Allegato al contratto Cliente SaaS

Misure di sicurezza per il trattamento dei dati personali e misure "Tecnico-organizzative"

TRA

Open Software S.r.l., in seguito denominato "Fornitore", con sede in Via Galielo Galilei n. 2/c/2 - 30035 Mirano (VE), partita IVA 02810000279 in atti legalmente rappresentata dal Sig. MILANESE NICOLA in qualità di Legale Rappresentante

E

i fruitori dei servizi SaaS per il software applicativo Visual Polcity Cloud, di seguito denominato "Cliente"

PREMESSO CHE

a) Il Cliente ha sottoscritto uno o più contratti (di seguito il "Contratto") con il Fornitore (CSP);

b) Il Cliente e il Fornitore hanno disciplinato le condizioni e le modalità del trattamento dei dati personali eseguito dal Fornitore nell'ambito del Contratto quale Responsabile del trattamento dei dati personali ai sensi dell'art. 28 del Regolamento generale europeo sulla protezione dei dati del 27 aprile 2016 n. 679 (nel seguito "GDPR");

c) I dati personali trattati dal Fornitore sono di proprietà del Cliente;

d) L'accesso ai dati personali trattati dal Fornitore è consentito solo a incaricati e Responsabili del trattamento che abbiano ricevuto una adeguata formazione e forniscano garanzie sull'applicazione di adeguate misure di sicurezza in merito al trattamento dei dati;

e) Il Fornitore dichiara che i dati saranno trattati utilizzando Data Center siti all'interno della Comunità Europea;

f) Nell'ambito dell'erogazione dei servizi cloud, il Fornitore si configura come Cloud Service Providers (CSP) o Data Processor dei Dati Personali nel cloud pubblico per i propri clienti. Il Fornitore si impegna a rispettare la legislazione cogente applicabile in materia di protezione dei dati personali e le condizioni contrattuali concordate tra il Data Processor dei Dati Personali nel cloud pubblico e i clienti (CSC), applicando le disposizioni previste dal Regolamento UE 679/20016 e dal D.Lgs. 196/2003 e s.m.i..

Tutto quanto sopra premesso le Parti convengono quanto segue:

1. DEFINIZIONI

1.1 Definizioni:

- CSC (Cloud Service Customer): Cliente del Servizio Cloud;
- CSP (Cloud Service Provider): Fornitore del Servizio Cloud;

1.2. Le Parti riconoscono e convengono che il CSP agisce quale Responsabile del trattamento in relazione ai Dati Personali e il CSC agisce di regola quale Titolare del trattamento dei Dati Personali.

1.3. SUB-RESPONSABILE:

1.3.1 Quando un CSP offre un servizio cloud che dipende da un CSP terzo, lo stesso si configura come Responsabile o sub responsabile del trattamento dei dati.

1.3.2 Qualora il CSC svolga operazioni di trattamento per conto di altro Titolare, il CSC potrà agire come Responsabile del trattamento. In tal caso, il CSC garantisce che le istruzioni impartite e le attività intraprese in relazione al trattamento dei Dati Personali, inclusa la nomina, da parte del CSC, del CSP quale Sub-Responsabile del trattamento, derivante dall'accettazione del presente allegato, sono state autorizzate dal relativo Titolare del trattamento e si impegna ad esibire al CSP, a seguito di richiesta scritta, la documentazione attestante quanto sopra.

1.4. Ciascuna delle Parti si impegna a conformarsi, nel trattamento dei Dati Personali, ai rispettivi obblighi derivanti dalla Legislazione in materia di Protezione dei Dati Personali applicabile.

1.5. Il CSP ha nominato un Responsabile della protezione dei dati (DPO), domiciliato presso la sede del CSP, che può essere contattato al seguente indirizzo e-mail: privacy@opensoftware.it

2. TRATTAMENTO DEI DATI PERSONALI

2.1. Con la stipula del presente Accordo il Cliente affida al CSP l'incarico di trattare i Dati Personali ai fini della prestazione dei Servizi.

2.2. Il CSP si impegna a conformarsi alle Istruzioni ricevute, fermo restando che, qualora il CSC richieda variazioni, il CSP valuterà gli aspetti di fattibilità e concorderà con il CSC le predette variazioni ed i costi connessi.

