Azienda USL Umbria 2
aslumbria2@postacert.umbria.it
Servizio Informatico e Telecomunicazioni

Oggetto: Modulo richiesta credenziali SIVA

Il sottoscritto effettua le presenti dichiarazioni sostitutive e le dichiarazioni sostitutive di notorietà ai sensi rispettivamente degli artt. 46 e 47 del DPR 445/00, essendo a conoscenza che chiunque rilascia dichiarazioni mendaci, forma atti falsi o ne fa uso nei casi previsti dal presente testo unico, e' punito ai sensi del codice penale e delle leggi speciali in materia come previsto dall'art.76 del D.P.R. 445/00

Dati del legale rappresentante della struttura richiedente:			
Cognome:		Nome:	
Codice Fiscale:		Telef.:	
Email:			

in qualità di legale rappresentate della struttura:

Dati della struttura richiedente:	
Denominazione:	
C.F./P.IVA:	
Indirizzo:	

in riferimento all'utente, sotto identificato, di cui, sotto la propria responsabilità, ha accertato l'idoneità ed affidabilità:

Dati dell'utente:			
Cognome		Nome	
Codice Fiscale		Telef.	
Email			
Figura Profes.le			
N.B.: le credenziali saranno inviate all'indirizzo email indicato per l'utente			

esprime la seguente richiesta:

Tipologia richiesta	**Scadenza dell'abilitazione (gg/mm/aaaa)**

Con riferimento alla superiore richiesta, il sottoscritto dichiara:

- *di aver preso visione ed accettare le istruzioni per l'uso delle credenziali di autenticazioni, obbligandosi per la struttura e l'assegnatario.*
- *di aver individuato l'assegnatario tra persone che offrono adeguate garanzie per l'esecuzione dei compiti affidati ed il rispetto della vigente normativa in materia di protezione dei dati personali.*
- *di aver preso visione ed accettare le istruzioni e gli obblighi ricevuti quale responsabile del trattamento dei dati personali.*
- *di aver informato, autorizzato, formato ed istruito adeguatamente l'assegnatario delle credenziali, obbligandosi a controllarne il corretto uso.*
- ***che procederà con tempestività a segnalare ogni variazione inerente alla necessità d'uso delle suddette credenziali, come pure la richiesta di disattivazione nel caso in cui cessino le condizioni d'uso**.*
- *di obbligarsi a comunicare tempestivamente all'Azienda ogni incidente o sospetta compromissione delle credenziali di autenticazione.*

Luogo, _____ *Data* _____

Il Legale Rappresentante (firmato digitalmente)

_____

USLUmbria2

Allegato 1 - **ISTRUZIONI PER LA COMPILAZIONE DELLA RICHIESTA**

1. *Il modulo **DEVE ESSERE COMPILATO ELETTRONICAMENTE***
2. *Il modulo di richiesta **NON DEVE ESSERE STAMPATO E COMPILATO A MANO***
3. *Il modulo **DEVE ESSERE FIRMATO DIGITALMENTE (in formato p7m o pdf)***
4. *Il modulo **DEVE ESSERE INVIATO ESCLUSIVAMENTE** mediante Posta Elettronica Certificata (**PEC**) all'indirizzo: aslumbria2@postacert.umbria.it .*
5. ***Moduli non compilati elettronicamente (scritti a mano e scansionati) e/o non firmati digitalmente non saranno presi in considerazione e cestinati senza fornire alcuna risposta.***
6. *La mail deve avere come oggetto "Gestione Credenziali – <nome ditta>".*
7. Per ogni richiesta di abilitazione utente deve essere predisposto e trasmesso un allegato (un allegato per ogni utente).

Allegato 2- **INFORMAZIONI INTEGRATIVE SUL TRATTAMENTO DEI DATI DEI FORNITORI/PARTNERS AI SENSI DELL'ART. 13 REG. UE 679/2016**

Gentile Fornitore/Partner,
ad integrazione della informativa sul "*trattamento dei dati dei fornitori/partners ai sensi dell'art. 13 reg. UE 679/2016"* già somministratale e comunque reperibile nella sua forma più aggiornata sul sito web aziendale all'indirizzo https://www.uslumbria2.it/pagine/privacy-000 , ai sensi dell'art. 13 par. 4 del GDPR, le forniamo le informazioni integrative che seguono.

1. **Finalità e basi giuridiche del trattamento.**

Saranno trattati i dati personali di coloro i quali prestando opera a suo favore, hanno necessità di accedere al nostro sistema informativo per le attività istituzionali previste dal Progetto Atlante e le successive modifiche che avverranno durante il periodo di validità dell'abilitazione.
La base giuridica è quella dell'art. 6 par. 1 lett. b) ovvero il trattamento è necessario all'esecuzione della convenzione del "SIVA" di cui lei è parte, e, per quanto riguarda i trattamenti connessi all'esecuzione di misure di sicurezza per la protezione dei dati personali (LOG), ovvero per attività di vigilanza del sistema informativo, l'art. 6 par. 1 lett. c) ovvero adempimento degli obblighi di legge di cui all'art. 32 GDPR.

