Richiesta di Accesso Sicuro Autorizzato (VPN) al Sistema Informativo Aziendale

**S**

**I**

**N**

**C**

**L**

**I**

**T**

**A**

**I**

**M**

**P**

**E**

**R**

**I**

**A**

**L**

**I**

**S**

**F**

**O**

**G**

**I**

**A**

**R**

**E**

**G**

**A**

**L**

**I**

**S**

**S**

**E**

**D**

**E**

(per Soggetti esterni)

**□ Nuovo accesso □ Rinnovo accesso**

Il Richiedente, dopo aver letto le istruzioni riportate a pag. 9, compilato correttamente ed in ogni sua parte la Sezione 1 e sottoscritto il documento, dovrà scansionarlo in formato pdf ed inviarlo via PEC all’indirizzo **servizioict.asl.foggia@pec.rupar.puglia.it** e al seguente indirizzo email **tommaso.petrosillo@aslfg.it.**

Alla richiesta dovrà essere allegata copia di un documento d’identità in corso di validità del richiedente unitamente della nomina a Responsabile del Trattamento.

**Sezione 1: da compilare a carico del Richiedente l’accesso VPN**

# Dati Richiedente (1)

□ Professionista: ……………………………………………………………………………………………

Delibera approvazione atti n. ………………. del ………………. durata contratto: …………………….

a decorrere dal: ……………………………………………………………………………………………….

cellulre: …………………………. PEC: ……………………………………………………………………..

□ Società: …………………………………………………………………………………………………….

con contratto CIG n. …………………………………………………………………………………………..

□ Società mandataria R.T.I. : ………………………………………………………………………………

□ Ente in Convenzione: …………………………………………………………………………………….

nella persona del: (*Ruolo*) ……………………………………………………………………………….

Nome e Cognome: ……………………………………………………………………………………….

con sede legale in: ……………………………………………………………………………..(……..).. Via/P.zza: ……………………………………………………………………………………..n. ………..

Riferimento telefonico: …………………………………………………………………………………...

P.E.C.: ……………………………………………………………………………………………………..

Motivo della richiesta (2)

**S**

**I**

**N**

**C**

**L**

**I**

**T**

**A**

**I**

**M**

**P**

**E**

**R**

**I**

**A**

**L**

**I**

**S**

**F**

**O**

**G**

**I**

**A**

**R**

**E**

**G**

**A**

**L**

**I**

**S**

**S**

**E**

**D**

**E**

**…………………………………………………………………………………………………………………**

**…………………………………………………………………………………………………………………**

**…………………………………………………………………………………………………………………**

**…………………………………………………………………………………………………………………**

**…………………………………………………………………………………………………………………**

# Localizzazione Server (App/DB):

**S**

**I**

**N**

**C**

**L**

**I**

**T**

**A**

**I**

**M**

**P**

**E**

**R**

**I**

**A**

**L**

**I**

**S**

**F**

**O**

**G**

**I**

**A**

**R**

**E**

**G**

**A**

**L**

**I**

**S**

**S**

**E**

**D**

**E**

□ presso datacenter interno aziendale

□ presso infrastruttura Cloud Telecom

□ altro: ………………………………………………………………………………………………………

***oppure:***

□ Manutenzione applicativi (*indicare l’/le applicazione/i e l’ubicazione delle postazioni sulle quali è/sono installata/e*):

…………………………………………………………………………………………………………………

…………………………………………………………………………………………………………………

…………………………………………………………………………………………………………………

…………………………………………………………………………………………………………………

…………………………………………………………………………………………………………………

□ Manutenzione sistemistica (*indicare il/i sistema/i e l’/la loro ubicazione*):

…………………………………………………………………………………………………………………

…………………………………………………………………………………………………………………

…………………………………………………………………………………………………………………

* Manutenzione tecnica/tecnologica (*indicare l’/gli elettromedicali e/o l’/gli impianto/i e l’/la loro ubicazione*):

…………………………………………………………………………………………………………………

…………………………………………………………………………………………………………………

…………………………………………………………………………………………………………………

…………………………………………………………………………………………………………………

**Periodo di attribuzione**:

□ **Annuale,** dal ………………………………. al …………………………………............