2.3. Nei casi di cui all'art. 2.2 e in caso di richieste del CSC che comportino il trattamento di Dati Personali che siano, ad avviso del CSP, in violazione della Legislazione in materia di Protezione dei Dati Personali, il CSP è autorizzato ad astenersi dall'eseguire tali Istruzioni e ne informerà prontamente il CSC. In tali casi il CSC potrà valutare eventuali variazioni alle Istruzioni impartite o contattare l'Autorità di controllo per verificare la liceità delle richieste avanzate.

2.4. In caso di eventuali ispezioni o richieste di informazioni presentate da Autorità di controllo e forze di Polizia, il CSP è tenuto a fornire alle stesse le informazioni richieste, ottemperando ai propri obblighi in osservanza alle indicazioni di riservatezza ricevute per il trattamento dei Dati Personali.

3. LIMITAZIONI ALL'UTILIZZO DEI DATI PERSONALI

3.1. Il CSP si impegna a non trattare i Dati Personali ricevuti per scopi diversi da quelli specificati e definiti nel presente accordo, garantendo la piena applicazione delle istruzioni generali ricevute dal CSC. Il CSP assicura che le informazioni personali trattate nell'ambito del contratto, non saranno utilizzate per scopi di marketing e/o pubblicitario, senza previo consenso scritto da parte dell'interessato.

3.2. Il Personale del CSP che accede, o comunque tratta i Dati Personali, è preposto al trattamento di tali dati sulla base di idonee autorizzazioni e ha ricevuto la necessaria formazione anche in merito al loro trattamento. Tale personale è altresì vincolato dalle policy di riservatezza e di protezione dei dati personali adottate dal CSP.

4. AFFIDAMENTO A TERZI

4.1. In relazione all'affidamento a Responsabili del Trattamento dei dati le Parti convengono quanto segue:

4.1.1. Il CSC acconsente all'affidamento di operazioni di Trattamento dei Dati Personali ad eventuali soggetti terzi preventivamente qualificati: l'elenco di tali soggetti sarà reso disponibile su richiesta.

5. DISPOSIZIONI IN MATERIA DI SICUREZZA

5.1. **MISURE DI SICUREZZA DEL FORNITORE (CSP)** – Il CSP ha adottato un Sistema di Gestione della Qualità conforme alla norma UNI EN ISO 9001:2015 e un Sistema di Gestione della Sicurezza delle Informazioni (SGSI) in conformità alle norme UNI CEI EN ISO/IEC 27001:2017, UNI CEI EN ISO/IEC 27002:2017, ISO/IEC 27017:2015, ISO/IEC 27018:2020 e UNI CEI EN ISO/IEC 27701:2021. Nell'eseguire il trattamento dei Dati Personali ai fini della prestazione dei servizi applica quindi misure tecnico-organizzative adeguate a evitare il trattamento illecito o non autorizzato, la distruzione accidentale o illecita, il danneggiamento, la perdita accidentale, l'alterazione e la divulgazione non autorizzata o l'accesso ai Dati Personali.

A titolo non esaustivo si riportano di seguito le principali misure di sicurezza adottate:

- Firewall, IDPS - I dati personali sono protetti contro il rischio d'intrusione di cui all'art. 615-quinquies del Codice Penale mediante sistemi di Intrusion Detection & Prevention mantenuti aggiornati in relazione alle migliori tecnologie disponibili.

- Sicurezza linee di comunicazione - Per quanto di propria competenza, sono adottati dal Fornitore protocolli di comunicazione sicuri e in linea con quanto la tecnologia rende disponibile.

- Protection from malware – I sistemi sono protetti contro il rischio di intrusione e dell'azione di programmi mediante l'attivazione di idonei strumenti elettronici aggiornati con cadenza periodica.

- Credenziali di autenticazione – I sistemi sono configurati con modalità idonee a consentirne l'accesso unicamente a soggetti dotati di credenziali di autenticazione che ne consentono la loro univoca identificazione.

- Logging – I sistemi sono configurati con modalità che consentono il tracciamento degli accessi e, ove appropriato, delle attività svolte in capo alle diverse tipologie di utenze (amministratore, utente, etc.) protetti da adeguate misure di sicurezza che ne garantiscono l'integrità. **Tutti i log di tracciamento degli accessi sono conservati nel rispetto delle normative di riferimento per un periodo non inferiore ai sei mesi e non superiore a sei anni.**

- Backup & Restore – Sono adottate idonee misure per garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati. Idonea documentazione dettaglia le modalità e le misure e può essere richiesta in visione se pertinente al servizio offerto e previa sottoscrizione di opportune clausole di riservatezza.

