

Matelica, 30-07-2021

Spett.le
COMUNE DI CASCIA

**ALLA C.A.
SIG.RA LATTANZI PATRIZIA**

OGGETTO: Offerta n. 170 del 30-07-2021 per Ced Remoto, Secure Box, Storage, White Box

Con la presente abbiamo il piacere di sottoporre alla Vostra cortese attenzione l'offerta economica, relativa ai servizi richiesti.

Il nostro impegno su oltre 3.400 enti pubblici e 40 anni di esperienza nel settore sistemistico, Vi garantiscono la massima affidabilità nella scelta di una soluzione unica, che consente all'Ente di lavorare in sicurezza ed efficienza, con la massima qualità del servizio.

La Halley Sistemistica è azienda leader per gli enti pubblici a livello sistemistico, con un team di oltre 60 persone e si distingue per: competenze, capacità organizzative, struttura, qualità dell'assistenza da remoto e sul posto, tempestività di intervento, innovazione e distribuzione sul territorio, poiché offre soluzioni complete con formule "zero pensieri".

Restando a Vostra disposizione per ulteriori informazioni, cogliamo l'occasione per porgerVi i nostri migliori saluti.

Halley Informatica s.r.l.
Moreno Pascucci
Consulente tecnico - commerciale
HALLEY sistemistica
cell. 346-3108883
www.halleysistemistica.it

Servizio Storage

Art. 1 - Servizi offerti

1.1 ARCHIVIAZIONE DATI

Halley garantisce la corretta ed automatica archiviazione dei dati presenti nei NAS (Network Area Storage).

1.2 RIDONDANZA DEI DATI

Halley garantisce il costante e corretto allineamento delle archiviazioni su entrambi i NAS.

Art. 2 - Impegni Halley

2.1 ARCHIVIAZIONE DATI

Halley si impegna a controllare da remoto la corretta archiviazione dei dati presenti nei NAS. In caso di malfunzionamento dei NAS o dell'archiviazione dei dati, Halley provvederà tempestivamente alla risoluzione del problema.

2.2 RIDONDANZA DEI DATI

Halley si impegna a controllare da remoto il costante e corretto allineamento dei dati nei due NAS. In caso di problemi nell'allineamento dei dati, Halley provvederà tempestivamente alla risoluzione del problema.

Art. 3 - Impegni del Cliente

3.1 ARCHIVIAZIONE DATI

Si rimanda a: *"Condizioni generali di protezione dati"* art. 3.3 e art. 4.

3.2 RIDONDANZA DEI DATI

Si rimanda a: *"Condizioni generali di protezione dati"* art. 3.3 e art. 4.

Art. 4 - Ottemperanza ai requisiti di legge

4.1 PROTEZIONE DEI DATI

Il presente servizio garantisce al Cliente l'adozione di procedure per la custodia di copie di sicurezza e il ripristino della disponibilità dei dati e dei sistemi.

4.2 MISURE DI SICUREZZA CONTRO INTRUSIONI ED ACCESSI ABUSIVI

I dati contenuti nei Nas sono inoltre protetti contro il rischio di intrusione ed accessi abusivi mediante l'utilizzo da parte di Halley di strumenti ragionevolmente sicuri per accedere e svolgere attività sugli apparati come indicato nelle *"Condizioni generali di protezione dati"* art. 6.1 della presente offerta a cui si rimanda.

L'archiviazione dati è protetta da password alfanumerica di minimo otto caratteri, contenente un carattere speciale e almeno una lettera maiuscola.

4.3 CONFORMITA' ALLE MISURE MINIME DI SICUREZZA ICT

Il servizio è conforme alla circolare AGID del 18 aprile 2017, n. 2/2017 contenente le "Misure minime per la sicurezza ICT delle pubbliche amministrazioni". In particolare i Server e le Workstation che hanno attivo il servizio:

- Copiano giornalmente le cartelle condivise scelte dal cliente mantenendo uno storico di 60 giorni (ABSC 10.1.1 all.1 circolare Agid n. 2/2017);
- Hanno password amministrative complesse (ABSC 5.7.2 all.1 circolare Agid n. 2/2017).

4.4 MISURE DI SICUREZZA IN CONFORMITA' AL REGOLAMENTO COMUNITARIO 679/2016 (GDPR)

Si rimanda a: *"Condizioni generali di protezione dati"* art. 10.

In particolare:

Contro i rischi di distruzione, perdita e modifica dei dati il Servizio Storage garantisce:

- L'archiviazione dei dati protetta da password secondo attuali standard;
- Il controllo effettuazione copia, con uno storico di 28 giorni;
- Che i backup avvengano ad intervalli di 3 giorni (domenica e giovedì) su entrambi i NAS;
- NAS ridondati e ampliabili;
- La non modificabilità del backup dei dati;
- Accessi limitati ai soli utenti che abbiano le competenze adeguate e la necessità operativa di modificare la configurazione dei sistemi;
- La sostituzione di password standard di amministratore con password complesse;
- Password amministrative complesse.

