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

(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 sistemainformativo.aou@pec.it e, per conoscenza, al seguente indirizzo: csi@pec.unina.it.

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

Sezione 1: da compilare a carico del soggetto esterno richiedente

(1) Dati Richiedente

☐ Professionista: ……

Delibera approvazione atti n. ..... del ..... Durata contratto: .....

a decorrere dal ……

cellulare:…… PEC: .....

☐ Società: ……

☐ Società mandataria R.T.I.:……

contratto CIG n. ……

☐ Ente in Convenzione: :……

nella persona del: *(Ruolo)*……

Dott.: ……

con sede legale in:……(……)

Via: ……..…n.……

Riferimento telefonico: ……

PEC: ..……

(All'indirizzo indicato verranno inviate tutte le comunicazioni ufficiali inerenti il servizio)

(2) Motivo della richiesta

……

……

……

……

……

oppure:

☐ Manutenzione applicativa (*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 elettromedicale/i e/o l'/gli impianto/i e l'/la loro ubicazione*):

……

……

……

……

……

☐ Telelavoro

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

☐ **dati che permettono l'identificazione diretta** *[come i dati anagrafici (ad es.: nome e cognome), 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 sensibili** *[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 relativi alle comunicazioni elettroniche** (via Internet o telefono) *[e-mail, pec, numeri di cellulare o di rete fissa, ecc.]*;

……...

……...

……...

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

……...

……...

……...

(3) Condizioni di attribuzione

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)*

……...

……...

……...

……...

Periodo di attribuzione:

- ☐ ***Annuale***, dal …… al ……
- ☐ ***Fino a scadenza del Contratto/Convenzione*** *prevista in data: ……*

(4) Parametri della VPN

a. 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: ……

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.

b. LAN to LAN:

- Brand e modello del remote peer:
- Indirizzo IP del remote peer:

- Authentication Method: ◯ Pre-shared Key *(comunicata per telefono)* ◯ Digital Certificates
- 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:

- Phase 2:

  Encryption Transform: ◯ DES ◯ 3DES ◯ AES-128 ◯ AES-192 ◯ AES-256

  Authentication Transform: ◯ MD5 ◯ SHA1 ◯ SHA256 ◯ SHA384 ◯ SHA512

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

  DH Group: ◯ 1 ◯ 2 ◯ 5 ◯ 14 ◯ 15 ◯ 16 ◯ 17 ◯ 18 ◯ 19 ◯ 20

  Key Life:

- Flussi di servizio:

1. Src: Dst: Port:
2. Src: Dst: Port:
3. Src: Dst: Port:
4. Src: Dst: Port:
5. Src: Dst: Port:
6. Src: Dst: Port:
7. Src: Dst: Port:

(5) Assunzione di Responsabilità

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'Università degli Studi di Napoli "Federico II" e quindi di operare secondo le policy dell'Ateneo;
- di essere a conoscenza che la rete Aziendale, unitamente a quella di Ateneo, sono parte della rete GARR e, quindi, di impegnarsi a rispettare quanto sancito dalle Regole di utilizzo della rete GARR nonché da eventuali regolamenti Aziendali o di Ateneo 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 figura del Direttore Generale dell'A.O.U. "Federico II";
- 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/-/docweb-display/docweb/9069637#1);
- di essere a conoscenza che i suoi dati verranno inseriti in liste formate, detenute ed utilizzate dal C.S.I. - Università degli studi di Napoli "Federico II" e dall'A.O.U. "Federico II" per finalità istituzionali o comunque collegate alla fornitura del servizio erogato. Per tale motivo, il richiedente si impegnerà a comunicare eventuali variazioni alle informazioni indicate ai punti (1), (2) e (3). I dati verranno trattati nel rispetto delle normative vigenti;
- 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.

