Allegato 4 – Voucher

L'Operatore di telecomunicazioni che - nell'ambito dell'implementazione delle attività relative al seguente progetto:

"Progetto voucher Banda ultralarga": misura con la quale si intende progettare e sviluppare un intervento per il sostegno alla domanda di servizi ultraveloci (NGA e VHCN) in tutte le aree del Paese allo scopo di ampliare il numero di Beneficiari che adottano servizi digitali utilizzando reti ad alta velocità ad almeno 30 Mbit/s"

intende sottoscrivere la *Convenzione per l'attivazione di una misura di incentivazione destinata all'incremento della domanda di servizi di connettività*, quale documento predisposto al fine di disciplinare le modalità di interazione fra l'Operatore e Infratel Italia S.p.A. per l'attivazione del servizio da erogare al beneficiario del progetto voucher

è tenuto a compilare e presentare ad Infratel Italia la seguente "*dichiarazione di compliance privacy e cybersecurity*". Trattasi di un adempimento necessario e propedeutico alla sottoscrizione della citata Convenzione.

DICHIARAZIONE DI COMPLIANCE PRIVACY E CYBERSECURITY

L'Operatore di telecomunicazioni:

……., con sede legale in……. Via ……, codice fiscale - Partita Iva ……, numero di iscrizione al registro delle imprese ……., in persona del legale rappresentante

DICHIARA

- di osservare tutti gli obblighi derivanti dalla normativa in materia di Protezione dei Dati Personali, in particolare il Regolamento UE n. 2016/679 ("GDPR") nonché ogni ulteriore norma dettata a livello nazionale o sovranazionale in materia di protezione dei dati, in particolare con riferimento ai provvedimenti emanati dall'Autorità Garante per la Protezione dei Dati Personali ovvero del Comitato Europeo per la Protezione dei Dati (la "Normativa Applicabile");
- di aver posto in essere tutti gli adempimenti richiesti dalla normativa in materia di Protezione dei Dati Personali, al fine di garantire piena riservatezza, integrità e disponibilità dei dati personali oggetto di trattamento;
- di aver adottato tutte le misure organizzative e tecniche idonee ad assicurare sia il rispetto della normativa in materia di Protezione dei Dati Personali sia la sicurezza delle informazioni.

A maggior specificazione di quanto sopra menzionato,

DICHIARA

di aver adottato le misure di seguito indicate:

- assessment management*:* sono stati definiti e resi noti ruoli e responsabilità inerenti il trattamento e la protezione dei dati personali per tutto il personale e per eventuali terze parti rilevanti (es.

fornitori, clienti, partner) e – a tale riguardo – sono stati adottati relativi atti di designazione/autorizzazione e nomine nel rispetto del cd. principio del minimo privilegio;

- i requisiti legali in materia di cybersecurity, con l'inclusione degli obblighi riguardanti la privacy e le libertà civili, sono compresi e gestiti;
- per quanto riguarda i suoi strumenti, prodotti, applicazioni o servizi, è garantito il rispetto dei principi della protezione dei dati fin dalla fase di progettazione (Privacy by Design) e della protezione dei dati per impostazione predefinita (Privacy by Default);
- tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, è stata messa in atto una gestione degli adempimenti privacy in linea con l'art. 32 GDPR e sono stati adottati misure tecniche ed organizzative idonee a garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:
    - la pseudonimizzazione e la cifratura dei dati personali;
    - la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
    - la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
    - una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento;
- sono stati nominati i propri Amministratori di Sistema, in adempimento a quanto previsto dal provvedimento del Garante del 27.11.08, pubblicato in G.U. n. 300 del 24.12.2008, ove ne ricorrano i presupposti;
- si è provveduto alla nomina del DPO, se obbligatorio;
- è stato adottato una compliance privacy idonea ad assicurare la corretta gestione dei seguenti adempimenti: analisi del rischio; valutazione di impatto; sicurezza del trattamento; valutazione fornitori/Responsabili del trattamento; tenuta del registro del trattamento; uso della rete, del sistema e delle risorse fisiche all'interno dell'organizzazione; definizione delle azioni vietate e consentite da parte dei dipendenti; definizione degli obblighi delle parti / persone coinvolte nel trattamento dei dati personali, compreso l'obbligo di confidenzialità; controllo della sicurezza degli accessi logico-fisica; adozione di procedure e policy di sicurezza per la protezione dei dati personali; gestione risorse/asset; sicurezza Server/Database; sicurezza postazioni di lavoro; sicurezza della rete/comunicazioni; accesso a Dispositivi Mobili/Portatili; protezione da malware; gestione password e account; inventario dispositivi e software; identificazione e rispetto delle leggi e/o i regolamenti con rilevanza in tema di cybersecurity che risultino applicabili; rispetto dei principi privacy e attuazione degli adempimenti volti a garantire l'informazione degli interessati e l'esercizio dei diritti a questi ultimi riconosciuti dalla legislazione vigente;
- è stata adottata una procedura sicura per la gestione degli incidenti e dei *data breach*;
- vengono utilizzati sistemi crittografici per la sicurezza dei dati memorizzati, archiviati o trasmessi;
- vengono disabilitati o modificati immediatamente i diritti di accesso quando lo stato di un dipendente o di un altro soggetto cambia (terminazione, trasferimento, ecc.);
- è stato adottato un piano di continuità aziendale;
- è stato adottato un piano di *disaster recovery*/ un piano di backup ed un piano di test di ripristino e/o ripristino del backup;
- vengono effettuate scansioni delle vulnerabilità e i *penetration test* periodici e corregge la vulnerabilità in modo tempestivo;