Servizio Secure Box

Art. 1 - Servizi offerti

1.1 PROTEZIONE DELLA RETE

Halley offre una ragionevole sicurezza della rete del Cliente proteggendola sia da rischi esterni (attacchi hacker, virus, Criptolocker o frodi informatiche), sia da rischi interni (semplice inserimento su PC di chiave usb contenente virus).

1.2 ANTIVIRUS

Halley garantisce la fornitura dell'antivirus ed i relativi aggiornamenti (versione, definizioni) sia sul firewall fornito che su tutti i pc inclusi nel servizio.

Gli aggiornamenti vengono effettuati sia tramite il software del firewall fornito, sia tramite un software che mantiene aggiornate versioni e definizioni.

1.3 CONTROLLO DEL FILTRAGGIO DEI CONTENUTI

Halley garantisce, su richiesta del Cliente, la fornitura di un software per il blocco di siti o categorie di siti non attinenti alle attività del Cliente (es. social network, giochi d'azzardo, etc.). L'elenco delle categorie è costantemente aggiornato ed è personalizzabile dal Cliente.

Gli aggiornamenti vengono effettuati tramite il software del firewall fornito.

1.4 PROTEZIONE WEB

Halley garantisce, tramite il software del firewall fornito, la protezione da contenuti malevoli (es siti malware, phishing, etc.). L'elenco dei contenuti è costantemente aggiornato.

Gli aggiornamenti vengono effettuati tramite il software del firewall fornito.

1.5 ANTISPAM

Halley garantisce, tramite il software del firewall fornito, un blocco di quasi il 100% delle mail indesiderate e pericolose.

Art. 2 - Impegni Halley

2.1 PROTEZIONE DELLA RETE

Halley si impegna a mantenere sempre aggiornata da remoto la configurazione del Firewall.

In caso di malfunzionamento, provvederà tempestivamente alla risoluzione del problema.

2.2 ANTIVIRUS

Halley si impegna a rilevare ed eliminare eventuali virus (all'occorrenza anche in intervento) ed a mantenere costantemente aggiornate le versioni e le definizioni dell'antivirus.

2.3 CONTROLLO DEL FILTRAGGIO DEI CONTENUTI

Halley si impegna a garantire il corretto funzionamento del servizio.

2.4 PROTEZIONE WEB

Halley si impegna a garantire il corretto funzionamento del servizio.

2.5 ANTISPAM

Halley si impegna a garantire il corretto funzionamento del servizio.

Art. 3 - Impegni del Cliente

3.1 PROTEZIONE DELLA RETE LAN (Local Area Network)

Si rimanda a: *"Condizioni generali di protezione dati"* art. 3.3 e art. 4

3.2 ANTIVIRUS

Il Cliente si impegna a non interferire con il regolare funzionamento dell'antivirus.

Si rimanda a: *"Condizioni generali di protezione dati"* art. 4

3.3 CONTROLLO DEL FILTRAGGIO DEI CONTENUTI

Il Cliente si impegna, se lo desidera, ad indicare ad Halley quali siti e/o categorie di siti intende bloccare. Qualora il Cliente in un secondo momento desiderasse bloccare altre categorie di siti, dovrà darne comunicazione ad Halley tramite i canali standard di assistenza.

Il Cliente si impegna a non interferire con il regolare funzionamento dell'antivirus.

Si rimanda a: *"Condizioni generali di protezione dati"* art. 4

3.4 PROTEZIONE WEB

Il Cliente si impegna a non interferire con il regolare funzionamento dell'antivirus.

Si rimanda a: *"Condizioni generali di protezione dati"* art. 4

3.5 ANTISPAM

Il Cliente si impegna a non interferire con il regolare funzionamento dell'antivirus.

Si rimanda a: *"Condizioni generali di protezione dati"* art. 4

Art. 4 - Ottemperanza ai requisiti di legge

4.1 PROTEZIONE DELLA RETE LAN

Nel rispetto degli obblighi di sicurezza di cui al D.Lgs. 196/2003 e s.m.i. e al Regolamento UE 679/2016, il Servizio Secure Box contribuisce a garantire la sicurezza della rete informatica del Cliente attraverso l'esclusiva apertura di porte necessarie al Cliente stesso, evitando l'apertura di porte in entrata (WAN to LAN) ed impedendo al Cliente l'accesso a siti ritenuti malevoli.

