POLITICA DI DATA RETENTION

DENOMINAZIONE TITOLARE TRATTAMENTO	INTERCOM S.R.L.
INDIRIZZO SEDE LEGALE	Via Piantà, 8, 28010 Vaprio D'Agogna NO
PIVA	01538710037
INDIRIZZO E-MAIL	amministrazione@intercom.it
LEGALE RAPPRESENTANTE	MARA AGAZZONE
ATTIVITA	Service Provider
RESPONSABILE PROTEZIONE DATI	AVV. Martina Marchetti
DATA CREAZIONE PROCEDURA	VERS. 001 15/11/2023

DATA ULTIMA MODIFICA	01/12/2023

INDICE

1. DEFINIZIONI

Dati di traffico: qualsiasi dato sottoposto a trattamento ai fini della trasmissione di una comunicazione su una rete di comunicazione elettronica o della relativa fatturazione, ivi compresi i dati necessari per identificare l'abbonato o l'utente.

Servizi di comunicazione elettronica: i servizi consistenti esclusivamente o prevalentemente nella trasmissione di segnali su reti di comunicazioni elettroniche;

Utente: qualsiasi persona fisica o giuridica che utilizza un servizio di comunicazione elettronica accessibile al pubblico, senza esservi necessariamente abbonata

Contraente: qualunque persona fisica, persona giuridica, ente o associazione parte di un contratto con un fornitore di servizi di comunicazione elettronica accessibili al pubblico per la fornitura di tali servizi, o comunque destinatario di tali servizi tramite schede prepagate

Dati relativi all'ubicazione: ogni dato trattato in una rete di comunicazione elettronica che indica la posizione geografica dell'apparecchiatura terminale dell'utente di un servizio di comunicazione elettronica accessibile al pubblico, ivi compresi quelli relativi alla cella da cui una chiamata di telefonia mobile ha origine o nella quale si conclude

Chiamata senza risposta: la connessione istituita da un servizio telefonico accessibile al pubblico, non seguita da un'effettiva comunicazione, in quanto il destinatario non ha risposto ovvero vi è stato un intervento del gestore della rete;

Identificativo dell'utente: l'identificativo unico assegnato a una persona al momento dell'abbonamento o dell'iscrizione presso un servizio di accesso internet o un servizio di comunicazione internet;

Indirizzo di protocollo Internet (IP) univocamente assegnato: indirizzo di protocollo (IP) che consente l'identificazione diretta dell'abbonato o utente che effettua comunicazioni sulla rete pubblica;

Posta elettronica: messaggi contenenti testi, voci, suoni o immagini trasmessi attraverso una rete pubblica di comunicazione, che possono essere archiviati in rete o nell'apparecchiatura terminale ricevente, fino a che il ricevente non ne ha preso conoscenza.

2. TIPOLOGIA DI SERVIZI E CONTENUTO DEI TABULATI DI TRAFFICO STORICO

Intercom offre all'utenza molteplici **SERVIZI DI COMUNICAZIONE ELETTRONICA**. In particolare, offre:

- **SERVIZI TELEFONICI**: chiamate telefoniche, incluse le chiamate vocali, di messaggeria vocale, in conferenza e di trasmissione dati tramite telefax; i servizi supplementari, inclusi l'inoltro e il trasferimento di chiamata; la messaggeria e i servizi multimediali, inclusi i servizi di messaggeria breve-sms.
- **SERVIZI TELEMATICI**: l'accesso alla rete Internet, alla posta elettronica, i fax (nonché i messaggi sms e mms) via Internet; la telefonia via Internet (cd. Voice over Internet Protocol–VoIP)

La seguente tabella riporta i contenuti che devono essere presenti all'interno dei TABULATI DI TRAFFICO STORICO.