Data Firma

Sezione 2: Autorizzazione da compilare a cura dell'U.O.C. Sistema Informativo

Il Responsabile dell'U.O.C. Sistema informativo, in relazione alla richiesta di cui sopra, esprime il seguente parere:

☐ **FAVOREVOLE**

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

……

……

……

……

……

Data

Il Resp. dell'U.O.C. Sistema Informativo

_____

(*In caso di parere FAVOREVOLE*)

Il Direttore Generale dell'AOU in qualità di Titolare

_____

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.
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.7**:
  - Datare e firmare l'assunzione di responsabilità

Informativa per gli utenti esterni del servizio di Accesso Sicuro ed Autorizzato (VPN) al Sistema Informativo dell'A.O.U. "Federico II" ai fini del trattamento dei dati personali raccolti

(ai sensi degli articoli 13 e 14 del Regolamento europeo in materia di protezione dei dati personali 679/2016)

1. Premessa

Il servizio di Accesso Sicuro ed Autorizzato (**Servizio**) al Sistema Informativo dell'A.O.U. "Federico II" consente l'accesso, ad un soggetto esterno autorizzato (**Richiedente**), alla rete privata ospedaliera come se il soggetto fosse fisicamente collegato e presente nell'infrastruttura telematica dell'A.O.U. stessa.

Il Servizio viene autorizzato dall'A.O.U. "Federico II" (**Titolare**) il cui rappresentante legale è il Direttore Generale, con sede legale in via S. Pansini n.5 – 80131 Napoli.

Il Servizio viene erogato, in nome e per conto dell'A.O.U., dal C.S.I. – Centro di ateneo per i Servizi Informativi dell'Università di Napoli "Federico II" (**Responsabile del Trattamento** o **RdT**) che si avvale di un'infrastruttura telematica appositamente realizzata e di un'organizzazione interna adibita a tale scopo.

Le informazioni personali (**Dati**) richieste all'atto dell'istanza vengono raccolte dal Titolare per gli adempimenti di sua pertinenza e comunicati al C.S.I. per l'erogazione del servizio.

L'accesso viene offerto laddove ne sia stata contemplata la fornitura in fase contrattuale, ma anche nel caso in cui il Titolare reputi, a suo insindacabile giudizio, che il servizio sia utile a garantire la continuità assistenziale e/o per conseguire un risparmio economico nei contratti di manutenzione.

Il Titolare tratterà i dati dei Richiedenti in base e con le modalità relative alla seguente casistica.

- La fornitura del Servizio **non** è contemplata nel contratto con l'A.O.U.. L'istanza viene ricevuta dal Titolare ma non viene autorizzata: nessun trattamento dei dati del richiedente.
- La fornitura del Servizio **è** contemplata nel contratto con l'A.O.U.. L'istanza viene ricevuta dal Titolare ma non viene autorizzata (ad es. per mancanza delle necessarie garanzie di sicurezza): il Titolare tratterà in ogni caso i dati del richiedente. La finalità è quella, prudenziale, di poter dimostrare di aver provato ad ottemperare agli obblighi contrattuali, ma il Professionista / Società / Ente non era in possesso dei requisiti per poterne usufruire.
- La fornitura del servizio **è**/**non è** contemplata nel contratto con l'A.O.U.. L'istanza viene ricevuta ed autorizzata dal Titolare che tratterà i dati del richiedente secondo le finalità indicate nella presente informativa.
- La fornitura del servizio **è**/**non è** contemplata nel contratto con l'A.O.U.. L'istanza viene ricevuta ed autorizzata dal Titolare, ma successivamente revocata (ad es. a seguito di un audit con esito negativo): il Titolare tratterà i dati del richiedente secondo le finalità indicate nella presente informativa. Il fine del trattamento è il legittimo interesse del Titolare nel verificare e tutelare l'integrità dei dati, accertare che nell'utilizzo del Servizio non vi sia stata compromissione dei sistemi, provare eventuali responsabilità in caso di data breach o reati informatici, ecc. oltreché effettuare delle verifiche a gestione di eventuali reclami da parte degli interessati.

Il soggetto esterno autorizzato assicurerà al Titolare le necessarie garanzie di sicurezza (ad es. quelle richiamate dall'art.32 del GDPR), senza le quali il RdT, in presenza di eventuali anomalie di utilizzo ed in base alle istruzioni impartite dal Titolare, interromperà senza preavviso l'erogazione del Servizio.

2. Gli interessati

Gli interessati sono gli utilizzatori autorizzati del Servizio.

Eventuali terzi (interessati del soggetto autorizzato) vengono disciplinati dal rapporto contrattuale con il Titolare.