4.2 ANTIVIRUS

In attuazione delle misure di sicurezza di cui al D.Lgs 196/2003 e s.m.i. e al Regolamento UE 679/2016, il presente Servizio contribuisce ad assicurare la protezione del sistema e dei dati contenuti nei PC del Cliente rispetto a determinati programmi informatici, garantendo la fornitura dei più accreditati firewall e antivirus sul mercato e la corretta e costante esecuzione degli aggiornamenti.

4.3 CONTROLLO DEL FILTRAGGIO DEI CONTENUTI E PROTEZIONE WEB

Per quanto concerne *Internet* e la *navigazione web* il Garante della Privacy, mediante le linee guida per posta elettronica e internet (Gazzetta Ufficiale n. 58 del 10 marzo 2007) ha stabilito che il datore di lavoro, per ridurre il rischio di usi impropri della "navigazione" in Internet (consistenti in attività non correlate alla prestazione lavorativa quali, a mero titolo esemplificativo e non esaustivo, la visione di siti non pertinenti, l'uso di servizi di rete con finalità ludiche o estranee all'attività), deve adottare opportune misure che possono prevenire controlli successivi sul lavoratore.

In attuazione delle anzidette linee guida il Cliente, mediante il presente servizio, nel rispetto della libertà e della dignità dei lavoratori, può individuare e bloccare categorie di siti ritenuti non correlati con la prestazione lavorativa.

Nel rispetto della vigente normativa in materia di privacy, si precisa che in nessun caso i tecnici o gli operatori Halley possono avere conoscenza dei siti internet a cui il Cliente accede o tenta di accedere.

4.4 ANTISPAM

Con l'entrata in vigore del Regolamento UE 679/2016 gli Enti hanno l'obbligo di adeguare il proprio sistema informatico in modo da renderlo il più sicuro possibile per evitare di essere vittime di attacchi hacker, utilizzando anche un servizio antispam.

4.5 MISURE DI SICUREZZA CONTRO INTRUSIONI ED ACCESSI ABUSIVI

Nel rispetto degli obblighi di sicurezza di cui al D.Lgs. 196/2003 e s.m.i. e al Regolamento UE 679/2016, l'accesso al Firewall è consentito unicamente ai tecnici Halley che ne necessitano, esclusivamente per provvedere alla manutenzione ordinaria e straordinaria da remoto.

Sia l'accesso al firewall che al PC e l'eventuale eliminazione di virus avvengono da remoto mediante l'utilizzo da parte di Halley di un collegamento criptato le cui caratteristiche sono indicate nelle *"Condizioni generali di protezione dati"* art. 6.1 della presente offerta a cui si rimanda.

4.6 CONFORMITA' ALLE MISURE MINIME DI SICUREZZA ICT

Il servizio è conforme alla circolare AGID del 18 aprile 2017, n. 2/2017 contenente le "Misure minime per la sicurezza ICT delle pubbliche amministrazioni". In particolare il servizio garantisce:

- accessi limitati ai soli utenti che abbiano le competenze adeguate e la necessità operativa di modificare la configurazione dei sistemi (ABSC 5.1.1 all.1 circolare Agid n. 2/2017);
- sostituzione delle password standard di amministratore con password complesse (ABSC 5.3.1 all.1 circolare Agid n. 2/2017);
- password amministrative complesse (ABSC 5.7.2 all.1 circolare Agid n. 2/2017);
- conservazione delle credenziali amministrative in modo da garantirne disponibilità e riservatezza (ABSC 5.11.3 all.1 circolare Agid n. 2/2017);
- un inventario del software installato tramite la Dashboard (ABSC 2.3.2 all.1 circolare Agid n. 2/2017);
- registrazione delle versioni del sistema operativo e le applicazioni installate (ABSC 2.3.3 all.1 circolare Agid n. 2/2017);
- trasmissione informazioni alle Dashboard in modo sicuro: per i server tramite tunnel crittografato ssh mentre per le workstation tramite protocollo https (ABSC 3.4.1 all.1 circolare Agid n. 2/2017);
- blocco dell'esecuzione di malware e sono mantenuti sempre aggiornati (ABSC 8.1.1 all.1 circolare Agid n. 2/2017);
- gestione centrale del servizio tramite Dashboard, senza possibilità per gli utenti di alterarne la configurazione (ABSC 8.2.1 all.1 circolare Agid n. 2/2017);
- possibilità di forzare manualmente dalla console centrale l'aggiornamento dei sistemi anti-malware installati su ciascun dispositivo e la corretta esecuzione dell'aggiornamento è automaticamente verificata e riportata alla console centrale (ABSC 8.2.2 all.1 circolare Agid n. 2/2017);
- un'analisi dei potenziali malware in un'infrastruttura dedicata basata sul cloud (ABSC 8.2.3 all.1 circolare Agid n. 2/2017);
- esecuzione di una scansione anti-malware dei supporti rimovibili al momento della loro Connessione (ABSC 8.8.1 all.1 circolare Agid n. 2/2017);
- utilizzo di strumenti di filtraggio che operano sull'intero flusso del traffico di rete per impedire che il codice malevolo raggiunga gli host (ABSC 8.5.1 all.1 circolare Agid n. 2/2017);
- blocco dei siti con cattiva reputazione (ABSC 8.6.1 all.1 circolare Agid n. 2/2017);
- filtro del contenuto del traffico web (ABSC 8.9.2 all.1 circolare Agid n. 2/2017);
- blocco del traffico da e verso url presenti in una blacklist o in categorie concordate (ABSC 13.8.1 all.1 circolare Agid n. 2/2017).