	TELEFONIA FISSA/MOBILE	**ACCESSO INTERNET**	**POSTA ELETTRONICA**	**TELEFONIA/FAX/SMS/MMS VIA INTERNET**
DATI NECESSARI PER RINTRACCIARE E IDENTIFICARE LA FONTE DI UNA COMUNICAZIONE	numero telefonico chiamante; nome e indirizzo dell'abbonato o dell'utente registrato	nome e indirizzo dell'abbonato o dell'utente registrato a cui al momento della comunicazione sono stati univocamente assegnati l'indirizzo di protocollo Internet (IP), un identificativo di utente o un numero telefonico	indirizzo IP utilizzato e indirizzo di posta elettronica ed eventuale ulteriore identificativo del mittente indirizzo IP e nome a dominio pienamente qualificato del mail exchanger host, nel caso della tecnologia SMTP ovvero di qualsiasi tipologia di host relativo ad una diversa tecnologia utilizzata per la trasmissione della comunicazione;	indirizzo IP, numero telefonico ed eventuale altro identificativo dell'utente chiamante; dati anagrafici dell'utente registrato che ha effettuato la comunicazione
DATI NECESSARI PER RINTRACCIARE E IDENTIFICARE LA DESTINAZIONE DI UNA COMUNICAZIONE	numero composto, ovvero il numero o i numeri chiamati e, nei casi che comportano servizi supplementari come l'inoltro o il trasferimento di chiamata, il numero o i numeri a cui la chiamata è trasmessa; nome e indirizzo dell'abbonato o dell'utente registrato	---	indirizzo di posta elettronica, ed eventuale ulteriore identificativo, del destinatario della comunicazione; 2.2 indirizzo IP e nome a dominio pienamente qualificato del mail exchanger host (nel caso della tecnologia SMTP), ovvero di qualsiasi tipologia di host (relativamente ad una diversa tecnologia utilizzata), che ha provveduto alla consegna del messaggio; 2.3 indirizzo IP utilizzato per la ricezione ovvero la consultazione dei messaggi di posta elettronica da	indirizzo IP, numero telefonico ed eventuale altro identificativo dell'utente chiamato; dati anagrafici dell'utente registrato che ha ricevuto la comunicazione; numero o numeri a cui la chiamata è trasmessa, nei casi di servizi supplementari come l'inoltro o il trasferimento di chiamata;

			parte del destinatario indipendentemente dalla tecnologia o dal protocollo utilizzato	
DATI NECESSARI PER DETERMINARE LA DATA, L'ORA E LA DURATA DI UNA COMUNICAZIONE	data e ora dell'inizio e della fine della comunicazione	data e ora (GMT) della connessione e della disconnessione dell'utente del servizio di accesso internet, unitamente all'indirizzo IP, dinamico o statico, univocamente assegnato dal fornitore di accesso internet a una comunicazione e l'identificativo dell'abbonato o dell'utente registrato	data e ora (GMT) della connessione e della disconnessione dell'utente del servizio di posta elettronica su internet ed indirizzo IP utilizzato, indipendentemente dalla tecnologia e dal protocollo impiegato;	data e ora (GMT) della connessione e della disconnessione dell'utente del servizio utilizzato su internet ed indirizzo IP impiegato, indipendentemente dalla tecnologia e dal protocollo usato;
DATI NECESSARI PER DETERMINARE IL TIPO DI COMUNICAZIONE	il servizio telefonico utilizzato	---	il servizio telefonico utilizzato	il servizio telefonico utilizzato
DATI NECESSARI PER DETERMINARE LE ATTREZZATURE DI COMUNICAZIONE DEGLI UTENTI	numeri telefonici chiamanti e chiamati per la telefonia mobile: numeri telefonici chiamanti e chiamati; marca modello e versione del software degli apparecchi	numero telefonico chiamante per l'accesso commutato (dial-up access); 3.2 digital subscriber line number (DSL) o un altro identificatore finale di chi è all'origine della comunicazione	---	numero telefonico chiamante per l'accesso commutato (dial-up access); 3.2 digital subscriber line number (DSL) o un altro identificatore finale di chi è all'origine della comunicazione
DATI NECESSARI PER DETERMINARE L'UBICAZIONE DELLE APPARECCHIATURE DI COMUNICAZIONE MOBILE	-----	---	---	---

Tabella 1

Ai sensi della normativa vigente in materia di conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione, **non viene conservato alcun dato relativo al contenuto della comunicazione**.