# □ Fino a scadenza del Contratto/Convenzione prevista in data: …………..……..

Se le attività oggetto della richiesta prevedono il trattamento di dati personali, indicare la tipologia di dati:

**S**

**I**

**N**

**C**

**L**

**I**

**T**

**A**

**I**

**M**

**P**

**E**

**R**

**I**

**A**

**L**

**I**

**S**

**F**

**O**

**G**

**I**

**A**

**R**

**E**

**G**

**A**

**L**

**I**

**S**

**S**

**E**

**D**

**E**

□ **dati che permettono l’identificazione diretta** [(*come i dati anagrafici, le immagini, ecc.*)]:

………………………………………………………………………………………………………..

………………………………………………………………………………………………………..

………………………………………………………………………………………………………..

□ **dati che permettono l’identificazione indiretta** [(*come un numero di identificazione (ad es.: il codice fiscale, l’indirizzo IP, il numero di targa, ecc.*)]:

………………………………………………………………………………………………………..

………………………………………………………………………………………………………..

………………………………………………………………………………………………………..

□ **dati appartenenti a categorie particolari** [*cioè quelli che rivelano l'origine razziale od etnica, le convinzioni religiose, filosofiche, le opinioni politiche, l'appartenenza sindacale, relativi alla salute o alla vita sessuale. Il Regolamento (UE) 2016/679 (art. 9) ha incluso nella nozione anche i dati genetici, i dati biometrici e quelli relativi all'orientamento sessuale*]

………………………………………………………………………………………………………..

………………………………………………………………………………………………………..

………………………………………………………………………………………………………..

□ **dati giudiziari** [*cioè quelli che possono rivelare l'esistenza di determinati provvedimenti giudiziari soggetti ad iscrizione nel casellario giudiziale (ad es.: i provvedimenti penali di condanna definitivi, la liberazione condizionale, il divieto od obbligo di soggiorno, le misure alternative alla detenzione, ecc.) o la qualità di imputato o di indagato. Il Regolamento (UE) 2016/679 (art. 10) ricomprende in tale nozione i dati relativi alle condanne penali e ai reati o a connesse misure di sicurezza*]:

………………………………………………………………………………………………………..

………………………………………………………………………………………………………..

………………………………………………………………………………………………………..

□ **dati che consentono la geolocalizzazione** [*cioè quelli che forniscono informazioni sui luoghi frequentati, sugli spostamenti, ecc.*]:

………………………………………………………………………………………………………..

………………………………………………………………………………………………………..

# Condizioni di attribuzione (3)

**S**

**I**

**N**

**C**

**L**

**I**

**T**

**A**

**I**

**M**

**P**

**E**

**R**

**I**

**A**

**L**

**I**

**S**

**F**

**O**

**G**

**I**

**A**

**R**

**E**

**G**

**A**

**L**

**I**

**S**

**S**

**E**

**D**

**E**

Tipo di VPN:

* **VPN IPSec** *(richiede l’uso di un client proprietario***)**
* **SSL VPN** *(utilizzabile attraverso qualsiasi browser***)**
* **LAN to LAN** *(motivare di seguito la necessità***)**

…………………………………………………………………………………………

…………………………………………………………………………………………

…………………………………………………………………………………………

…………………………………………………………………………………………

**Parametri della VPN (4)**

**S**

**I**

**N**

**C**

**L**

**I**

**T**

**A**

**I**

**M**

**P**

**E**

**R**

**I**

**A**

**L**

**I**

**S**

**F**

**O**

**G**

**I**

**A**

**R**

**E**

**G**

**A**

**L**

**I**

**S**

**S**

**E**

**D**

**E**

1. **VPN IPSec / SSL VPN:**
   * Indirizzo IP, porte (e protocollo) delle postazioni da raggiungere tramite VPN:

1. IP: . . . Porte: ………………………………………

2. IP: . . . Porte: ………………………………………

3. IP: . . . Porte: ………………………………………

4. IP: . . . Porte: ………………………………………

5. IP: . . . Porte: ………………………………………

6. IP: . . . Porte: ………………………………………

* + La presente richiesta si intende per i seguenti dipendenti della/dell’ Società/Ente su indicata:

1. Nome: …………………………………… Cognome: ………………………………….

Ruolo: …………………………………………………………………………………….

PEC personale/Email: ………………………………………………………………….

2. Nome: …………………………………… Cognome: ………………………………….

Ruolo: …………………………………………………………………………………….

PEC personale/Email: ………………………………………………………………….

3. Nome: …………………………………… Cognome: ………………………………….

Ruolo: …………………………………………………………………………………….

PEC personale/Email: ………………………………………………………………….

4. Nome: …………………………………… Cognome: ………………………………….

Ruolo: …………………………………………………………………………………….

