Trasmissione via PEC
FG/bp

Al/Alla Responsabile
Ufficio Tecnico
Comune di Francavilla Bisio

protocollo.francavilla.bisio@cert.ruparpiemonte.it

Oggetto: Servizi di Posta Elettronica Certificata 2024

Di seguito la nostra offerta relativa ai Servizi di Posta Elettronica Certificata, redatta sulla base di quanto definito nel “Catalogo e Listino dei servizi CSI” attualmente in vigore.

Come di consueto, il nostro Referente cliente è a disposizione per integrare o mettere a punto i contenuti dell’offerta a fronte di necessità non ancora definite.

Con i migliori saluti,

Firmato digitalmente da
Franco Gola
Funzione Organizzativa
Servizi Digitali per la P.A.

108.5.1, 369/2024A/CSI
RIF.CSI: 1015512/00

CSI Piemonte - Consorzio per il Sistema Informativo
Corso Unione Sovietica, 216 10134 Torino tel. +39 011 316 81 11 fax +39 011 316 82 12 P.Iva 01995120019
Posta Elettronica Certificata protocollo@cert.csi.it www.csipiemonte.it

1. RIFERIMENTI CSI PIEMONTE

Riferimento Cliente:

Direzione P.A. Digitale
Account di riferimento: Francesco Menzio
Mail: francesco.menzio@csi.it

Mail: supporto_entilocali@csi.it

Contatto per supporto tecnico Servizio Posta Elettronica Certificata

Direzione Infrastrutture
Mail: hd_entilocali@csi.it

2. OFFERTA ECONOMICA – CANONI 2024

Servizio	Valorizzazione	Tariffa ordinari/ valore driver	Volumi	Importo
PEC -Posta elettronica certificata	Casella Standard (3 GB)	0,84€	1	0,84€
TOTALE € (IVA esclusa)				**0,84€**

Gli importi sono comprensivi degli eventuali oneri per la sicurezza.

Entro 60 gg dal ricevimento della presente offerta dovrà essere inviata a CSI Piemonte, alla casella di posta elettronica certificata protocollo@cert.csi.it, la conferma d'ordine o la presente offerta debitamente sottoscritta per accettazione.

Le caselle PEC oggetto della presente offerta sono le seguenti:

- protocollo.francavilla.bisio@cert.ruparpiemonte.it

3. CANALI DI ACCESSO ALL'ASSISTENZA

Per richieste di supporto tecnico relativamente al servizio di Posta Elettronica Certificata (malfunzionamenti, richieste di creazione o chiusura caselle) occorre fare riferimento ai canali sotto indicati specificando la natura dell'esigenza e la casella a cui è riferita la richiesta."

Servizio	Canale	Riferimento
Posta elettronica certificata	Mail	hd_entilocali@csi.it

4. POSTA ELETTRONICA CERTIFICATA - TRATTAMENTI DATI

Descrizione del trattamento: Servizio di Posta Elettronica Certificata

Categorie di interessati i cui dati personali sono trattati: Utenti di Comune di Francavilla Bisio

Categorie di dati personali trattati: Dati anagrafici e codice fiscale degli utenti che accedono alle caselle di posta, e dati personali per quanto concerne il contenuto dei messaggi di posta elettronica

Finalità del trattamento: Erogazione del servizio di Posta Elettronica Certificata

Tempo di conservazione dei dati personali trattati: La piattaforma mantiene il contenuto dei messaggi solo se essi sono presenti nella inbox di una casella attiva. Nel caso in cui una casella venga dismessa, non sarà più possibile utilizzarla per spedire o ricevere nuovi messaggi, e per i 30 giorni successivi alla dismissione l'utente potrà consultare i messaggi presenti in casella che siano pervenuti prima della revoca. Il contenuto della casella viene mantenuto per un periodo finito successivo alla dismissione (185 giorni) e il nome della medesima viene riservato (non potrà essere assegnato a diverso titolare): in questo periodo il titolare può eventualmente procedere al rinnovo della casella, ripristinandone le funzionalità e il contenuto. Trascorso tale termine, tutti i contenuti della casella verranno eliminati. Il nome della casella verrà riservato e non sarà più utilizzabile per nuove attivazioni.