4.7 MISURE DI SICUREZZA IN CONFORMITA' AL REGOLAMENTO COMUNITARIO 679/2016 (GDPR)

Si rimanda a: *Condizioni generali di protezione dati* art. 10.

In particolare:

Contro i rischi di accesso in modo illegale a dati personali trasmessi, conservati o comunque trattati il Servizio Secure Box garantisce:

- un apparato di ultima generazione per la protezione da attacchi esterni della rete comunale;
- la ragionevole sicurezza della rete informatica attraverso l'esclusiva apertura di porte necessarie al Cliente (es. SAIA, Entratel, etc.), evitando l'apertura di porte in entrata (WAN to LAN);
- aggiornamento firmware e regole di accesso;

- accessi limitati ai soli utenti che abbiano le competenze adeguate e la necessità operativa di modificare la configurazione dei sistemi;
- la sostituzione delle password standard di amministratore con password complesse;
- l'utilizzo di password amministrative complesse;
- la scansione ogni singolo dispositivo (pc, chiave usb o altri device);
- la protezione del file system di tutti i file;
- la rilevazione rootkit, spyware, adware, dialer, keylogger;
- la creazione eccezioni di massa per falsi positivi (es. programmi ministeriali) o su richiesta (es. programmi di terze parti);
- la visualizzazione delle quarantene;
- scansioni complete e scansioni forzate di aggiornamenti e definizioni virus all'occorrenza;
- un servizio gestito centralmente tramite Dashboard senza consentire agli utenti di alterarne la configurazione;
- un'analisi dei potenziali malware in un'infrastruttura dedicata basata sul cloud;
- l'esecuzione di una scansione anti-malware dei supporti rimovibili al momento della loro connessione;
- la protezione del PC con un software che riconosce i contenuti malevoli e segnala potenziali siti dannosi;
- un elenco costantemente aggiornato di siti malevoli;
- la trasmissione delle informazioni alle Dashboard in modo sicuro tramite protocollo https;
- l'utilizzo di strumenti di filtraggio che operano sull'intero flusso del traffico di rete per impedire che il codice malevolo raggiunga gli host.

Servizio White Box

Art. 1 - Servizi offerti

1.1 AGGIORNAMENTI WINDOWS DEL PC

Halley garantisce gli aggiornamenti del sistema operativo (es. patch e service pack).

Ove concordato, Halley garantisce altresì gli aggiornamenti dell'antivirus e del web protection, di ogni singolo PC.

Gli aggiornamenti vengono effettuati automaticamente tramite un software che mantiene aggiornate versioni e definizioni.

Halley mette a disposizione, ove pattuito, un hard disk aggiuntivo per effettuare backup del PC due volte a settimana.

Art. 2 - Impegni Halley

2.1 AGGIORNAMENTI WINDOWS DEL PC

Halley si impegna a controllare l'esito degli aggiornamenti e a risolvere tempestivamente eventuali anomalie in fase d'aggiornamento.

2.2 INVIO REPORT

Halley si impegna ad inviare settimanalmente tramite e-mail un report contenente l'esito dei controlli di sicurezza e il funzionamento dello stato di sistema di ogni singolo PC.

Art. 3 - Impegni del Cliente

3.1 AGGIORNAMENTI WINDOWS DEL PC

Il Cliente si impegna a rendersi disponibile nei casi in cui debba autorizzare l'accesso al proprio PC per effettuare la manutenzione.

Si rimanda a: *"Condizioni generali di protezione dati"* art. 3.3 e art. 4.

Art. 4 - Ottemperanza ai requisiti di legge

4.1 PROTEZIONE DEI DATI RISPETTO A DETERMINATI PROGRAMMI INFORMATICI

In attuazione delle misure di sicurezza di cui al D.Lgs. 196/2003 e s.m.i. e al Regolamento UE 679/2016 il Servizio White Box mantiene aggiornato il sistema operativo contribuendo ad assicurare la protezione del PC del Cliente.