2. **Modalità e categorie di dati trattati.**

I dati personali degli assegnatari sono trattati dagli autorizzati, dai designati, dagli amministratori di sistema, dai responsabili del trattamento che svolgono servizi IT. Maggiori informazioni possono essere richieste al titolare. Sono trattati i dati identificativi ed i dati associati ai *log* di collegamento.

3. **Periodo di conservazione dei dati personali e criteri utilizzati**

I dati personali oggetto di trattamento sono conservati per la durata della convenzione e per le finalità di archiviazione richieste dalla normativa amministrativa.

Allegato 3 - **ISTRUZIONI PER GLI ASSEGNATARI DELLE CREDENZIALI DI AUTENTICAZIONE**

In osservanza della vigente normativa, ed in considerazione del trattamento dei dati personali ai quali, nello svolgimento delle proprie mansioni, ciascuno è autorizzato e dovrà attenersi scrupolosamente al rispetto della normativa osservando le norme regolamentari qui di seguito riportate e le altre ulteriori che potranno essere eventualmente impartite. In caso di dubbio, l'assegnatario deve astenersi dal procedere al trattamento e chiedere istruzioni al suo responsabile gerarchico. Il mancato rispetto delle istruzioni ricevute costituisce inadempimento.

1. Norme generali

1.1. Negli ambiti e negli archivi per i quali l'assegnatario è autorizzato, questi è tenuto a trattare i soli dati strettamente necessari all'espletamento degli incarichi ricevuti.

1.2. L'assegnatario è tenuto a custodire i dati personali oggetto di trattamento in maniera tale da ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato da parte di terzi o di trattamento non consentito o non conforme alle finalità della raccolta.

1.3. L'assegnatario è tenuto a rispettare le misure di sicurezza a protezione dei dati personali che gli sono comunicate. In ogni caso, qualora non vi fossero specifiche misure di sicurezza, l'assegnatario deve proteggere i dati personali con la diligenza del buon padre di famiglia.

1.4. L'assegnatario deve dare immediatamente notizia al suo superiore gerarchico se avesse conoscenza o il sospetto di un incidente delle informazioni. Per incidente si intende ogni evento avverso che interessi dati personali.

1.5. Qualora l'assegnatario ricevesse da parte di un interessato una richiesta di esercizio dei diritti, di competenza della Azienda USL Umbria n.2, dovrà immediatamente consegnarla al suo superiore gerarchico, al fine di consentirne la tempestiva trasmissione a codesta Azienda.

2. Misure per l'uso corretto delle credenziali di autenticazione

2.1. La password assegnata è provvisoria per il primo collegamento, pertanto l'assegnatario ha l'obbligo di sostituirla con una password di propria scelta da mantenere segreta che deve rispondere ai seguenti requisiti:

- deve essere abbastanza lunga (almeno 8 caratteri)
- deve contenere caratteri di almeno 3 diverse tipologie, da scegliere tra le 4 seguenti: lettere maiuscole, lettere minuscole, numeri, caratteri speciali (punti, trattino, underscore, ecc.)
- non deve contenere riferimenti personali facili da indovinare (nome, cognome, data di nascita, ecc.)
- deve essere periodicamente cambiata, almeno ogni 90 giorni
- non deve essere memorizzata su alcun tipo di supporto, quali, ad esempio, Post-it (sul monitor o sotto la tastiera) o agende (cartacee, posta elettronica, telefono cellulare) né su biglietti conservati nel portafoglio o indosso, oppure in file non protetti su pc, smartphone o tablet
- non deve essere condivisa via e-mail, sms, social network, instant messaging, ecc.. (anche se comunicata a persone conosciute, le credenziali potrebbero essere diffuse involontariamente a terzi o «rubate» da pirati informatici)
- deve essere digitata in modo riservato non in presenza di altri soggetti che possano vedere la tastiera, anche se collaboratori o dipendenti dell'Azienda
- deve essere evitata, soprattutto se si usano pc, smartphone e altri device che non sono direttamente assegnati, la possibilità che le password utilizzate sia conservata in memoria da tali supporti.

2.2. Attenzione: in caso di smarrimento o sospetta compromissione della password, l'assegnatario deve darne immediata comunicazione al proprio responsabile; ogni attività, infatti, compiuta con l'utilizzo delle credenziali di accreditamento si presume nella responsabilità dell'assegnatario, salvo che questi fornisca prova contraria.

2.3. Per alcun motivo dovrà comunicare la password ad altri e, nel caso in cui qualcuno ne faccia richiesta deve avvisare immediatamente il proprio responsabile.

2.4. L'assegnatario è informiamo altresì che il sistema informativo aziendale è controllato nel rispetto della vigente normativa al fine di garantirne il corretto funzionamento e la protezione dei dati in esso contenuti; pertanto le sono fornite le informazioni di cui art. 13 del Regolamento EU 679/2016 GDPR come disponibili sul sito web aziendale https://www.uslumbria2.it/pagine/privacy-000 .

2.5. L'assegnatario dovrà custodire i dati personali durante il periodo di trattamento.