- I dati di backup sono disponibili per un periodo di 30 giorni.

- È posto in uso un Piano di continuità operativa integrato con il Piano di Disaster Recovery; essi garantiscono la disponibilità e l'accesso ai sistemi anche nel caso di eventi negativi di portata rilevante che dovessero perdurare nel tempo.

- Al fine di garantire la continuità operativa, il CSP provvede ad effettuare regolari attività di manutenzione del sistema informativo aziendale e ad eseguire periodici test di verifica del corretto funzionamento delle attrezzature in uso.

Il CSP esegue regolarmente le attività di manutenzione del software, dandone preventiva comunicazione al CSC e garantendo l'adozione delle seguenti misure tecniche:

- **Le attività di sviluppo software sono attuate da parte del CSP utilizzando prevalentemente risorse interne che garantiscono un controllo continuo delle attività svolte. Lo Sviluppo sicuro del software è attuato applicando le best practices in materia di sicurezza applicativa per una buona ingegnerizzazione del software, che consente di valutare le minacce e vulnerabilità più comuni in ogni fase del ciclo di sviluppo, secondo quanto previsto dalle Linee Guida per l'adozione di un ciclo di sviluppo del software sicuro di AgiD.**

- Ogni attività di manutenzione, ordinaria o straordinaria si traduce nel rilascio di una nuova versione del software. La nuova versione del software è identificata dal numero di versione. Ogni nuova versione del software possiede un "changelog", cioè un documento che elenca le modifiche apportate nella nuova versione, classificate in nuove funzionalità e correzione di problemi.

- I tempi e le modalità di installazione della nuova versione vengono preventivamente concordati con il responsabile IT del CSC. Su richiesta del CSC la nuova versione può essere rilasciata preventivamente in un ambiente demo prima di essere installata in ambiente di produzione.

- Le attività di manutenzione ordinaria vengono eseguite "a caldo" ovvero senza interruzione del servizio, tuttavia la fase di manutenzione potrebbe causare un sovraccarico del sistema che comporta dei rallentamenti; il periodo di sovraccarico può durare da pochi secondi a 1 ora.

- Ogni nuova versione del software prima di essere rilasciata viene verificata, controllando la corretta esecuzione della nuova versione del software nonché l'aderenza ai requisiti oggetto dell'attività di manutenzione.

- Quando la nuova versione del software viene effettivamente rilasciata nell'ambiente di produzione del CSC, il responsabile IT del CSP provvede a segnalarlo al CSC.

5.1.1. Qualora il CSC richieda di adottare misure di sicurezza aggiuntive, il CSP si riserva il diritto di valutarne la fattibilità.

5.1.2. Il CSC riconosce e accetta che il CSP, tenuto conto della natura dei Dati Personali e delle informazioni disponibili al CSP stesso, presterà assistenza al CSC nel garantire il rispetto degli obblighi di sicurezza di cui agli artt. 32-34 del GDPR nei modi seguenti:

5.1.2.1. Implementando e mantenendo aggiornate le Misure di Sicurezza secondo quanto previsto al precedente punto 5.1 conformandosi agli obblighi di cui al punto 5.3.

5.1.3. Qualora il prodotto consenta l'integrazione con applicativi di terze parti, il CSP non sarà responsabile dell'applicazione delle Misure di Sicurezza relative alle componenti delle terze parti o delle modalità di funzionamento del prodotto derivanti dall'integrazione effettuata dalle terze parti.

5.2. **MISURE DI SICUREZZA DEL CLIENTE (CSC)** – Il CSC riconosce e accetta che, nella fruizione dei Servizi, rimane sua responsabilità esclusiva l'adozione di adeguate misure di sicurezza in relazione alla fruizione dei Servizi da parte del proprio personale e di coloro che sono autorizzati ad accedere a detti Servizi.