Tempo di conservazione dei log di accesso: I log relativi alle attività del server di posta sono conservati per 30 mesi

Durata del trattamento: Durata annuale come previsto dall'offerta CTE

Elenco dei sub-responsabili: fatto salvo quanto specificato al punto 7) dell'Allegato "Data Protection Agreement", i sub-responsabili per il trattamento oggetto del servizio, alla data della presente proposta, sono:

- Infocert S.p.A.

Ulteriori misure di sicurezza tecniche verticali implementate sul trattamento:

Misura	Descrizione/Esempi
Minimizzazione della quantità dei dati personali	Nel trattamento sono adottate misure tecniche e/o di progetto per ridurre la quantità dei dati necessari quali tecniche di filtraggio e rimozione, riduzione della sensibilità attraverso la conversione, riduzione della natura identificativa del dato, riduzione dell'accumulazione, limitazione dell'accesso
Sistema di autorizzazione	Sono utilizzati sistemi di gestione delle autorizzazioni/ruoli applicativi che garantiscono che gli autorizzati accedano ai soli dati necessari per l'esecuzione delle attività assegnate
Sistema di autenticazione	Si utilizza un sistema di autenticazione (locale o nazionale) con un grado di sicurezza adeguato in relazione al trattamento
Gestione del ciclo di vita delle credenziali	È garantita la gestione del provisioning delle credenziali di autenticazione (creazione, revoca, modifica di credenziali) e la gestione delle autorizzazioni/ruoli applicativi (attribuzione, aggiornamento o revoca del ruolo)
Tracciabilità accessi risorse	Vengono tracciati gli accessi alle risorse critiche impiegate nel trattamento (es database, front end e back end del servizio, share di rete). Il controllo può ad es. essere implementato per un database, andando a garantire la tracciatura dell'identificativo dell'utente che ha inserito/modificato/cancellato i dati della tabella
Audit log applicativi	Vengono tracciati mediante log operazioni significative compiute dagli utenti su dati personali.
Abilitazioni puntuali accessi DB	Ad ogni utente che accede a dati personali su database è assegnata una credenziale univoca

Misura	Descrizione/Esempi
Minimizzazione della vulnerabilità delle risorse utilizzate nel trattamento	Sono previste opportune tecniche per ridurre la vulnerabilità delle risorse impiegate nel trattamento (es politiche di aggiornamento del software, test funzionale e di vulnerabilità del software utilizzato, limitazioni dell'accesso fisico al materiale che contiene dati personali)
Cifratura del canale	Viene utilizzato un canale cifrato per le comunicazioni mediante l'impiego di protocolli sicuri (es. HTTPS e SSH) nelle connessioni esposte all'esterno.
Protezione applicativa (WAF WEB Application Firewall)	Il traffico da e verso il sistema IT viene monitorato e controllato dal fornitore del servizio attraverso firewall e i sistemi di rilevamento delle intrusioni (IDS), e tecniche di filtraggio selettivo quali: • Packet filtering • Stateful inspection • Application inspection
Disaster Recovery	Il fornitore del servizio prevede un'architettura di disaster recovery
Business continuity	Sono adottate dal fornitore le procedure previste per garantire la BC

5. SEGNALAZIONE O RECLAMI

Nel caso in cui l'ente volesse inoltrare una segnalazione o un reclamo, previa verifica con i referenti clienti di cui al precedente capitolo 1, occorrerà inviare una comunicazione riportante in oggetto la dicitura "Segnalazione" o "Reclamo", seguita da una breve descrizione, alla casella PEC: protocollo@cert.csi.it e agli stessi referenti.