3. CLASSIFICAZIONE DEI DATI PERSONALI

CLASSIFICAZIONE DATI/ETICHETTA	LIVELLO RISCHIO PERDITA DATI	AUTORIZZAZIONI DI ACCESSO AI DATI	TIPOLOGIE DI DATI	REGOLE
DATI PUBBLICI	TRASCURABILE I dati pubblici non richiedono alcun controllo, essendo destinati ad una fruizione pubblica	tutti possono avere accesso	denominazione clienti dati di contatto dei clienti	nessuna
DATI AD USO INTERNO	LIMITATO La divulgazione non autorizzata di dati/informazioni potrebbe creare solo lievi disagi in capo agli interessati	Tali dati sono a disposizione di tutto il personale di Intercom	dati di contatto del personale dipendente e dei fornitori	Tali dati possono essere acquisiti ed utilizzati da tutto il personale di Intercom con ordinaria diligenza per esclusive finalità lavorative, consapevole che, in ogni caso, costituiscono un bene da proteggere. È quindi vietato qualsiasi utilizzo degli stessi per finalità personali. I documenti "ad uso interno" possono circolare liberamente nell'ambito di Intercom ma non sono destinati alla diffusione. L'eventuale divulgazione esterna può risultare inopportuna rispetto ai diritti e alle libertà degli interessati. Pertanto, a tal fine, è necessario richiedere un'autorizzazione al datore di lavoro.

DATI RISERVATI	ALTO La divulgazione non autorizzata di dati/informazioni riservati potrebbe comportare un pericolo per i diritti e le libertà degli interessati	L'accesso ai dati personali deve essere regolamentato in base al principio del "need to know" e del "need to do", ossia limitato a quelle attività strettamente necessarie allo svolgimento delle mansioni assegnate in funzione delle specifiche esigenze operative. Pertanto, il personale che può accedervi deve essere espressamente autorizzato.	dati di traffico telefonico e telematico	Tali dati possono essere acquisiti ed utilizzati solo dal personale di Intercom espressamente autorizzato e per esclusive finalità lavorative, consapevole che, in ogni caso, costituiscono un bene da proteggere. È quindi vietato qualsiasi utilizzo delle stesse per finalità personali. I documenti "riservati" non possono circolare liberamente nell'ambito di Intercom e non possono essere messi a disposizione di terze parti a meno di una preventiva e formale autorizzazione del datore di lavoro e della stipula di specifici accordi di riservatezza. Poiché l'eventuale divulgazione, interna o esterna a personale non autorizzato, può danneggiare i diritti e le libertà dell'interessato, è indispensabile adottare ogni precauzione necessaria ad impedire la rivelazione di tali dati a soggetti non autorizzati ed a garantire il trattamento degli stessi. In caso di divulgazione esterna deve essere sempre richiesta un'autorizzazione al datore di lavoro. I dati personali riservati devono essere contenuti in documenti cartacei o in supporti di memorizzazione, devono essere conservati in mobili chiusi a chiave (ad es. armadi, cassettiere, ecc.). Tali dati, se risiedono in locale all'interno di postazioni lavorative, occorre procedere con un back-up locale nell'ambito dell'ufficio su idonei supporti di memorizzazione (ad es. hard disk esterni, CD, DVD, Token USB, ecc.), opportunamente etichettati, in grado di assicurare l'inalterabilità nel tempo e la disponibilità dell'informazione, in accordo con le politiche della società. L'indicazione "dati riservati", seppur opzionale, è raccomandata in quanto è in grado di ridurre al minimo i rischi di distruzione o perdita, anche accidentale, delle informazioni stesse o di accesso non autorizzato o di trattamento non consentito.

				I supporti rimovibili contenenti tali dati possono essere riutilizzati solo se le informazioni in essi precedentemente contenute non siano intelligibili e tecnicamente in alcun modo ricostruibili
DATI STRETTAMENTE RISERVATI	MOLTO ALTO La divulgazione non autorizzata potrebbe recare un danno eccezionale a BT. Le informazioni strettamente riservate richiedono i controlli di sicurezza più severi e pertanto l'utente è tenuto a valutarne attentamente la natura	L'accesso a tali dati è destinato a un numero estremamente limitato di soggetti, in particolare, solo la dirigenza ha accesso ai dati.		Tali dati possono essere acquisiti ed utilizzati solo da parte della dirigenza. È quindi vietato qualsiasi utilizzo delle stesse per finalità personali. I documenti "strettamente riservati" non possono circolare liberamente nell'ambito di Intercom in quanto vincolati da direttive interne, normative nazionali e internazionali, né essere messi a disposizione di terze parti a meno di una preventiva e formale autorizzazione del datore di lavoro e/o della stipula di specifici accordi di riservatezza. Nessun dato può essere divulgato o diffuso a soggetti non autorizzati a conoscerli. I dati devono essere conservati in armadi la cui resistenza ed il cui dispositivo di chiusura sono considerati sicuri e affidabili. Tali dati, contenuti in documenti elettronici dati devono essere conservati centralmente e sottoposte a backup secondo quanto previsto dalle politiche della società. La riservatezza delle informazioni classificate ad uso strettamente confidenziale, memorizzate su supporti rimovibili deve essere garantita attraverso opportuni algoritmi di cifratura e compressione. L'indicazione "dati strettamente riservati" è raccomandata in quanto è in grado di ridurre al minimo i rischi di distruzione o perdita, anche accidentale, delle informazioni stesse o di accesso non autorizzato o di trattamento non consentito. I supporti rimovibili contenenti tali dati possono essere riutilizzati solo se le informazioni in essi precedentemente contenute non siano intelligibili e tecnicamente in alcun modo ricostruibili.