5.3. **VIOLAZIONI DI SICUREZZA** – Fatta eccezione per il caso di Contratti aventi ad oggetto prodotti installati presso il CSC o presso fornitori del CSC per i quali non trova applicazione il presente punto 5.3, qualora il CSP venga a conoscenza di una Violazione di Sicurezza dei Dati Personali (Data Breach), dovrà:

5.3.1. informare il CSC, senza ingiustificato ritardo e ove possibile entro 72 ore dal momento in cui ne sia venuto a conoscenza, mediante specifica comunicazione inoltrata con e-mail di notifica;

5.3.2. adottare ulteriori misure per limitare i possibili danni e la sicurezza dei Dati Personali;

5.3.3. fornire al CSC, per quanto possibile, una descrizione della Violazione della Sicurezza dei Dati Personali ivi incluse le misure adottate per evitare o mitigare i potenziali rischi e le attività raccomandate dal CSP al CSC per la gestione della Violazione di Sicurezza;

5.3.4. ai sensi di quanto previsto nel Contratto, considerare informazioni Confidenziali quelle attinenti le eventuali Violazioni della Sicurezza, i relativi documenti, comunicati e avvisi, non comunicare a terzi tali informazioni, fuori dai casi strettamente necessari all'assolvimento degli obblighi del CSC derivanti dalla Legislazione in materia di Protezione dei Dati Personali, senza il previo consenso scritto del Titolare del Trattamento.

5.4. Nei casi di cui al precedente punto 5.3, è responsabilità esclusiva del CSC adempiere agli obblighi di notificazione della Violazione di Sicurezza ai terzi (all'Utente Finale qualora il CSC sia un Responsabile del Trattamento); e se il CSC è Titolare del Trattamento all'Autorità di controllo e agli interessati.

5.5. Il CSC dovrà comunicare tempestivamente al CSP eventuali utilizzi impropri degli account o delle credenziali di autenticazione oppure eventuali Violazioni di Sicurezza di cui abbia avuto conoscenza riguardanti i Servizi.

5.6 Il CSP applica un controllo sugli incidenti in base a quanto stabilito da uno specifico piano di Disaster Recovery e Business Continuity. Le responsabilità risultano definite per tutte le attività richieste. È stata predisposta apposita procedura per la segnalazione dei "Data breaches" secondo quanto previsto dal Regolamento UE privacy. Con cadenza annuale viene pubblicata sul sito internet la statistica degli incidenti e su richiesta del CSC viene fornito lo specifico piano dei test di simulazione attuati per garantire la sicurezza del sistema informativo aziendale.

5.7 Il CSP svolge periodicamente attività di Vulnerability Assestment (VA) e Penetration Test (PT).

5.8 In riferimento ai punti 5.6 e 5.7 eventuali informazioni aggiuntive saranno date a seguito di sottoscrizione di apposite Clausole di Riservatezza, inviando formale richiesta all'indirizzo e-mail info@opensoftware.it.

6. LIMITAZIONI AL TRASFERIMENTO DEI DATI PERSONALI AL DI FUORI DELLO SPAZIO ECONOMICO EUROPEO (SEE)

6.1. Il CSP non trasferirà i Dati Personali al di fuori dello SEE senza darne preventiva comunicazione al CSC.

7. VERIFICHE E CONTROLLI

7.1. Il CSP sottopone ad audit periodici la sicurezza dei sistemi e degli ambienti di elaborazione dei Dati Personali dallo stesso utilizzati per l'erogazione dei Servizi e le sedi in cui avviene tale trattamento. Il CSP avrà la facoltà di incaricare dei professionisti indipendenti selezionati dal CSP per lo svolgimento di audit secondo standard internazionali e/o best practice, i cui esiti saranno riportati in specifici report ("Report"). Tali Report, che costituiscono informazioni confidenziali del CSP, potranno essere resi disponibili al CSC per consentirgli di verificare la conformità dei servizi offerti dal CSP agli obblighi di sicurezza di cui al presente Accordo.

7.2. Il CSP riconosce il diritto del CSC, con le modalità e nei limiti di seguito indicati, ad effettuare audit indipendenti per verificare la conformità del CSP agli obblighi previsti nel presente Accordo e di quanto previsto dalla normativa. Il CSC potrà avvalersi per tali attività di proprio personale specializzato o di valutatori esterni, purché tali soggetti siano previamente vincolati da idonei impegni alla riservatezza.

7.3. Nel caso di cui al precedente punto 7.2 il CSC dovrà preventivamente inviare richiesta scritta al Responsabile della Protezione dei Dati (DPO) del CSP. Successivamente alla richiesta di audit o ispezione il CSP e il CSC concorderanno, prima dell'avvio delle attività, i dettagli di tali verifiche (data di inizio e durata), le tipologie di controllo e l'oggetto delle verifiche, i vincoli di riservatezza a cui devono essere vincolati il CSC e coloro che effettuano le verifiche e i costi che il CSP potrà addebitare per tali verifiche e che saranno determinati in relazione all'estensione e alla durata delle attività di verifica.