6. CONDIZIONI GENERALI DI FORNITURA

Periodo di erogazione del dal 01/01/2024 al 31/12/2024

Fatturazione: annuale anticipata a ricevimento ordine

Disdetta dei servizi:	dovrà essere formalmente comunicata entro il 31/10 di ogni anno, ed avrà effetto a decorrere dal 01/01 dell'anno successivo
Condizioni di pagamento:	30gg data ricevimento fattura, come previsto dal D.lgs. 231/02 e s.m.i. Qualora il pagamento della prestazione non sia effettuato per cause imputabili al Cliente entro il termine sopra citato, saranno dovuti gli interessi moratori ai sensi degli artt. 4 e 5 del D.Lgs. 231/02 e s.m.i, fatta salva la possibilità per il CSI-Piemonte, di rifiutare i servizi richiesti dal Cliente in caso di accertata e grave inadempienza dello stesso pagamento dei corrispettivi dei servizi oggetto della presente Offerta.
IVA:	esclusa dai prezzi indicati, a carico del Cliente

7. SICUREZZA E PROTEZIONE DEI DATI PERSONALI

I servizi oggetto della presente proposta comportano un trattamento di dati personali e/o particolari di titolarità del Cliente. In virtù di quanto prevede oggi la normativa in materia di protezione dei dati (Codice Privacy modificato dal d.lgs. 101/2018 e GDPR 2016/679), il CSI Piemonte assume il ruolo di Responsabile del trattamento dei dati relativi ai servizi oggetto dell'offerta. Le attività sui trattamenti dati sono realizzate nel rispetto dei vincoli contenuti nelle prescrizioni dell'art. 28 comma 3 del GDPR declinati per i servizi nell'Allegato "Data Protection Agreement" di seguito riportato e nella Convezione sottoscritta fra le Parti.

Di seguito si specificano alcune informazioni relative al trattamento di dati personali e alle misure tecniche ed organizzative implementate per garantire la sicurezza e la protezione dei dati personali trattati nell'ambito delle attività dettagliate nella presente offerta.

Istruzioni in materia di protezione dei dati (art 28 comma 3 punti a) - h) GDPR): tutte le specifiche contenute nel presente documento sono concordate e condivise con il Cliente e rappresentano - tutte - anche le "istruzioni" in materia di protezione dei dati personali.

Misure organizzative, tecniche, procedurali e logistiche sulla sicurezza nei trattamenti: Per garantire la disponibilità, la riservatezza, l'integrità e la tutela dei dati degli interessati, ai fini di mitigare i seguenti rischi:

- distruzione, perdita, modifica, divulgazione non autorizzata o accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati;
- trattamento dei dati non consentito o non conforme alle finalità delle operazioni di trattamento;
- interruzione della disponibilità dei dati involontaria o volontaria (dolosa);

sono implementate le misure di seguito elencate, scelte 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 gravita per i diritti e le liberta delle persone fisiche. Tutte le misure di sicurezza sono rivalutate periodicamente e ogni qualvolta si ravvede una variazione dell'efficacia delle stesse o del livello di rischio iniziale.

Misure di sicurezza organizzative:

Misura	Descrizione/Esempi
Formazione e sensibilizzazione del personale	E' definito un piano di formazione in materia di protezione dei dati per il trattamento. Sono stati eseguiti gli interventi formativi previsti dal piano
Istruzioni per il trattamento	Sono definite le istruzioni per l'esecuzione del trattamento (principi, regole da applicare nel trattamento, procedure, linee guida, manuali di organizzazione del servizio ecc..) Sono definite le procedure/istruzioni di lavoro per la gestione degli incidenti che possano comportare violazione di dati personali (data breach)
Definizione di regole di archiviazione	Sono definiti la politica e i processi di gestione dell'archivio cartaceo (consegna dei documenti, archiviazione, consultazione etc.)
Definizione del modello organizzativo	Sono definite regole e responsabilità a livello aziendale in materia di sicurezza e privacy e a livello di ruoli e responsabilità del progetto o servizio (es codice etico, profili professionali, regolamento privacy)
Audit	E' definito un piano di audit a campione sui trattamenti di dati personali

Misura	Descrizione/Esempi
Regolamentazione delle misure applicate nei rapporti con i fornitori	I contratti con i fornitori che operano sul trattamento includono le clausole privacy definite a livello aziendale per il rispetto del GDPR. Sono definite eventuali clausole e condizioni di dettaglio specifiche per il trattamento
Predisposizione di un modello per l'analisi dei rischi di privacy/sicurezza	E' definito un modello per l'analisi, la valutazione e il trattamento dei rischi di sicurezza e privacy
Documentazione del software e del servizio	Sono predisposti e aggiornati i documenti di progettazione, architettura, installazione del software utilizzato (es vista d'insieme, documento di architettura, deploy, ..) e per la gestione del servizio