3. Data Protection Officer (DPO)

Il Titolare ha nominato un Responsabile della Protezione dei Dati (DPO) che può essere contattato dagli interessati per tutte le questioni relative al trattamento dei loro dati personali e all'esercizio dei loro diritti derivanti dalla normativa in materia di protezione dei dati personali:

Ing. Guglielmo Toscano
Indirizzo: via S. Pansini 5 - 80131 Napoli
PEC: rpd.aou@pec.it
Tel.: 081 746 4223

4. Dati raccolti

I dati, richiesti all'atto della istanza, sono necessari alla corretta identificazione del Richiedente e dei soggetti autorizzati alla connessione. In base all'art.5 lett c del GDPR, i dati raccolti sono i minimi necessari rispetto alle finalità indicate nel §6 - *Finalità del trattamento e base giuridica*.

I dati raccolti appartengono alle seguenti categorie:

- **Dati anagrafici** (nome, cognome, ecc.): hanno il principale scopo di identificare univocamente il richiedente, in quanto referente apicale per la richiesta del Servizio, ed i dipendenti da lui autorizzati all'utilizzo dello stesso, in quanto destinatari delle credenziali personali di accesso.
- **Dati di contatto** (numeri di telefono, mail, pec): sono necessari, al Titolare e al RdT, per poter comunicare con il richiedente in maniera formale (tramite gli strumenti legalmente riconosciuti come lettera raccomandata o PEC) o, al RdT, con i soggetti autorizzati alla connessione per la comunicazione delle modalità di utilizzo del servizio e l'invio delle credenziali di accesso.
- **Dati utili alla verifica del possesso di un contratto in essere con l'A.O.U. "Federico II"** (n. CIG, Delibera approvazione atti, n. protocollo, ecc.): il Richiedente, per poter effettuare una richiesta elegibile ad ottenere il Servizio, deve essere in possesso di un contratto in essere con l'A.O.U. "Federico II"; tali dati, forniti dal Richiedente, sono trattati per poter verificare la sussistenza del contratto ai fini dell'erogazione del servizio.
- **Dati utili alla verifica del possesso della nomina a Responsabile del Trattamento Dati** (copia nomina, ove applicabile): il Richiedente, per poter effettuare una richiesta elegibile ad ottenere il servizio, deve essere in possesso della nomina a Responsabile del Trattamento che lo autorizza a trattare i dati per conto del Titolare; tali dati, forniti dal Richiedente, sono trattati per poter verificare la sussistenza della designazione ai fini dell'erogazione del servizio.

5. Altri dati trattati

I sistemi e le procedure informatiche, preposte al funzionamento delle connessioni richieste, acquisiscono, nel corso del loro normale esercizio, alcuni dati personali e tecnici, la cui trasmissione è implicita nell'uso dei protocolli alla base del loro funzionamento.

Si tratta di informazioni raccolte automaticamente e che associano, a ciascun account rilasciato, i flussi di dati ad esso relativi, consentendo, quindi, l'identificazione dell'utente e delle sue azioni.

In questa categoria di dati rientrano: gli indirizzi IP ed i mac-address utilizzati dagli utenti che si connettono, gli indirizzi di destinazione delle risorse per le quali è stato richiesto l'accesso, l'orario della connessione, il metodo utilizzato nel sottoporre richieste ai server, la dimensione dei file ottenuti in risposta, il codice numerico indicante lo stato della risposta data dai server (buon fine, errore, ecc.) ed altri parametri relativi al sistema operativo e all'ambiente informatico dell'utente.

Tali dati rientrano nella categoria dei **Dati di connessione**.

Il fine è quello della tutela dell'integrità dei dati e delle verifiche a gestione di eventuali reclami da parte degli interessati, ma anche quello di ricavare informazioni statistiche sull'uso delle connessioni, per controllarne il corretto funzionamento e l'esatto accesso alle risorse. Tali dati potrebbero essere utilizzati per l'accertamento di responsabilità in caso di reati informatici o data breach ai danni del Sistema informativo dell'A.O.U., degli utenti aziendali e/o degli utenti ospedalieri; potranno, inoltre, essere forniti agli organi di pubblica sicurezza su richiesta dell'autorità giudiziaria.