4.2 MISURE DI SICUREZZA CONTRO INTRUSIONI ED ACCESSI ABUSIVI

Nel rispetto degli obblighi di sicurezza di cui al D.Lgs. 196/2003 e s.m.i. e al Regolamento UE 679/2016, qualora si ravvisasse la necessità di provvedere alla manutenzione ordinaria e straordinaria da remoto, l'accesso al pc del Cliente è consentito unicamente ai tecnici Halley che ne necessitano, previa autorizzazione del Cliente stesso. In tal caso l'accesso al PC avviene mediante un collegamento criptato le cui caratteristiche sono indicate nelle *"Condizioni generali di protezione dati"* art. 6.1 della presente offerta a cui si rimanda.

4.3 CONFORMITA' ALLE MISURE MINIME DI SICUREZZA ICT

Il servizio è conforme alla circolare AGID del 18 aprile 2017, n. 2/2017 contenente le "Misure minime per la sicurezza ICT delle pubbliche amministrazioni". In particolare le Workstation e i concentratori che hanno attivo il servizio:

- Mantengono un inventario del software installato tramite la Dashboard (ABSC 2.3.2. all.1 circolare Agid n. 2/2017);
- Registrano le versioni del sistema operativo, le applicazioni installate e il livello di patch (ABSC 2.3.3 all.1 circolare Agid n. 2/2017);

- Trasmettono informazioni alle Dashboard in modo sicuro tramite protocollo https (ABSC 3.4.1 all.1 circolare Agid n. 2/2017);
- Eseguono una scansione delle vulnerabilità ed installano le patch critiche ed importanti dei prodotti Microsoft (ABSC 4.1.1 e 4.1.2 all.1 circolare Agid n. 2/2017);
- Hanno attivo il log delle scansioni delle vulnerabilità (ABSC 4.2.1 all.1 circolare Agid n. 2/2017);
- Registrano le attività dei sistemi di scanning delle vulnerabilità (ABSC 4.2.2 all.1 circolare Agid n. 2/2017);
- Vengono regolarmente aggiornate con le più rilevanti vulnerabilità di sicurezza dei prodotti Microsoft (ABSC 4.4.1 all.1 circolare Agid n. 2/2017);
- Sono in grado di riconoscere le patch critiche ed importanti dei prodotti Microsoft (ABSC 4.4.2 all.1 circolare Agid n. 2/2017);
- Installano le patch critiche ed importanti dei prodotti Microsoft (ABSC 4.5.1 all.1 circolare Agid n. 2/2017);
- Trasmettono alla Dashboard un alert se una patch critica ed importante dei prodotti Microsoft fallisce (ABSC 4.7.1 all.1 circolare Agid n. 2/2017);
- Eseguono una scansione delle vulnerabilità ed installano le patch critiche e importanti dei prodotti Microsoft (ABSC 4.8.2 all.1 circolare Agid n. 2/2017);
- Hanno sempre il firewall di sistema attivo (ABSC 8.1.2 all.1 circolare Agid n. 2/2017).

4.4 MISURE DI SICUREZZA IN CONFORMITA' AL REGOLAMENTO COMUNITARIO 679/2016 (GDPR)

Si rimanda a: *"Condizioni generali di protezione dati"* art. 10.

In particolare:

Contro i rischi di accesso in modo illegale a dati il Servizio White Box garantisce:

- La tracciabilità delle configurazioni hardware e software;
- Aggiornamento Patch di sicurezza di Windows e principali applicativi;
- Scansione di ogni singolo dispositivo (pc, chiave usb o altri device);
- La protezione del file system di tutti i file;
- Rilevamento rootkit, spyware, adware, dialer, keylogger;
- Creazione eccezioni di massa per falsi positivi (es. programmi ministeriali) o su richiesta (es. programmi di terze parti) dove previsto;
- Visualizzazione delle quarantene;
- Scansioni complete e scansioni forzate di aggiornamenti e definizioni virus all'occorrenza dove previsto;
- L'utilizzo di configurazioni standard per la protezione dei sistemi operativi;
- La trasmissione delle informazioni alle Dashboard in modo sicuro tramite protocollo https;
- L'esecuzione di una scansione delle vulnerabilità e installazione delle patch critiche ed importanti dei prodotti Microsoft;
- Il log delle scansioni delle vulnerabilità sempre attivo;
- La registrazione delle attività dei sistemi di scanning delle vulnerabilità;
- Regolare aggiornamento con le più rilevanti vulnerabilità di sicurezza dei prodotti Microsoft;
- Il riconoscimento delle patch critiche ed importanti dei prodotti Microsoft;
- L'installazione di patch critiche ed importanti dei prodotti Microsoft;
- La trasmissione alla Dashboard un alert se una patch critica ed importante dei prodotti Microsoft fallisce;
- L'esecuzione di una scansione delle vulnerabilità ed installazione delle patch critiche e importanti dei prodotti Microsoft;
- Il firewall di sistema sempre attivo.

