N.A.</b>	<b>N.A.</b>
<b>Distruzione</b> (attività di eliminazione definitiva dei dati)	<b>N.A.</b>	<b>N.A.</b>
<b>Estrazione</b> (attività di estrapolazione di dati da gruppi già memorizzati)	<b>N.A.</b>	<b>X</b>
<b>Organizzazione</b> (consiste nella classificazione dei dati secondo un metodo prescelto)	<b>N.A.</b>	<b>X</b>
<b>Raccolta</b> (consiste nell'attività di acquisizione del dato)	<b>X</b>	<b>N.A.</b>
<b>Raffronto</b> (operazione di confronto tra dati)	<b>N.A.</b>	<b>N.A.</b>
<b>Strutturazione</b> (attività di distribuzione dei dati secondo schemi precisi)	<b>N.A.</b>	<b>N.A.</b>
<b>Uso</b> (attività generica che ricopre qualsiasi tipo di impiego dei dati)	<b>X</b>	<b>X</b>
<b>Registrazione</b> (memorizzazione dei dati su un qualsiasi supporto)	<b>X</b>	<b>X</b>

#### 4 – Categorie Dati Personali trattati

Ai fini dell'erogazione delle prestazioni previste dal Contratto, il sub-responsabile può trattare le seguenti categorie di Dati Personali:

**X**  **Dati anagrafici**

Nome e Cognome

Luogo e Data di nascita

Luogo e indirizzo di Residenza

**X**  **Dati identificativi**

Codice Fiscale

Partita Iva

Dati Catastali

Targa veicolo

Altro

[SPECIFICARE \_\_\_\_\_]

**X**  **Dati di contatto**

Indirizzo e-mail

Indirizzo PEC

Numero di telefono

**X**  **Dati Fiscali e Contabili**

Coordinate Bancarie

Metodo di pagamento



<input type="checkbox"/> Altro [SPECIFICARE _____ ]															
<input type="checkbox"/> <b>Dati di log, indirizzo IP</b> <input type="checkbox"/> Altro [SPECIFICARE _____ ]															
<b>5 – Categorie particolari di Dati Personali trattati (ove applicabile)</b>															
<input checked="" type="checkbox"/> <b>Reati e condanne penali ex art. 10 GDPR</b> <input checked="" type="checkbox"/> <b>Categorie particolari di dati personali ex art. 9 GDPR</b> [SPECIFICARE _____ ]															
<b>6 – Ubicazione/Conservazione dei Dati Personali</b>															
<input type="checkbox"/> Server locale del responsabile <input checked="" type="checkbox"/> Server locale del sub-responsabile del trattamento <input checked="" type="checkbox"/> Cloud															
<b>7 – Eliminazione dei Dati Personali al termine del periodo di conservazione</b>															
<input type="checkbox"/> Cancellazione <input type="checkbox"/> Restituzione <input type="checkbox"/> Processo di anonimizzazione (se richiesto) <input checked="" type="checkbox"/> Altro [CONSERVAZIONE PER 12 MESI DALL'ULTIMA RELEASE PER POI PROCEDERE CON LA CANCELLAZIONE DEL DATO]  Ove non diversamente specificato, il trattamento è effettuato nello Spazio Economico Europeo (SEE).															
<b>8 – Basi legali in caso di trasferimento dei Dati Personali al di fuori dello Spazio Economico Europeo</b>															
Nella tabella che segue sono riportate, per ciascuno dei Paesi interessati al di fuori dello Spazio Economico Europeo, le informazioni rilevanti															
<table border="1" style="width: 100%; border-collapse: collapse; text-align: center;"> <thead> <tr> <th style="padding: 5px;">Paese</th> <th style="padding: 5px;">Decisione di adeguatezza</th> <th style="padding: 5px;">Norme Vincolanti d'Impresa</th> <th style="padding: 5px;">Clausole contrattuali standard</th> <th style="padding: 5px;">Autorizzazione dell'Autorità preposta alla Protezione dei Dati Personali</th> </tr> </thead> <tbody> <tr> <td style="padding: 5px;">N.A.</td> <td style="padding: 5px;">N.A.</td> <td style="padding: 5px;">N.A.</td> <td style="padding: 5px;">N.A.</td> <td style="padding: 5px;">N.A.</td> </tr> <tr> <td style="padding: 5px;"> </td> <td style="padding: 5px;"> </td> <td style="padding: 5px;"> </td> <td style="padding: 5px;"> </td> <td style="padding: 5px;"> </td> </tr> </tbody> </table>	Paese	Decisione di adeguatezza	Norme Vincolanti d'Impresa	Clausole contrattuali standard	Autorizzazione dell'Autorità preposta alla Protezione dei Dati Personali	N.A.	N.A.	N.A.	N.A.	N.A.					
Paese	Decisione di adeguatezza	Norme Vincolanti d'Impresa	Clausole contrattuali standard	Autorizzazione dell'Autorità preposta alla Protezione dei Dati Personali											
N.A.	N.A.	N.A.	N.A.	N.A.											