Misure di sicurezza tecniche trasversali:

Misura	Descrizione/Esempi
Armadi e contenitori dotati di serrature	Sono disponibili contenitori per la conservazione sicura dotati di serratura
Armadi, cassaforti e contenitori ignifughi	Sono disponibili contenitori per la conservazione sicura ignifughi
Misure antincendio	L'edificio in cui si svolge il trattamento è dotato di misure antincendio di protezione dei beni e dei documenti
Sistemi di sorveglianza	L'edificio in cui si svolge il trattamento è dotato di misure di controllo accessi ai locali e di videosorveglianza
Gestione delle postazioni di lavoro	Sono adottate misure per ridurre la possibilità che le postazioni di lavoro (sistemi operativi, applicazioni aziendali, software per ufficio, impostazioni etc.) vengano sfruttate per violare la sicurezza dei dati personali
Utilizzo di infrastrutture sicure (hw e complementari)	Le infrastrutture hardware e i sistemi complementari sono manutenute regolarmente (es. utilizzo infrastrutture in sala CED per ospitare i servizi applicativi erogati e i dati)

Misura	Descrizione/Esempi
Infrastrutture logiche aggiornate	Le infrastrutture software (es middleware, software dei sistemi, ecc…) sono costantemente aggiornate
Antivirus	Sulle postazioni di lavoro sono installati antivirus aggiornati quotidianamente
DLP (Data Loss Prevention)	viene utilizzato sulle postazioni CSI Piemonte un sistema di DLP (data loss prevention) per tracciare operazioni quali la trasmissione e la stampa di documenti riservati dalle postazioni di lavoro
Network monitoring	Si utilizzano strumenti di packet filtering
Separazione LAN	L'infrastruttura LAN adotta la separazione tra ambienti sviluppo, test, collaudo e produzione
Protezione della navigazione web (web filtering)	Si utilizzano sistemi di web filtering per evitare l'accesso a risorse web non autorizzate
Accessi da remoto con VPN	Si utilizza il sistema/protocollo VPN per l'accesso alle risorse da remoto
Protezione perimetrale (firewall)	vengono utilizzati strumenti di protezione della rete
Protezione perimetrale di rete	vengono utilizzati strumenti di protezione degli attacchi DDoS
Protezione applicativa (WAF WEB Application Firewall)	vengono utilizzati strumenti di protezione degli applicativi WEB
Gestione Log accessi privilegiati (es. SIEM)	Si utilizzano strumenti per la gestione dei log dei sistemi. (es log dei server dei database, dei firewall, etc). Si utilizzano strumenti che permettono di correlare log in relazione ad un evento di sicurezza (es a fronte di un accesso illecito da un ip si possono correlare i log degli apparati tracciati per esaminare cosa è avvenuto)
Backup e restore	Sono disponibili servizi infrastrutturali di backup e restore. Viene periodicamente eseguito test del servizio di backup

Ulteriori misure tecniche di sicurezza applicate:

Misura	Descrizione/Esempi
Minimizzazione della quantità dei dati personali	Nel trattamento sono adottate misure per ridurre la quantità dei dati necessari quali tecniche di filtraggio e rimozione, riduzione della sensibilità attraverso la conversione, riduzione della natura identificativa del dato, riduzione dell'accumulazione, limitazione dell'accesso
Profilazione	Sono utilizzati sistemi di profilazione con un grado di sicurezza adeguato in relazione al trattamento (es sistemi di profilazione centralizzati con adeguato livello di sicurezza in relazione all'esigenza del trattamento)
Autenticazione	Si utilizza un sistema di autenticazione (locale o nazionale) con un grado di sicurezza adeguato in relazione al trattamento
Utilizzo di sistemi di autenticazione multifattore	è previsto l'uso di certificati digitali, PIN per l'autenticazione dell'utente e/o per i servizi di cooperazione applicativa
Gestione del ciclo di vita delle credenziali	E' garantita la gestione del provisioning delle credenziali di autenticazione e della profilazione (creazione, revoca, modifica di credenziali di autenticazione e di informazioni di profilazione) in particolare della scadenza della credenziale (anche in termini di gestione delle segnalazioni da sistemi centralizzati)
Tracciabilità accessi risorse	E' garantita la possibilità di tracciare accessi alle risorse critiche impiegate nel trattamento (es database, front end e back end del servizio, share di rete). Il controllo può ad esempio essere implementato per un database, andando a garantire la tracciatura dell'identificativo dell'utente che ha inserito/modificato/cancellato i dati della tabella
Audit log applicativi	L'applicazione software traccia mediante log operazioni significative compiute dagli utenti su dati personali
Abilitazioni puntuali accessi DB	Ad ogni utente che accede a dati personali su database è assegnata una credenziale univoca (es. mediante utilizzo di proxy SQL)
Minimizzazione della vulnerabilità delle risorse utilizzate nel trattamento	Sono previste opportune tecniche per ridurre la vulnerabilità delle risorse impiegate nel trattamento (es politiche di aggiornamento del software, test funzionale e di vulnerabilità del software utilizzato, limitazioni dell'accesso fisico al materiale che contiene dati personali,)

Misura	Descrizione/Esempi
Cifratura del dato	Sono adottati opportuni mezzi per cifrare i dati (in database, file, backup etc.), così come le procedure per gestire chiavi crittografiche (creazione, archiviazione, aggiornamento in caso di compromissione etc.)
Cifratura del canale	Viene utilizzato un canale cifrato per le comunicazioni mediante l'impiego di protocolli sicuri (es. HTTPS e SSH)
Pseudonimizzazione	Sono adottate tecniche che garantiscono la non attribuzione a una persona identificata o identificabile di un dato ma consentono di identificare in un secondo momento i dati anche in maniera indiretta o da remoto (es conservando separatamente le informazioni che permettono di associare la persona al dato)
Backup cifrati	Sono utilizzati sistemi per la cifratura dei backup
Business continuity/disaster recovery	Sono adottate procedure per garantire la BC e/o il DR

Le ulteriori misure tecniche sono esplicitate – ove e se necessario - nei capitoli relativi ai singoli servizi erogati.

ALLEGATO IN MATERIA DI PROTEZIONE DEI DATI

DATA PROTECTION AGREEMENT

ex art. 28 del Regolamento Europeo GDPR 679/2016
(Regolamento relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE)

Accettando l'offerta, l'ENTE Comune di Francavilla Bisio (di seguito ENTE) affida al CSI Piemonte il relativo trattamento di dati personali, sensibili (o particolari) e giudiziari di Titolarità dell'ENTE, ai sensi del D. Lgs. 196/03 e s.m.i "Codice in materia di protezione dei dati personali" così come successivamente modificato ed integrato (di seguito anche solo "Codice") e del GDPR 679/2016 Regolamento europeo in materia di privacy, (di seguito anche solo "GDPR").

L'ENTE e il CSI Piemonte si impegnano a garantire il rispetto dell'articolo 28, paragrafi 3 e 4, del GDPR, tenendo anche conto di quanto contenuto nelle *"clausole contrattuali tipo tra titolari del trattamento e responsabili del trattamento"* emanate con Decisione di Esecuzione (UE) 2021/915 della Commissione Europea del 4 giugno 2021

In particolare, l'art. 28 del GDPR attribuisce al Titolare del trattamento la facoltà di ricorrere ad un Responsabile che presenti, per esperienza, capacità ed affidabilità garanzie sufficienti per mettere in atto misure tecniche ed organizzative adeguate in modo tale che il trattamento soddisfi i requisiti previsti dalle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza e garantisca la tutela dei diritti dell'interessato.