PEC personale/Email: ………………………………………………………………….

5. Nome: …………………………………… Cognome: ………………………………….

Ruolo: …………………………………………………………………………………….

PEC personale/Email: ………………………………………………………………….

6. Nome: …………………………………… Cognome: ………………………………….

Ruolo: …………………………………………………………………………………….

PEC personale/Email: ………………………………………………………………….

7. Nome: …………………………………… Cognome: ………………………………….

Ruolo: …………………………………………………………………………………….

PEC personale/Email: ………………………………………………………………….

8. Nome: …………………………………… Cognome: ………………………………….

Ruolo: …………………………………………………………………………………….

PEC personale/Email: ………………………………………………………………….

9. Nome: …………………………………… Cognome: ………………………………….

Ruolo: …………………………………………………………………………………….

PEC personale/Email: ………………………………………………………………….

10. Nome: …………………………………… Cognome: ………………………………….

Ruolo: …………………………………………………………………………………….

PEC personale/Email: ………………………………………………………………….

Il sottoscritto dichiara di aver istruito i suindicati dipendenti al rispetto delle norme di sicurezza aziendali e di quelle impartite dal Titolare; in particolare ha ammonito gli stessi a custodire le proprie credenziali, inviate agli indirizzi PEC/email forniti, e a non consentire l'uso delle stesse a terzi anche se appartenenti alla stessa azienda.

# LAN to LAN:

**S**

**I**

**N**

**C**

**L**

**I**

**T**

**A**

**I**

**M**

**P**

**E**

**R**

**I**

**A**

**L**

**I**

**S**

**F**

**O**

**G**

**I**

**A**

**R**

**E**

**G**

**A**

**L**

**I**

**S**

**S**

**E**

**D**

**E**

* + Brand e modello del remote peer:
  + Indirizzo IP del remote peer:

IP: . . . Porte: ……………………………………

* + Authentication Method: □ Pre-shared Key □ Digital Certificate
  + VPN Settings:
  + IKE: □ Version 1 □ Version 2
  + Mode: □ Main □ Aggressive
  + Options: □ Mode Config □ Manually Set □ DHCP over IPSEC
  + Phase 1:

Encryption Algorithm: □ DES □ 3DES □ AES-128 □ AES-192 □ AES-256 Hash Algorithm: □ MD5 □ SHA1 □ SHA256 □ SHA384 □ SHA512 DH Group: □ 1 □ 2 □ 5 □ 14 □ 15 □ 16 □ 17 □ 18 □ 19 □ 20

Key Life:

NAT Traversal: □ Auto □ Force

Dead Peer Detection: □ abilitato □ non abilitato Dead Peer Detection (secondi): 10

Dead Peer Detection (tentativi): 5

* + Phase 2:

**S**

**I**

**N**

**C**

**L**

**I**

**T**

**A**

**I**

**M**

**P**

**E**

**R**

**I**

**A**

**L**

**I**

**S**

**F**

**O**

**G**

**I**

**A**

**R**

**E**

**G**

**A**

**L**

**I**

**S**

**S**

**E**

**D**

**E**

Mode Tunnel IPv4

Protocol: □ ESP □ AH

Encryption Transform: □ DES □ 3DES □ AES-128 □ AES-192 □AES-256 Authentication Transform: □ MD5 □ SHA1 □ SHA256 □ SHA384 □ SHA512 DH Group: □ 1 □ 2 □ 5 □ 14 □ 15 □ 16 □ 17 □ 18 □ 19 □ 20

Key Life: 86400 seccondi

Perfect Forward Secrecy (PFS): □ abilitato □ non abilitato

o Indirizzo IP delle reti remote a cui appartengono le postazioni da cui sarà avviata la VPN:

1. Network: . . . Subnet: . . .
2. Network: . . . Subnet: . . .
3. Network: . . . Subnet: . . .
4. Network: . . . Subnet: . . .
5. Network: . . . Subnet: . . .
6. Network: . . . Subnet: . . .