Servizio CED remoto

Art. 1 - Servizi offerti

1.1 AGGIORNAMENTI DEL PC (WINDOWS E ANTIVIRUS)

Halley garantisce gli aggiornamenti del sistema operativo (es. patch e service pack) e dell'antivirus (es. versione e definizioni) di ogni singolo PC.

Gli aggiornamenti vengono effettuati automaticamente tramite un software che mantiene aggiornate versioni e definizioni.

Art. 2 - Impegni Halley

2.1 AGGIORNAMENTI DEL PC (WINDOWS E ANTIVIRUS)

Halley si impegna a controllare l'esito degli aggiornamenti e a risolvere tempestivamente eventuali anomalie in fase d'aggiornamento.

2.2 INVIO REPORT

Halley si impegna ad inviare settimanalmente tramite e-mail un report contenente l'esito dei controlli di sicurezza e il funzionamento dello stato di sistema di ogni singolo PC.

Art. 3 - Impegni del Cliente

3.1 AGGIORNAMENTI DEL PC (WINDOWS E ANTIVIRUS)

Il Cliente si impegna a rendersi disponibile solo nei casi in cui debba autorizzare l'accesso al proprio PC per effettuare la manutenzione.

Si rimanda a: *"Condizioni generali di protezione dati"* art. 7.1 e art. 4.

Art. 4 - Ottemperanza ai requisiti di legge

4.1 PROTEZIONE DEI DATI RISPETTO A DETERMINATI PROGRAMMI INFORMATICI

In attuazione delle misure di sicurezza di cui al D.lgs 196/2003 e s.m.i. e al Regolamento UE 679/2016 il Servizio Ced Remoto mantiene aggiornato il sistema operativo e contribuisce ad assicurare la protezione del sistema e dei dati contenuti nei PC del Cliente rispetto a determinati programmi informatici (virus), garantendo la fornitura del più accreditato antivirus sul mercato e la corretta e costante esecuzione degli aggiornamenti.

Si invita in ogni caso il Cliente a tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico mediante virus o ogni altro software aggressivo evitando, a titolo meramente esemplificativo e non esaustivo, lo scarico e l'installazione di programmi di cui non si conosce la natura e la provenienza, nonché l'apertura di link e allegati e-mail sospetti.

4.2 MISURE DI SICUREZZA CONTRO INTRUSIONI ED ACCESSI ABUSIVI

Nel rispetto degli obblighi di sicurezza di cui al D.lgs 196/2003 e s.m.i. e al Regolamento UE 679/2016, qualora si ravvisasse la necessità di provvedere alla manutenzione ordinaria e straordinaria da remoto, l'accesso al pc del Cliente è consentito unicamente ai tecnici Halley che ne necessitano, previa autorizzazione del Cliente stesso.

In tal caso l'accesso al PC e l'eventuale eliminazione di virus avviene mediante un collegamento criptato le cui caratteristiche sono indicate nelle *"Condizioni generali di protezione dati"* art. 6.1 della presente offerta a cui si rimanda.

4.3 CONFORMITA' ALLE MISURE MINIME DI SICUREZZA ICT

Il servizio è conforme alla circolare AGID del 18 aprile 2017, n. 2/2017 contenente le "Misure minime per la sicurezza ICT delle pubbliche amministrazioni". In particolare le Workstation e i concentratori che hanno attivo il servizio:

- Mantengono un inventario del software installato tramite la Dashboard (ABSC 2.3.2 all.1 circolare Agid n. 2/2017);
- Registrano le versioni del sistema operativo, le applicazioni installate e il livello di patch (ABSC 2.3.3 all.1 circolare Agid n. 2/2017);
- Utilizzano configurazioni standard per la protezione dei sistemi operativi (ABSC 3.1.1 all.1 circolare Agid n. 2/2017);
- Trasmettono informazioni alle Dashboard in modo sicuro tramite protocollo https (ABSC 3.4.1 all.1 circolare Agid n. 2/2017);
- Eseguono una scansione delle vulnerabilità ed installano le patch critiche ed importanti dei prodotti Microsoft (ABSC 4.1.1 e 4.1.2 all.1 circolare Agid n. 2/2017);
- Hanno attivo il log delle scansioni delle vulnerabilità (ABSC 4.2.1 all.1 circolare Agid n. 2/2017);
- Registrano le attività dei sistemi di scanning delle vulnerabilità (ABSC 4.2.2 all.1 circolare Agid n. 2/2017);
- Vengono regolarmente aggiornate con le più rilevanti vulnerabilità di sicurezza dei prodotti Microsoft (ABSC 4.4.1 all.1 circolare Agid n. 2/2017);
- Sono in grado di riconoscere le patch critiche ed importanti dei prodotti Microsoft (ABSC 4.4.2 all.1 circolare Agid n. 2/2017);
- Installano le patch critiche ed importanti dei prodotti Microsoft (ABSC 4.5.1 all.1 circolare Agid n. 2/2017);
- Trasmettono alla Dashboard un alert se una patch critica ed importante dei prodotti Microsoft fallisce (ABSC 4.7.1 all.1 circolare Agid n. 2/2017);
- Eseguono una scansione delle vulnerabilità ed installano le patch critiche e importanti dei prodotti Microsoft (ABSC 4.8.2 all.1 circolare Agid n. 2/2017);
- Hanno sempre il firewall di sistema attivo (ABSC 8.1.2 all.1 circolare Agid n. 2/2017).

4.4 MISURE DI SICUREZZA IN CONFORMITA' AL REGOLAMENTO COMUNITARIO 679/2016 (GDPR)

Si rimanda a: *"Condizioni generali di protezione dati"* art. 10.

In particolare:

Contro i rischi di accesso in modo illegale a dati il Servizio CED Remoto garantisce:

- La tracciabilità delle configurazioni hardware e software;
- Aggiornamento Patch di sicurezza di Windows e principali applicativi;
- Scansione di ogni singolo dispositivo (pc, chiave usb o altri device);
- La protezione del file system di tutti i file;
- Rilevamento rootkit, spyware, adware, dialer, keylogger;
- Creazione eccezioni di massa per falsi positivi (es. programmi ministeriali) o su richiesta (es. programmi di terze parti);
- Visualizzazione delle quarantene;
- Scansioni complete e scansioni forzate di aggiornamenti e definizioni virus all'occorrenza;
- L'utilizzo di configurazioni standard per la protezione dei sistemi operativi ;
- La trasmissione delle informazioni alle Dashboard in modo sicuro tramite protocollo https;
- L'esecuzione di una scansione delle vulnerabilità e installazione delle patch critiche ed importanti dei prodotti Microsoft ;
- Il log delle scansioni delle vulnerabilità sempre attivo;
- La registrazione delle attività dei sistemi di scanning delle vulnerabilità;
- Regolare aggiornamento con le più rilevanti vulnerabilità di sicurezza dei prodotti Microsoft;
- Il riconoscimento delle patch critiche ed importanti dei prodotti Microsoft;
- L'installazione di patch critiche ed importanti dei prodotti Microsoft;
- La trasmissione alla Dashboard un alert se una patch critica ed importante dei prodotti Microsoft fallisce;
- L'esecuzione di una scansione delle vulnerabilità ed installazione delle patch critiche e importanti dei prodotti Microsoft;
- Il firewall di sistema sempre attivo.

Prezzi di fornitura

PROSPETTO ECONOMICO

Codice	Descrizione servizi sistemistici	Qty	Prezzo a Voi riservato
X12415	servizio white box ssd 1500	26	7.500,00
X11562	- integrazione ram 8gb	26	
X11550	- integrazione disco fisso 500gb ssd	26	
X11788	- integrazione microsoft windows 10 enterprise 64bit	26	
X12495	- integrazione microsoft office 2019 home & business	26	
X11548	servizio white box ssd 3000	10	
X11563	- integrazione ram 16gb	10	
X11550	- integrazione disco fisso 500gb ssd	10	
X11788	- integrazione microsoft windows 10 enterprise 64bit	10	
X12495	- integrazione microsoft office 2019 home & business	10	
X10360	attivazione white box con trasferimento dati	36	
X12233	servizio secure box 3000	1	
X12252	attivazione servizio secure box	1	
X11746	servizio storage 4tb	2	
X10965	attivazione servizio storage	2	
X10221	attivazione servizio storage per n.1 pc	37	
X11736	servizio ced remoto halley per pc	1	
X10173	attivazione servizio ced remoto	1	
X5554	trasferta	10	
		Totale servizi	
		IVA*	1.650,00
		Totale	9.150,00

* si espone l'IVA attualmente vigente.

Eventuali variazioni dell'aliquota comporteranno conseguenti variazioni sul totale.