Tabella 2

4. FINALITA', GARANZIE E TERMINI DI CONSERVAZIONE DEI DATI DI TRAFFICO

4.1 Finalità di conservazione

Durante l'utilizzo di un servizio di comunicazione elettronica, ogni utente lascia specifiche tracce digitali che, nell'insieme, rappresentano un'ombra digitale. Alla maggior parte di queste informazioni possono accedere solo le Autorità Giudiziarie e la Polizia giudiziaria delegata da questa.

Ciò premesso, la normativa in materia di traffico dati e di protezione dati personali prevede che i dati di traffico debbano essere conservati al fine di ottemperare due finalità:

FINALITA'	TERMINI CONSERVAZIONE	DATI PERSONALI	BASE GIURIDICA
DI FATTURAZIONE (contestazione della fattura o gestione delle pretese di pagamento)	non più di 6 mesi salva l'ulteriore specifica conservazione necessaria per effetto di una contestazione anche in sede giudiziale	Minuti complessivi di chiamata fatti dai clienti PIVA e-mail indirizzo nome firmatario	obbligo di legge- 123 Codice Privacy
ACCERTAMENTO E REPRESSIONE DEI REATI	i dati di traffico telematico per non più di **12 mesi** dalla comunicazione; i dati di traffico telefonico per non più di **24 mesi** dalla comunicazione;	Si veda tabella 1	obbligo di legge- 132 Codice Privacy
	Per le finalità dell'accertamento e della repressione dei reati di cui agli articoli 51, comma 3-quater, e 407, comma 2, lettera a), del codice di procedura penale il termine di conservazione è di **72 mesi**.		

Tabella 3

4.2 Misure e accorgimenti da porre a garanzia degli interessati nell'ambito della conservazione dei dati di traffico per finalità di accertamento e repressione di reati (*)

AMBITO OPERATIVO	PRESCRIZIONI TECNICO-ORGANIZZATIVE PREVISTE DAL GARANTE	SITUAZIONE AZIENDALE
Acquisizione dati	I dati traffico possono essere acquisiti solo per finalità di accertamento e repressione di reati e non per controversie civili, amministrative e contabili	CONFORME
Sistemi di autenticazione	Il trattamento dei dati di traffico telefonico e telematico oggetto è consentito solo al personale incaricato mediante l'utilizzo di specifici sistemi di autenticazione informatica basati su tecniche di *strong authentication*, consistenti nell'uso combinato di almeno due differenti tecnologie di autenticazione. Una di tali tecnologie deve essere inoltre basata sull'elaborazione di caratteristiche biometriche. Si può eventualmente prescindere da tali sistemi solo per i trattamenti effettuati nello svolgimento di mansioni tecniche di gestione dei sistemi e delle apparecchiature informatiche. In tal caso, resta fermo, in ogni caso, l'obbligo di assicurare adeguate misure di sicurezza tecniche per le credenziali di autenticazione (robustezza, storicità ecc. cfr. politica gestione password)	PARZIALMENTE CONFORME Le tecniche di strong authentication sono presenti per l'accesso ai server con due fattori ma non biometrici.
Sistemi di autorizzazione	Occorre separare i compiti di chi accede ai dati dai compiti di chi assegna le credenziali di autenticazione.	NON CONFORME il numero di personale non è sufficiente per tale separazione