7.4. Il CSP potrà opporsi per iscritto alla nomina da parte del CSC di eventuali valutatori esterni che siano, ad insindacabile giudizio del CSP, non adeguatamente qualificati o indipendenti, siano concorrenti del CSP o che siano evidentemente inadeguati. In tali circostanze il CSC sarà tenuto a nominare altri valutatori o a condurre le verifiche in proprio.

7.5. Il CSC si impegna a corrispondere al CSP gli eventuali costi calcolati dal CSP e comunicati al CSC nella fase di cui al precedente punto 7.3, con le modalità e nei tempi ivi concordati. Restano a carico esclusivo del CSC i costi delle attività di verifica dallo stesso commissionate a terzi.

7.6. Il presente punto 7 non è applicabile ai Contratti aventi ad oggetto prodotti installati presso il CSC o presso fornitori del CSC.

7.7. Le attività di verifica che interessino eventuali Sub-Responsabili dovranno essere svolte nel rispetto delle regole di accesso e delle politiche di sicurezza degli stessi.

8. ASSISTENZA A FINI DI CONFORMITÀ

8.1. Il CSP presterà assistenza al CSC e coopererà nei modi di seguito indicati al fine di consentire al CSC il rispetto degli obblighi previsti dalla Legislazione in materia di Protezione dei Dati Personali.

8.2. Qualora il CSP riceva richieste o reclami da un Interessato in relazione ai Dati Personali, il CSP raccomanderà all'Interessato di rivolgersi al CSC o all'Utente Finale, nel caso in cui quest'ultimo sia il Titolare del Trattamento. In tali casi il CSP informerà tempestivamente il CSC del ricevimento della richiesta mediante invio di e-mail di notifica e fornirà al CSC le informazioni ad esso disponibili unitamente a copia della richiesta o del reclamo. Resta inteso che tale attività di cooperazione **sarà svolta in via eccezionale, in quanto la gestione dei rapporti con gli Interessati resta esclusa dai Servizi ed è responsabilità del CSC** gestire eventuali reclami in via diretta e garantire che il punto di contatto per l'esercizio dei diritti da parte degli Interessati sia il CSC stesso, o l'Utente Finale se Titolare del Trattamento. Sarà responsabilità del CSC, o dell'Utente Finale qualora questi sia Titolare del Trattamento, provvedere a dar seguito a tali richieste o reclami.

8.3. Il CSP provvederà a informare tempestivamente il CSC, salvo il caso in cui ciò sia vietato dalla legge, con avviso all'e-mail di notifica di eventuali ispezioni o richieste di informazioni presentate da Autorità di controllo e forze di Polizia rispetto a profili che riguardano il trattamento dei Dati Personali.

8.4. Qualora, ai fini dell'evasione delle richieste di cui ai precedenti punti, il CSC abbia necessità di ricevere informazioni dal CSP circa il trattamento dei Dati Personali, il CSP presterà la necessaria assistenza nei limiti di quanto ragionevolmente possibile, a condizione che tali richieste siano presentate con un congruo preavviso di almeno 15 giorni.

8.5. Il CSP, tenuto conto della natura dei Dati Personali e delle informazioni ad esso disponibili, fornirà assistenza al CSC nel rendere disponibili informazioni utili per consentire al CSC l'effettuazione di valutazioni di impatto sulla protezione dei Dati Personali nei casi previsti dalla legge. In tal caso il CSP renderà disponibili informazioni di carattere generale in base al Servizio, quali le informazioni contenute nel Contratto di fornitura e nel presente Accordo. Eventuali richieste di assistenza personalizzate potranno essere soggette al pagamento di un corrispettivo da parte del CSC. Resta inteso che è responsabilità e onere esclusivo del CSC, o dell'Utente Finale se Titolare del trattamento, procedere alla valutazione di impatto in base alle caratteristiche del trattamento dei Dati Personali dallo stesso posto in essere nel contesto dei Servizi.

8.6. Il CSP si impegna a rendere Servizi improntati ai principi di minimizzazione del trattamento, fermo restando che è responsabilità esclusiva del CSC, o dell'Utente Finale, se Titolare del Trattamento, assicurare che il trattamento sia condotto poi concretamente nel rispetto di detti principi.