# Assunzione di Responsabilità (5)

**S**

**I**

**N**

**C**

**L**

**I**

**T**

**A**

**I**

**M**

**P**

**E**

**R**

**I**

**A**

**L**

**I**

**S**

**F**

**O**

**G**

**I**

**A**

**R**

**E**

**G**

**A**

**L**

**I**

**S**

**S**

**E**

**D**

**E**

Il Richiedente, identificato dai dati di cui al punto (1), avendo fatto richiesta di connessione VPN, alle condizioni di cui al punto (3), dichiara sotto la propria responsabilità:

* + di essere a conoscenza della natura della connessione e di assumersi le responsabilità che derivano dall'utilizzo della connessione in oggetto;
  + di non utilizzare quanto richiesto, per scopi diversi da quelli dichiarati o per interessi di qualsiasi natura riconducibili o meno al campo di attività della propria azienda e a non cedere per alcun motivo il servizio a terzi;
  + di essere a conoscenza di essere connesso con un indirizzo IP dell’ASL di Foggia e quindi di operare secondo le policy del Titolare;
  + di essere a conoscenza che la rete Aziendale sono parte della rete CN RUPAR-SPC Puglia e, quindi, di impegnarsi a rispettare quanto sancito dalle regole del CN RUPAR-SPC Puglia nonché da eventuali regolamenti Aziendali anche pubblicati durante il corso di validità della presente autorizzazione;
  + di essere a conoscenza che, nel caso che la connessione venga richiesta per attività che implichino il trattamento di dati personali, gli stessi non potranno essere prelevati dal sistema informativo aziendale (server, postazioni di lavoro, NAS dipartimentali/aziendali, ecc.) e memorizzati sulla postazione da cui ha origine la VPN senza esplicito consenso scritto del Titolare degli stessi nella persona del Direttore Generale dell’ASL di Foggia;
  + di essere a conoscenza che, nel caso che la connessione venga richiesta per attività che implichino il trattamento di dati personali per scopi statistici e scientifici e/o di tutela della salute, vale quanto detto al punto precedente. Il Richiedente dichiara altresì di essere consapevole che, nel caso specifico di richiesta della connessione per le succitate attività, la presente assunzione di responsabilità implica l’accettazione delle “Regole Deontologiche per trattamenti a fini statistici o di ricerca scientifica” allegate dal Garante al provvedimento n.

515 del 19 dicembre 2018 ([https://www.garanteprivacy.it/web/guest/home/docweb/-](https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9069637#1)

[/docweb-display/docweb/9069637#1](https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9069637#1));

* + di essere a conoscenza che il servizio è monitorato 24/7 e che i dati di accesso e di traffico verranno trattati secondo le finalità ed i mezzi riportati nell’Informativa allegata;
  + di essere a conoscenza che la mancata osservanza di una o più di tali regole provocherà l’immediata interruzione del servizio, fatte salve le ulteriori conseguenze di natura penale, civile, amministrativa relative alla violazione compiuta;
  + di aver preso visione del Regolamento aziendale per l'utilizzo e la gestione delle risorse strumentali informatiche e telematiche aziendali reso disponibile sul sito internet istituzionale nell'apposita sezione "Regolamenti aziendali";
  + di impegnarsi a conservare la password personale assegnata e a non comunicarla a terzi;
  + di impegnarsi a non consentire a terzi, a nessun titolo, l'utilizzo del servizio di accesso VPN concesso;
  + di osservare e fare osservare ai propri dipendenti, incaricati e collaboratori, l'obbligo alla riservatezza nei confronti di chiunque, per quanto riguarda fatti, informazioni, dati e atti di cui vengano a conoscenza nell'espletamento del servizio in modalità VPN. In particolare, si impegna a non cedere, non consegnare, non copiare, non riprodurre, non comunicare, non divulgare, non rendere disponibili in qualsiasi modo o a qualsiasi titolo a terzi, le informazioni acquisite nell'esecuzione del servizio in modalità VPN;
  + a comunicare tempestivamente per iscritto, al Responsabile dei Sistemi informativi e TLC dell’ASL di Foggia, eventuali avvicendamenti di personale, sia ai fini dell’aggiornamento degli stessi in ordine alla compilazione dei necessari aggiornati elenchi interni, sia al fine di provvedere alla variazione dei profili di autenticazione distinti per i diversi operatori;
  + a comunicare tempestivamente al Responsabile della S.S. Sistemi informativi e TLC dell’ASL di Foggia e al Responsabile della protezione dei dati eventuali incidenti che possano comportare la violazione di dati personali di cui è Titolare l’ASL di Foggia (data-breach).