- sono stati adottati presidi per restituire o smaltire/distruggere in modo sicuro tutti i dati del titolare al momento della risoluzione del contratto;
- è stato adottato un piano di risposta agli incidenti per notificare al titolare al momento del rilevamento di eventuali incidenti di sicurezza che coinvolgono o che hanno un impatto sul titolare o che hanno compromesso il sistema informativo e informativo del titolare;
- sono definiti, implementati e documentati i processi di trasferimento dei dati in ambito internazionale assicurando rispetto della normativa di settore;
- gli archivi ove i dati saranno conservati sono protetti mediante misure di sicurezza efficaci e adeguati a contrastare i rischi di violazione. Gli archivi sopra citati si trovano all'interno dei confini dell'EU (o SEE) e non è prevista la loro connessione o interazione con database locati al di fuori dell'Unione Europea.

Avendo riguardo anche alla cybersecurity,

DICHIARA

di aver adottato le misure di seguito indicate:

- *Governance*

Le politiche, le procedure e i processi per gestire e monitorare i requisiti dell'organizzazione (organizzativi, legali, relativi al rischio, ambientali) sono compresi e utilizzati nella gestione del rischio di cybersecurity.

- *Risk Assessment*

L'impresa comprende il rischio di cybersecurity inerente l'operatività dell'organizzazione (incluse la mission, le funzioni, l'immagine o la reputazione), gli asset e gli individui.

- *Supply Chain Risk Management*

Le priorità, i vincoli, le tolleranze al rischio e le ipotesi dell'organizzazione sono stabilite e utilizzate per supportare le decisioni di rischio associate alla gestione del rischio legato alla catena di approvvigionamento. L'organizzazione ha definito e implementato i processi atti a identificare, valutare e gestire il rischio legato alla catena di approvvigionamento.

- *Identity Management, Authentication and Access Control*

L'accesso agli asset fisici e logici ed alle relative risorse è limitato al personale, ai processi e ai dispositivi autorizzati, ed è gestito in maniera coerente con la valutazione del rischio di accesso non autorizzato alle attività ed alle transazioni autorizzate, avendo cura di rispettare la normativa privacy e garantire la sicurezza informatica.

- *Awareness and Training*

Il personale e le terze parti sono sensibilizzati in materia di tutela dei dati personali e cybersecurity e vengono addestrate per adempiere ai loro compiti e ruoli coerentemente con le politiche, le procedure e gli accordi esistenti.

- *Data Security*

I dati sono memorizzati e gestiti in accordo alla strategia di gestione del rischio dell'organizzazione, al fine di garantire l'integrità, la confidenzialità e la disponibilità delle informazioni.

- *Information Protection Processes and Procedures*

Sono attuate e adeguate nel tempo politiche di sicurezza (che indirizzano scopo, ambito, ruoli e responsabilità, impegno da parte del management e coordinamento tra le diverse entità organizzative), processi e procedure per gestire la protezione dei sistemi informativi e degli assets.

- *Maintenance*

La manutenzione dei sistemi informativi e di controllo industriale è fatta in accordo con le politiche e le procedure esistenti.

- *Protective Technology*

Le soluzioni tecniche di sicurezza sono gestite per assicurare sicurezza e resilienza di sistemi e asset, in coerenza con le relative politiche, procedure ed accordi.

- *Anomalies and Events*

Le attività anomale sono rilevate e il loro impatto potenziale viene analizzato.

- *Security Continuous Monitoring*

I sistemi informativi e gli asset sono monitorati per indentificare eventi di cybersecurity e per verificare l'efficacia delle misure di protezione

- *Detection Processes*

Sono adottati, mantenuti e verificati processi e procedure di monitoraggio per assicurare la comprensione di eventi anomali.

- *Response Planning*

Procedure e processi di risposta sono eseguiti e mantenuti per assicurare una risposta agli incidenti di cybersecurity rilevati ed il rispetto della normativa in materia di protezione dei dati personali

- *Communications*

Le attività di risposta sono coordinate con le parti interne ed esterne (es. eventuale supporto da parte degli organi di legge o dalle forze dell'ordine).

- *Analysis*

Vengono condotte analisi per assicurare un'efficace riposta e supporto alle attività di ripristino.

- *Mitigation*

Vengono eseguite azioni per prevenire l'espansione di un evento di sicurezza, per mitigare i suoi effetti e per risolvere l'incidente.

- *Improvements*

Le attività di risposta sono migliorate incorporando le "*lesson learned*" da attività precedenti di monitoraggio e risposta.

- *Recovery Planning*

I processi e le procedure di ripristino sono eseguiti e mantenuti per assicurare un recupero dei sistemi o asset coinvolti da un incidente di cybersecurity.

- *Improvements*

I piani di ripristino ed i relativi processi sono migliorati tenendo conto delle "*lesson learned*" per le attività future.

- *Communications*

Le attività di ripristino a seguito di un incidente sono coordinate con le parti interne ed esterne (es. le vittime, gli ISP, i proprietari dei sistemi attaccati, i *vendor*, i CERT/CSIRT).

DICHIARA

- di impegnarsi a fornire evidenza di quanto dichiarato nella presente dichiarazione;

DICHIARA

- che quanto sopra dichiarato riguarda anche i dealer.

Data _____

Firma del dichiarante *(per esteso e leggibile)* _____