Il CSI Piemonte, in qualità di Responsabile del trattamento dei dati personali ai sensi dell'art. 28 del GDPR e nei limiti del contesto, della durata, della natura e della finalità del trattamento, del tipo di dati personali e delle categorie di interessati indicati nella presente offerta, si impegna:

1) ad attenersi alle disposizioni previste dal Codice e dal GDPR ed operare nel rispetto dei principi espressi dalle norme in materia di trattamento di dati personali, sensibili (o particolari) e giudiziari, e in particolare dei principi di protezione dei dati sin dalla fase di progettazione e per impostazione predefinita (cd. *Privacy by design & by default*), nonché - in tutti i casi in cui vi ricorrono i presupposti - dei provvedimenti vigenti a carattere generale emanati dal Garante in materia, ed in particolare il Provv. sulle funzioni degli Amministratori di Sistema;

2) a svolgere le attività di trattamento dati, soltanto su istruzione documentata del Titolare, salvo che lo richieda una norma di legge cui è soggetto il CSI Piemonte. In tal caso, il Consorzio informa il Titolare circa tale obbligo giuridico prima del trattamento, a meno che il diritto lo vieti per rilevanti motivi di interesse pubblico. Il Titolare può anche impartire istruzioni successive per tutta la durata del trattamento dei dati personali. Tali istruzioni sono sempre documentate;

3) ad informare immediatamente il Titolare qualora, a suo parere, le istruzioni ricevute violino il GDPR o le disposizioni applicabili, nazionali o europee, relative alla protezione dei dati;

4) a adottare le misure tecniche ed organizzative di sicurezza dei dati personali e particolari concordate formalmente con il Titolare e dettagliate nell'offerta, per la protezione dalle violazioni di sicurezza che comportino accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati. Nel valutare l'adeguato livello di sicurezza, le Parti tengono debitamente conto dello stato dell'arte, dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi per gli interessati.

5) a redigere il registro delle attività di trattamento in conformità ai requisiti previsti all'art. 30 comma 2 del GDPR;

6) a non trasferire tutti o alcuni dati personali trattati verso un paese terzo o un' organizzazione internazionale, se non su istruzione del Titolare o previa autorizzazione dello stesso e fornendo in tale ultimo caso, indicazioni sulla base legale che legittima il trasferimento in conformità a quanto previsto nel capo V del GDPR;

7) in virtù della qualità del CSI Piemonte di ente strumentale per l'informatica della Pubblica Amministrazione e dell'autorizzazione generale del Titolare, a ricorrere ai sub-Responsabili presenti nella sezione "Trasparenza" del sito internet del CSI Piemonte, a cui sono affidate specifiche attività nel rispetto della disciplina sui contratti pubblici. Nel caso di eventuali modifiche riguardanti l'aggiunta o la sostituzione dei sub-Responsabili, il Consorzio informa il Titolare in merito, mediante comunicazione scritta o aggiornamento del sito, al fine di dare l'opportunità allo stesso di opporsi in conformità all'art. 28 comma 2 del GDPR. Il CSI Piemonte si impegna a selezionare sub-responsabili tra soggetti che per esperienza, capacità e affidabilità forniscano garanzie sufficienti in merito a trattamenti effettuati in applicazione della normativa pro tempore vigente e che garantiscano la tutela dei diritti degli interessati. Si impegna altresì a stipulare specifici contratti, o altri atti giuridici, in cui siano descritti analiticamente i loro compiti e imponga a tali soggetti di rispettare nella sostanza i medesimi obblighi in materia di protezione dei dati personali derivanti dalle presenti clausole. Il CSI Piemonte rimane pienamente responsabile dell'adempimento degli obblighi dei sub-responsabili, notifica al Titolare qualunque loro inadempimento e si impegna a fornire, se richiesto, copia del contratto stipulato con il sub-responsabile;

8) a concedere l'accesso ai dati personali unicamente ai soggetti autorizzati al trattamento ai sensi dell'art. 29 del GDPR nella misura strettamente necessaria per l'attuazione e la gestione delle attività oggetto dei trattamenti e a garantire che gli stessi si siano impegnati a rispettare gli obblighi di segretezza e riservatezza e abbiano ricevuto la formazione necessaria e le istruzioni dettagliate finalizzate a trattare in modo sicuro e riservato i dati affidati, custodendoli e controllandoli nel modo più appropriato;