## MISURE TECNICHE E ORGANIZZATIVE

Si riportano di seguito i principali requisiti di sicurezza delle informazioni e delle relative misure di sicurezza richieste dal Responsabile

Area tematica	Requisiti
<b>Password</b>	Il Responsabile del trattamento manterrà le policy per password sicure per tutti i sistemi che trattano i dati per conto del responsabile del trattamento.
<b>Antivirus</b>	Il sub-responsabile del trattamento manterrà un sistema antivirus e definizioni dei virus sempre aggiornati su tutti i sistemi che trattano i dati per conto del responsabile del trattamento.
<b>Hardening* della rete e del firewall</b>	<p>Il sub-responsabile del trattamento dei dati manterrà e implementerà gli standard di hardening della rete e del firewall per tutte le reti che trattano i dati per conto del responsabile del trattamento.</p> <p>Il sub-responsabile del trattamento fornirà questi standard di hardening al responsabile del trattamento, su richiesta.</p>
<b>Designazione delle Persone Autorizzate al Trattamento</b>	Il sub-responsabile del trattamento dei dati adotterà adeguate misure di sicurezza organizzativa volte ad individuare e designare le persone autorizzate a trattamento. Sarà cura del sub-responsabile fornire agli addetti idonee istruzioni sul corretto trattamento dei dati personali e sulle misure attuate.
<b>Consapevolezza della sicurezza delle informazioni</b>	Il sub-responsabile del trattamento dei dati manterrà un programma di formazione sulla consapevolezza della sicurezza delle informazioni a garanzia che tutti gli addetti che trattano i dati per conto del responsabile del trattamento siano a conoscenza delle loro responsabilità in materia di sicurezza delle informazioni.
<b>Backup</b>	<p>Il sub-responsabile del trattamento garantirà l'adozione di opportune policy di backup e predisporrà il relativo piano. In particolare, è richiesto il rispetto delle seguenti misure "minime":</p> <ul style="list-style-type: none"> <li>• Numero di backup giornalieri dei dati <b>non inferiore a due</b>;</li> <li>• Verificare l'esito della procedura di Backup almeno con una cadenza giornaliera. Se si utilizzano software specifici per la pianificazione ed esecuzione di backup prevedere, se possibile, l'invio di e-mail di notifica (sia in caso positivo che negativo) anche al Responsabile della sicurezza IT;</li> </ul>
<b>Sub-Responsabili</b>	Il sub-responsabile del trattamento che volesse affidarsi ad altri responsabili per l'esecuzione di attività di trattamento eseguite per conto del responsabile dovrà inoltrare formale richiesta di autorizzazione. La richiesta dovrà essere corredata da tutti gli elementi utili per una valutazione, anche in termini di garanzie adeguate e di misure adatte per la protezione delle informazioni trattate.

Si riportano di seguito le principali misure di sicurezza attuate dal sub-responsabile.

N.	AMBITI DI PROTEZIONE DEI DATI	LINEE GUIDA PER LE MISURE DA ADOTTARE	MISURE TECNICHE E ORGANIZZATIVE ADOTTATE AI FINI DELLA CONFORMITA' ALL'ART.32 GDPR
1	<b>Meccanismi di identificazione e autenticazione</b>	Sono identificati e resi noti meccanismi di identificazione e autenticazione e meccanismi per il controllo centralizzato degli accessi. Deve essere implementato un sistema di controllo degli accessi applicabile a tutti gli utenti che accedono al sistema IT. Il sistema deve consentire la creazione, l'approvazione, la revisione e l'eliminazione degli account utente.	<ul style="list-style-type: none"> <li>-Nome utenze e password alfanumerica personale</li> <li>-Segmentazione indirizzi IP (autorizzati ad accedere ai dati)</li> <li>-Raccolta LOG accessi ai dati</li> </ul>
2	<b>Utilizzo di utenze nominative sui sistemi</b>	Sono previste sui sistemi solo utenze nominative (evitando account generici o di gruppo) al fine di garantire la tracciabilità delle operazioni eseguite. L'uso di account comuni (con credenziali di accesso condivise tra più utenti) non deve essere consentito.	SI Vengono utilizzati account e password personali
3	<b>Gestione / assegnazione diritti utente</b>	I permessi specifici di controllo degli accessi devono essere assegnati a ciascun ruolo (coinvolto nel trattamento di dati personali) in base al principio della stretta pertinenza e necessità.	Gli account sono dotati di privilegi differenziati in base al ruolo assegnato per lettura\scrittura
4	<b>Log Management</b>	Sono previsti sistemi di gestione e memorizzazione centralizzata di eventi e log provenienti dai servizi di monitoring presenti nella rete sottoposta al controllo. Devono essere generati file di log per ogni sistema utilizzato per il trattamento dei dati personali. Essi devono: <ul style="list-style-type: none"> <li>-includere tutti i tipi di accesso ai dati (visualizzazione, modifica, cancellazione);</li> <li>-essere contrassegnati con data e ora;</li> <li>-essere adeguatamente protetti da manomissioni e accessi non autorizzati.</li> </ul>	Vengo registrati i LOG e conservati per tutta la durata del progetto
5	<b>Patch Management</b>	Sono verificate e applicate le patch di sicurezza necessarie per i sistemi e le applicazioni in uso.	Aggiornamento costante