Il Titolare ha delegato il RdT alla raccolta e la conservazione di tali informazioni per le finalità di cui al §6 - *Finalità del trattamento e base giuridica*.

6. Finalità del trattamento e base giuridica

Tutti i dati forniti in sede di istanza sono trattati dal Titolare. Gli stessi sono resi sotto la personale responsabilità del richiedente ed allo stesso è rimandata anche la responsabilità ed il diritto di rettificarli (§8 – *I diritti degli interessati*).

La base giuridica per il trattamento dei dati forniti **in fase di istanza** è l'adempimento degli obblighi contrattuali per l'erogazione del Servizio (GDPR art.6 lett. b).

Tutti i dati raccolti in maniera automatizzata, e riferiti all'utilizzo del servizio, sono connessi alla tecnologia delle attrezzature utilizzate e sono trattati dal RdT su istruzione del Titolare.

La base giuridica per il trattamento dei dati raccolti **in fase di utilizzo del servizio** è il legittimo interesse del Titolare nel verificare e tutelare l'integrità dei dati, per la sicurezza delle reti e delle comunicazioni, accertare che l'utilizzo del Servizio avvenga secondo gli accordi contrattuali, provare eventuali responsabilità in caso di data breach o reati informatici, ecc. oltreché effettuare delle verifiche a gestione di eventuali reclami da parte degli interessati (GDPR art.6 lett. f).

7. Destinatari dei dati

Nei limiti pertinenti alle finalità di trattamento indicate, il destinatario dei dati è il C.S.I., in qualità di Responsabile del Trattamento.

I dati non saranno in alcun modo oggetto di diffusione.

Per legittimo interesse del Titolare i dati potranno essere comunicati all'autorità competente e agli autorizzati che operano sotto il controllo del Titolare.

8. I diritti degli interessati

Gli interessati hanno il diritto di ottenere dal Titolare, nei casi previsti, l'accesso ai propri dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento che li riguarda o di opporsi al trattamento (artt. 15 e ss. del Regolamento). E' possibile presentare istanza al Titolare contattando il Responsabile della Protezione dei Dati (DPO) attraverso i canali ufficiali descritti nel §3 - *Data Protection Officer (DPO)*

9. Modalità di trattamento

I dati forniti saranno sottoposti a trattamento cartaceo e/o elettronico da parte del Titolare e degli RdT individuati, non saranno tuttavia sottoposti a processi decisionali automatizzati.

10. Luogo del trattamento

I dati verranno trattati dal Titolare e dal Responsabile del Trattamento presso le proprie sedi operative tutte situate nel territorio Italiano.

Nell'eventualità di utilizzo di servizi in cloud, i dati raccolti non saranno oggetto di trasferimento in paesi terzi non autorizzati dall'UE.

11. Periodo di conservazione

I dati saranno conservati in modo da consentire l'identificazione degli interessati per un tempo non superiore a quello necessario al conseguimento delle finalità del trattamento o del legittimo interesse del Titolare. Una volta soddisfatte tali finalità, i dati saranno cancellati. In particolare:

- I dati relativi alle connessioni saranno trattati in relazione alle finalità sopra descritte per adempiere agli obblighi di legge. In ogni caso gli stessi saranno conservati per ulteriori 12 mesi dopo la regolare scadenza del contratto al fine di verificare l'integrità dei dati sui quali il Servizio ha consentito le attività, per la sicurezza delle reti e delle comunicazioni, per provare eventuali responsabilità in caso di data breach o reati informatici, ecc. e a gestione di eventuali reclami da parte degli interessati.
- I dati relativi alle richieste presentate saranno trattati fino alla scadenza del contratto e, in ogni caso, entro i limiti di legge. Poiché tali dati sono intrinsecamente collegati a quelli relativi alle connessioni, il loro periodo di conservazione sarà almeno pari a quello di questi ultimi.

12. Attestazione di presa visione

☐ Ho letto e compreso la presente informativa. In particolare, ho compreso che i dati personali forniti in fase di istanza verranno trattati per l'adempimento degli obblighi contrattuali di cui sono parte e che, i dati raccolti in fase di utilizzo del servizio verranno trattati per interesse legittimo del Titolare.

Firma del Richiedente