9) tenendo conto delle informazioni a sua disposizione, dei limiti delle responsabilità previste dall'art. 28 per i Responsabili del trattamento e secondo le modalità dettagliate in specifici atti nel corso della durata della Convenzione, a coadiuvare ed assistere il Titolare nelle attività svolte per la conformità al Codice e al GDPR, ed in particolare a soddisfare i suoi obblighi di garantire:

- il rispetto dei principi di esattezza e aggiornamento dei dati;
- l'esercizio dei diritti degli interessati di cui agli artt. da 12 a 22 del GDPR, notificando prontamente al Titolare qualunque richiesta nel rispetto delle istruzioni e delle modalità di erogazione dei servizi dettagliati nelle specifiche offerte;
- la redazione o l'aggiornamento della valutazione d'impatto sulla protezione dei dati e/o la necessità di consultare preventivamente l' Autorità di Controllo;

10) a cooperare ed assistere il Titolare in caso di violazioni di dati personali nell' adempimento degli obblighi previsti dagli artt. 33 e 34 del GDPR, tenuto conto della natura del trattamento e delle informazioni a disposizione del Consorzio. In particolare, in caso di violazione di dati trattati dal CSI Piemonte, lo stesso notifica al Titolare senza ingiustificato ritardo dopo esserne venuto a conoscenza, le seguenti informazioni:

- una descrizione della natura della violazione (compresi, ove possibile, le categorie e il numero approssimativo di interessati e di registrazioni dei dati in questione);
- i recapiti di un punto di contatto presso il quale possono essere ottenute maggiori informazioni sulla violazione dei dati personali;
- le probabili conseguenze della violazione dei dati personali e le misure adottate o di cui si propone l'adozione per porre rimedio alla violazione, anche per attenuarne i possibili effetti negativi.

Qualora, e nella misura in cui, non sia possibile fornire tutte le informazioni contemporaneamente, la notifica iniziale contiene le informazioni disponibili in quel momento, e le altre informazioni sono fornite successivamente, non appena disponibili, senza ingiustificato ritardo.

11) a rispondere alle richieste di informazioni del Titolare e a fornire tutte le informazioni e la documentazione necessaria al fine di dimostrare il rispetto degli obblighi previsti dal Codice e dal GDPR consentendo, a intervalli ragionevoli, attività di ispezione, audit o riesame delle attività, anche in caso di inosservanza. A tal fine, il Titolare può tenere conto delle pertinenti certificazioni in possesso del CSI Piemonte e può scegliere di condurre l'attività di revisione autonomamente o incaricare un revisore indipendente. Le attività di revisione possono comprendere anche ispezioni nei locali o nelle strutture fisiche del Consorzio e, se del caso, sono effettuate con un preavviso ragionevole. Su richiesta, le Parti mettono a disposizione delle autorità competenti le informazioni di cui alla presente clausola, compresi i risultati di eventuali attività di revisione;

12) per quanto di competenza, a prestare tutta la collaborazione necessaria a fronte di richieste di informazioni, controlli, ispezioni ed accessi da parte del Garante o di altre pubbliche autorità competenti (informando contestualmente il Titolare con la massima celerità);

13) in caso di contestazione di una violazione degli obblighi di cui sopra e su richiesta del Titolare, a sospendere immediatamente il trattamento dei dati personali a cui tale contestazione si riferisce e ad informare prontamente il Titolare in merito al fatto di essere in grado o meno di rispettare tali obblighi, al fine di consentire al Titolare di intraprendere, entro un termine ragionevole, le misure necessarie, a tutela del trattamento dei dati;

14) a sospendere il trattamento di dati personali nel caso in cui, dopo aver informato il Titolare che le sue istruzioni violano i principi previsti dal GDPR, lo stesso insista sul rispetto delle istruzioni;

15) al termine del trattamento, a restituire o cancellare i dati del Titolare sulla base della sua scelta formale, certificandone la cancellazione delle copie, fatto salvo il caso in cui una norma di legge non ne preveda la conservazione.