N.	AMBITI DI PROTEZIONE DEI DATI	LINEE GUIDA PER LE MISURE DA ADOTTARE	MISURE TECNICHE E ORGANIZZATIVE ADOTTATE AI FINI DELLA CONFORMITA' ALL'ART.32 GDPR
6	<b>Identificazione dei ruoli e responsabilità in ambito data protection</b>	Sono definiti e resi noti ruoli e responsabilità inerenti al trattamento dei dati personali e alla protezione degli stessi per tutto il personale e per eventuali terze parti rilevanti (es. fornitori, clienti, partner).	Si
7	<b>Identificazione dei trattamenti di dati personali</b>	I trattamenti di dati personali sono identificati e catalogati all'interno del Registro dei Trattamenti.	Registro Trattamenti non obbligatorio
8	<b>Processi per l'informazione dell'interessato</b>	Sono definiti, implementati e documentati i processi riguardanti l'informazione dell'interessato in merito al trattamento dei dati.	N.A.
9	<b>Valutazione Privacy correlata alle Terze Parti</b>	Al momento dell'ingaggio del fornitore sono valutati gli aspetti Privacy.	N.A.
10	<b>Sistema di videosorveglianza e/o guardiania</b>	Le aree/edifici ove avvengono trattamenti di dati è protetto mediante il ricorso a presidi di vigilanza e/o tramite un sistema di videosorveglianza esterna e interna. Quella interna si attiva automaticamente solo dopo la chiusura della sede.	I locali sono dotati di videosorveglianza esterna
11	<b>Censimento e nomina degli Amministratori di Sistema</b>	Sono individuati gli A.d.S. secondo la definizione del provvedimento dell'Autorità Garante per la Protezione dei Dati Personali mediante designazione nominativa ed individuale. L'elenco inoltre è periodicamente aggiornato.	N.A.
12	<b>Monitoraggio sugli accessi degli Amministratori di Sistema</b>	Gli accessi degli A.d.S. agli archivi informatici sono registrati mediante log di sistema e conservati per un periodo di tempo di almeno 3 mesi. I log inoltre possiedono le caratteristiche minime richieste (username, host, IP, data e ora di login e logout).	N.A.
13	<b>Malware Protection</b>	Sono implementate misure di protezione da: <ul style="list-style-type: none"> <li>• infezioni da software malevoli;</li> <li>• azioni non autorizzate;</li> <li>• applicazioni sospette;</li> <li>• tentativi di sottrazione di dati personali.</li> </ul>	Aggiornamento costante



N.	AMBITI DI PROTEZIONE DEI DATI	LINEE GUIDA PER LE MISURE DA ADOTTARE	MISURE TECNICHE E ORGANIZZATIVE ADOTTATE AI FINI DELLA CONFORMITA' ALL'ART.32 GDPR
14	<b>Gestione delle Postazioni di Lavoro (PdL)</b>	Gli utenti non devono essere in grado di disattivare o bypassare le impostazioni di sicurezza e non devono avere i privilegi per installare o disattivare applicazioni software non autorizzate. Il sistema, inoltre, deve attivare un timeout di sessione quando l'utente non è in stato attivo per un certo periodo di tempo. Gli aggiornamenti critici di sicurezza rilasciati dallo sviluppatore del sistema operativo devono essere installati regolarmente.	N.A.
15	<b>Gestione degli ambienti fisici</b>	Sono rispettate le policy ed i regolamenti relativi agli ambienti fisici in cui operano le risorse dell'organizzazione. Il perimetro fisico dell'infrastruttura del sistema IT non deve essere accessibile da personale non autorizzato. L'identificazione chiara tramite mezzi appropriati (ad es. badge identificativi) per tutto il personale e i visitatori che accedono ai locali dell'organizzazione, deve essere stabilita a seconda dei casi.	N.A.
16	<b>Gestione dell'accesso remoto alle risorse</b>	L'accesso remoto alle risorse è gestito mediante l'utilizzo di metodi di connessione sicura da remoto (es. VPN C2S/S2S).	SI
17	<b>Certificazioni</b>	Eventuali certificazioni (es. ISO) possedute e in corso di validità.	NO