	Inoltre, nei profili di autorizzazione devono essere differenziati gli incaricati che: - trattano i dati di traffico per finalità di fatturazione e gestione degli aspetti contrattuali; - trattano i dati di traffico per l'accertamento e repressione dei reati.	
Conservazione separata	I dati di traffico conservati per esclusive finalità di accertamento e repressione di reati vanno trattati necessariamente tramite sistemi informatici distinti fisicamente da quelli utilizzati per gestire dati di traffico anche per altre finalità aziendali (fatturazione, frode, marketing), sia nelle componenti di elaborazione, sia nell'immagazzinamento dei dati (storage). Le attrezzature informatiche utilizzate per i trattamenti di dati di traffico per le esclusive finalità di giustizia devono essere collocate all'interno di aree ad accesso selezionato (ovvero riservato ai soli soggetti legittimati ad accedervi per l'espletamento di specifiche mansioni) e munite di dispositivi elettronici di controllo o di procedure di vigilanza che comportino la registrazione dei dati identificativi delle persone ammesse, con indicazione dei relativi riferimenti temporali. Nel caso di trattamenti di dati di traffico telefonico per esclusive finalità di giustizia, il controllo degli accessi deve comprendere una procedura di riconoscimento biometrico. Le forme di separazione dei dati che garantiscano il rispetto del principio di finalità dei trattamenti e l'efficacia dei profili di autorizzazione definiti possono essere ottenuti: - mediante separazione fisica, predisponendo sistemi del tutto separati nelle componenti di elaborazione e di archiviazione, oppure - mediante separazione logica, intervenendo sulla struttura delle basi di dati e/o sui sistemi di indicizzazione e/o sui metodi di accesso e/o sui profili di autorizzazione. ad oggi c'è per la telefonia e per il traffico internet è da fare Devono essere adottate misure idonee a garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli	NON CONFORME è possibile programmare di implementare la misura della separazione logica, intervenendo sulla struttura delle basi di dati e/o sui sistemi di indicizzazione e/o sui metodi di accesso e/o sui profili di autorizzazione. ad oggi c'è per la telefonia e per il traffico internet è da fare

	strumenti elettronici in tempi compatibili con i diritti degli interessati e comunque non superiori a sette giorni.	
Incaricati al trattamento	Gli incaricati che accedono ai dati di traffico conservati per le finalità di accertamento e repressione dei reati, devono essere designati specificamente in rapporto ai dati medesimi. Il processo di designazione deve prevedere la frequenza di una periodica attività formativa concernente l'illustrazione delle istruzioni, il rispetto delle misure di sicurezza e le relative responsabilità. L'effettiva partecipazione al corso deve essere documentata.	CONFORME
Cancellazione dei dati	Allo scadere dei termini previsti dalle disposizioni vigenti, i dati di traffico vanno cancellati o resi anonimi nei data base e nei sistemi di elaborazione utilizzati per i trattamenti, nonché nei sistemi e nei supporti per la realizzazione di copie di sicurezza (backup e disaster recovery) effettuate da Intercom, documentando tali operazioni al più tardi entro trenta giorni successivi alla scadenza dei termini di cui all´art. 132 del Codice privacy.	
Audit log	Devono essere adottate soluzioni informatiche idonee ad assicurare il controllo delle attività svolte sui dati di traffico da ciascun incaricato del trattamento, quali che siano la sua qualifica, le sue competenze e gli ambiti di operatività e le finalità del trattamento. Tali soluzioni comprendono la registrazione, in un apposito audit log, delle operazioni compiute, direttamente o indirettamente, sui dati di traffico e sugli altri dati personali a essi connessi, sia quando consistono o derivano dall'uso interattivo dei sistemi, sia quando sono svolte tramite l'azione automatica di programmi informatici. I sistemi di audit log devono garantire la completezza, l'immodificabilità e l'autenticità delle registrazioni in essi contenute, con riferimento a tutte le operazioni di trattamento e a tutti gli eventi relativi alla sicurezza informatica sottoposti ad auditing. A tali scopi devono essere adottati, per la registrazione dei dati di auditing, anche in forma centralizzata per ogni impianto di elaborazione o per datacenter, sistemi di memorizzazione su dispositivi non alterabili. Prima della scrittura, i dati o i raggruppamenti di dati devono essere sottoposti a procedure	PARZIALMENTE CONFORME nel senso che i controlli vengono fatti solo per chi accede alle macchine dove sono conservati i log ma non è possibile arrivare a capire quali log