9. OBBLIGHI DEL CSC E LIMITAZIONI

9.1. Il CSC si impegna a impartire al proprio personale istruzioni conformi alla normativa e a utilizzare i servizi in modo conforme alla Legislazione in materia di Protezione dei Dati Personali.

9.2. Qualora il rilascio dell'informativa e l'ottenimento del consenso debbano avvenire per il tramite del prodotto oggetto del Contratto, il CSC dichiara di aver valutato il prodotto e che esso risponda alle proprie esigenze. Resta altresì a carico del CSC valutare se l'eventuale modulistica resa disponibile dal CSP per agevolare l'assolvimento degli obblighi di informativa e consenso (es. modello di privacy policy per App o informative presenti negli applicativi), sia conforme alla Legislazione in materia di Protezione dei Dati Personali e adattare la stessa alle proprie esigenze, ove ritenuto opportuno.

9.3. È onere del CSC mantenere l'account collegato all'e-mail di notifica, attivo ed aggiornato.

9.4. Il CSC prende atto che, ai sensi dell'art. 30 del GDPR, il CSP è tenuto a mantenere un Registro delle attività di trattamento eseguite per conto dei Titolari (o Responsabili) del Trattamento e a raccogliere a tal fine i dati identificativi e di contatto di ciascun Titolare (e/o Responsabile) del Trattamento per conto del quale il CSP agisce e che tali informazioni devono essere rese disponibili all'autorità competente, su richiesta. Pertanto, quando richiesto, il CSC si impegna a dare al CSP i dati identificativi e di contatto sopra indicati con le modalità individuate dal CSP nel tempo e a mantenere aggiornate tali informazioni tramite i medesimi canali.

10. DURATA

10.1. Il presente Accordo avrà efficacia dalla Data di Decorrenza del contratto e cesserà automaticamente, alla data di cancellazione di tutti i Dati Personali da parte del CSP, come previsto nel presente Accordo.

11. DISPOSIZIONI PER LA RESTITUZIONE O LA CANCELLAZIONE DEI DATI PERSONALI

11.1. Alla cessazione del Servizio, per qualunque causa intervenuta, il CSP cesserà ogni trattamento dei Dati Personali e:

11.1.0. provvederà alla restituzione al CSC di tutti i Dati Personali afferenti al servizio SaaS e a disattivare le credenziali di accesso al servizio stesso entro 10 giorni lavorativi.

11.1.1. provvederà alla cancellazione dei Dati Personali (ivi incluse eventuali copie) dai sistemi del CSP o da quelli su cui lo stesso abbia controllo entro il termine previsto 30 giorni, tranne il caso in cui la conservazione dei dati da parte del CSP sia necessaria al fine di assolvere ad una disposizione di legge;

11.1.2. distruggerà eventuali Dati Personali conservati in formato cartaceo in suo possesso, tranne il caso in cui la conservazione dei dati da parte del CSP sia necessaria ai fini del rispetto di norme di legge;

11.1.3. manterrà a disposizione del CSC i Dati Personali per l'estrazione per il periodo di 30 giorni successivi alla cessazione del Contratto. Durante tale periodo, il trattamento sarà limitato alla sola conservazione finalizzata a mantenere i Dati Personali a disposizione del CSC per l'estrazione, di cui al punto 11.2.

11.2. Fermo restando quanto altrimenti previsto nel presente Accordo, il CSC riconosce di poter estrarre i Dati Personali, alla cessazione del Servizio e conviene che è sua responsabilità provvedere all'estrazione totale o parziale dei soli Dati Personali che ritenga utile conservare e che tale estrazione dovrà essere effettuata prima della scadenza del termine di cui al punto 11.1.3.

11.3. Resta inteso che quanto previsto ai punti 11.1 e 11.2 non si applica ai Contratti aventi ad oggetto prodotti installati presso il CSC o presso fornitori del CSC. In tali casi, è responsabilità del CSC estrarre i Dati Personali che ritenga utile conservare; il CSC riconosce che successivamente al predetto termine i Dati Personali potrebbero non essere più accessibili. Nei casi di cui al presente punto 11.3 resta altresì responsabilità del CSC provvedere alla cancellazione dei Dati Personali nel rispetto delle norme di legge.

Data, 3 gennaio 2023

Firma CSP

Open Software S.r.l.