Data **Firma del Richiedente**

**Sezione 2 : Autorizzazione da compilare a cura del Titolare**

**(ASL FOGGIA)**

# Il Delegato interno al trattamento dei dati (Direttore/Responsabile interno competente)

**S**

**I**

**N**

**C**

**L**

**I**

**T**

**A**

**I**

**M**

**P**

**E**

**R**

**I**

**A**

**L**

**I**

**S**

**F**

**O**

**G**

**I**

**A**

**R**

**E**

**G**

**A**

**L**

**I**

**S**

**S**

**E**

**D**

**E**

# …………………………………………………………… in relazione alla richiesta in oggetto

* **AUTORIZZA**
* **NON AUTORIZZA**

# Il Responsabile della S.S. Sistemi informativi e TLC dell’ASL di Foggia, in relazione alla richiesta di cui sopra, esprime il seguente parere tecnico:

**S**

**I**

**N**

**C**

**L**

**I**

**T**

**A**

**I**

**M**

**P**

**E**

**R**

**I**

**A**

**L**

**I**

**S**

**F**

**O**

**G**

**I**

**A**

**R**

**E**

**G**

**A**

**L**

**I**

**S**

**S**

**E**

**D**

**E**

* **FAVOREVOLE**
* **NON FAVOREVOLE,** per i seguenti motivi …………………………………………………………

…………………………………………………………………………………………………………………

…………………………………………………………………………………………………………………

…………………………………………………………………………………………………………………

…………………………………………………………………………………………………………………

…………………………………………………………………………………………………………………

Data

Responsabile S.S. Sistemi informativi e TLC

**Sezione 3 : istruzioni per la compilazione**

Il presente modulo è stato prodotto in formato “PDF compilabile elettronicamente”. Qualsiasi modifica, alterazione, cancellazione, ecc. apportata al documento e non preventivamente approvata dallo scrivente ufficio, invalida il modulo di richiesta.

**S**

**I**

**N**

**C**

**L**

**I**

**T**

**A**

**I**

**M**

**P**

**E**

**R**

**I**

**A**

**L**

**I**

**S**

**F**

**O**

**G**

**I**

**A**

**R**

**E**

**G**

**A**

**L**

**I**

**S**

**S**

**E**

**D**

**E**

Il richiedente, dopo aver riempito i campi opportuni, dovrà stamparlo, firmarlo e scannerizzarlo per inviarlo via PEC agli indirizzi in epigrafe.

Di seguito alcune istruzioni per una corretta compilazione derivanti dalle domande frequenti che sono pervenute allo scrivente ufficio.

* Pag.1
  + Il numero CIG (Codice Identificativo Gara) è un codice alfanumerico di 10 caratteri adottato per identificare un contratto pubblico stipulato in seguito ad una gara d'appalto o affidato con una delle altre modalità consentite dal codice dei contratti pubblici. E’ presente sulla copia del contratto in vostro possesso.
  + Nel caso di Società / Società mandataria R.T.I. / Ente in convenzione, va compilata anche la parte "nella persona del...con sede legale in...". La figura del richiedente deve coincidere con quella del Responsabile del Trattamento Dati - RdT o, in base all’organizzazione interna della società, di un responsabile apicale suo diretto collaboratore (General Manager della filiale, Direttore Tecnico della sede, ecc.). L’indirizzo PEC deve essere quello del richiedente. Allo stesso indirizzo verranno inviate tutte le comunicazioni ufficiali inerenti al servizio.
* Pag. 2
  + Specificare il motivo della richiesta solo ove diverso da quelli sottoelencati. Per ciascuna delle voci di interesse in elenco, invece, indicare, oltre al nome dell'applicazione/il sistema/l’elettromedicale, una breve descrizione sulla sua tipologia oltreché l'edificio ed il dipartimento/reparto presso cui è installata (se su macchine di vostra proprietà o di proprietà dell'ente, ecc.). In generale, più informazioni vengono fornite, più risulterà rapida l’erogazione del servizio.
* Pag. 3
  + Indicare il tipo di dati trattati per ciascuna varietà ed inserire una breve descrizione sulla motivazione/necessità per cui vengono trattati.
* Pag. 4
  + La scadenza del contratto è riportata sul contratto stesso.
* Pag. 5
  + Insieme alle porte è necessario indicare anche il protocollo utilizzato (Telnet, SSH, RDP, ecc.).
  + In caso di istanza a favore di più dipendenti, specificare, in un allegato a parte da includere alla presente richiesta, quale/i dipendente/i si collegherà/collegheranno verso quale/i postazione/i e con quale/i protocollo/i, avendo cura di ridurre al minimo le ridondanze al fine di garantire una corretta gestione degli accessi.
* Pag. 6
  + Da compilare solo nel caso si necessiti di una Lan-to-Lan.
* Pag. 8
  + Datare e firmare l’assunzione di responsabilità.