	informatiche per attestare la loro integrità, basate sull'utilizzo di tecnologie crittografiche.	
Audit interno– Rapporti periodici	La gestione dei dati di traffico per finalità di accertamento e repressione di reati deve essere oggetto, con cadenza almeno annuale, di un´attività di controllo interno da parte di Intercom, in modo che sia verificata costantemente la rispondenza alle misure organizzative, tecniche e di sicurezza riguardanti i trattamenti dei dati di traffico previste dalle norme vigenti e dal provvedimento del Garante, anche per ciò che riguarda la verifica della particolare selettività degli incaricati legittimati. L'attività di controllo deve essere demandata a un'unità organizzativa o, comunque, a personale diverso rispetto a quelli cui è affidato il trattamento dei dati per la finalità di accertamento e repressione dei reati. I controlli devono comprendere anche verifiche a posteriori, a campione o su eventuale allarme derivante da sistemi di Alerting e di Anomaly Detection, sulla legittimità e liceità degli accessi ai dati effettuati dagli incaricati, sull'integrità dei dati e delle procedure informatiche adoperate per il loro trattamento. Sono svolte, altresì, verifiche periodiche sull'effettiva cancellazione dei dati decorsi i periodi di conservazione. L'attività di controllo deve essere adeguatamente documentata in modo tale che sia sempre possibile risalire ai sistemi verificati, alle operazioni tecniche su di essi effettuate, alle risultanze delle analisi condotte sugli accessi e alle eventuali criticità riscontrate. L'esito dell'attività di controllo deve essere messo, a richiesta, a disposizione del Garante o dell'autorità giudiziaria.	CONFORME
Cifratura e protezione dei dati	I dati di traffico trattati per esclusive finalità di giustizia vanno protetti con tecniche crittografiche, in particolare contro rischi di acquisizione fortuita o di alterazione accidentale derivanti da operazioni di manutenzione sugli apparati informatici o da ordinarie operazioni di amministrazione di sistema. In particolare, devono essere adottate soluzioni che rendano le informazioni, residenti nelle basi di dati a servizio delle applicazioni informatiche utilizzate per i trattamenti, non intelligibili a chi non disponga di diritti di	NON CONFORME Le macchine che producono i dati lo fanno in chiaro e pertanto non è possibile una crittografia per i primi 6 mesi, ovvero il tempo che i dati rimangono conservati sulle medesime macchine

	accesso e profili di autorizzazione idonei, ricorrendo a forme di cifratura od offuscamento di porzioni dei database o degli indici o ad altri accorgimenti tecnici basati su tecnologie crittografiche. Tale misura deve essere efficace per ridurre al minimo il rischio che incaricati di mansioni tecniche accessorie ai trattamenti (amministratori di sistema, data base administrator e manutentori hardware e software) possano accedere indebitamente alle informazioni registrate, anche fortuitamente, acquisendone conoscenza nel corso di operazioni di accesso ai sistemi o di manutenzione di altro genere, oppure che possano intenzionalmente o fortuitamente alterare le informazioni registrate. Eventuali flussi di trasmissione dei dati di traffico tra sistemi informatici del fornitore devono aver luogo tramite protocolli di comunicazione sicuri, basati su tecniche crittografiche, o comunque evitando il ricorso alla trasmissione in chiaro dei dati. Protocolli di comunicazione sicuri devono essere adottati anche per garantire, più in generale, la sicurezza dei sistemi, evitando di esporli a vulnerabilità e a rischio di intrusione (a titolo esemplificativo, l'accesso interattivo in modalità "emulazione di terminale", anche per scopi tecnici, non deve essere consentito su canali non sicuri, così come deve essere evitata l'attivazione di servizi di rete non necessari che si possono prestare alla realizzazione di forme di intrusione).	

Tabella 4

(*) Il Garante privacy ha previsto soluzioni di tipo associativo per la messa in sicurezza dei dati di traffico telefonico e telematico conservati a fini di giustizia e per le altre finalità ammesse dalla normativa. I piccoli Isp riuniti in gruppo potranno affidare a uno di loro o a una società esterna la realizzazione e la gestione della piattaforma di conservazione dei dati di traffico. L'Autorità ha ritenuto che le misure suggerite rappresentino una soluzione tecnica accettabile per garantire un'adeguata protezione dei dati di traffico telefonico e telematico da parte di realtà medio
piccole. Pertanto, agli Isp che intendono gestire la messa in sicurezza dei dati in modo "federativo" dovranno essere garantiti credenziali di accesso differenziate e spazi di memoria separati all'interno del server centralizzato. La memorizzazione dei dati dovrà avvenire in forma criptata, con un meccanismo in cui l'Isp è l'unico ad avere la chiave privata di decodifica, in modo che l'amministratore della piattaforma comune non possa aver accesso ai contenuti dei file archiviati. Come previsto dalla normativa europea, gli Isp potranno inoltre, scegliere il formato del file di archivio per la memorizzazione dei dati raccolti. Scaduti infine, i termini di conservazione i dati di traffico dovranno essere cancellati automaticamente.