Canone da gennaio a dicembre 2022: € 16.200,00 al netto di IVA

Canone da gennaio a dicembre 2023: € 16.200,00 al netto di IVA

ESTREMI PER LA FATTURAZIONE (compilare tutti i campi)

Ufficio ordinante:

Referente:

N. impegno:

Data impegno:

Capitolo di spesa:

N. Determina:

Data determina:

CIG (distinguere chiaramente le lettere dai numeri):

Cod. univoco (distinguere chiaramente le lettere dai numeri):

DATA

.....
Halley Informatica s.r.l.

.....
Il Cliente (timbro e firma)

Allegato A : apparecchiature concesse in comodato d'uso gratuito

Servizio	Descrizione	Q.tà
White Box	PC Sicomputer Productiva One 24" con Cpu intel i3, Webcam, Microfono frontale, n.2 speaker 3Watt, scheda di rete Gigabit e WiFi 802.11n Bluetooth, n.4 Porte USB 2.0 e n.3 Porte USB 3.2 gen1 Alimentatore esterno 120Watt dimensioni 198 (P) x 425 (H) x 540 (L) mm	26
White Box	Tastiera e Mouse Wireless usb Microsoft Desktop 2000 (La sostituzione delle batterie della tastiera e mouse è a cura del cliente)	26
White Box	Manutenzione preventiva e proattiva da remoto, teleassistenza facilitata, controllo funzionalità del PC, gestioni patch, tracciabilità degli asset inventario	26
White Box	Intervento presso il cliente per assistenza hardware con fulmini e sistemistica PC	26
White Box	Integrazione Ram 8GB	26
White Box	Integrazione Disco fisso 500GB SSD	26
White Box	Integrazione Microsoft Windows 10 Enterprise 64bit	26
White Box	Integrazione Microsoft Office 2019 Home & Business	26
White Box	PC Sicomputer Productiva One 24" con Cpu intel i7, Webcam, Microfono frontale, n.2 speaker 3Watt, scheda di rete Gigabit e WiFi 802.11n Bluetooth, n.4 Porte USB 2.0 e n.3 Porte USB 3.2 gen1 Alimentatore esterno 120Watt dimensioni 198 (P) x 425 (H) x 540 (L) mm	10
White Box	Tastiera e Mouse Wireless usb Microsoft Desktop 2000 (La sostituzione delle batterie della tastiera e mouse è a cura del cliente)	10
White Box	Manutenzione preventiva e proattiva da remoto, teleassistenza facilitata, controllo funzionalità del PC, gestioni patch, tracciabilità degli asset inventario	10
White Box	Intervento presso il cliente per assistenza hardware con fulmini e sistemistica PC	10
White Box	Integrazione Ram 16Gb	10
White Box	Integrazione Disco fisso 500GB SSD	10
White Box	Integrazione Microsoft Windows 10 Enterprise 64bit	10
White Box	Integrazione Microsoft Office 2019 Home & Business	10
Secure Box	WatchGuard Firebox M270	1
Secure Box	numero di postazioni da 31-60 utenti	1
Secure Box	Total Security Suite	1
Secure Box	Servizio Antivirus fino a 60 postazioni	1
Servizi Storage	n.1 Synology Rack 19" 1-unità con n.2 dischi fissi da 8000GB (8TB) in raid-1	2
Servizi Storage	n.1 Synology Disk Station con n.2 dischi fissi da 8000GB (8TB) in raid-1	2
Servizi Storage	4000GB (4TB)	2
Servizi Storage	n.2 Gruppi di continuità Legrand Keor SP 800	2
Ced Remoto	Manutenzione preventiva e proattiva da remoto Agent Client	1
Ced Remoto	Antivirus gestito	1
Ced Remoto	Creazione ed invio al cliente delle attività gestite da remoto	1
Ced Remoto	Teleassistenza facilitata	1
Ced Remoto	Gestioni Patch	1
Ced Remoto	Tracciabilità degli asset inventario	1
Ced Remoto	Controllo funzionalità del PC	1
Ced Remoto	Creazione ed invio al cliente delle attività gestite da remoto	1

Condizioni generali di protezione dati

Art. 1 Fornitura degli apparati e del software (es. sistema operativo, office, antivirus, ecc..)

1.1 IMPEGNI HALLEY

Halley si impegna a distribuire il software necessario all'erogazione dei servizi ed a consegnare (ove necessari) apparati in buone condizioni e opportunamente dimensionati in relazione alla quantità dei dati e al contesto del Cliente.

Halley si impegna altresì a controllare il buon funzionamento dell'applicativo software installato.

1.2 IMPEGNI DEL CLIENTE

Il Cliente si impegna a custodire e conservare gli apparati (ove presenti) con la diligenza del buon padre di famiglia, nel rispetto di quanto disposto dall'art. *"Uso e conservazione degli apparati"*.

Il Cliente si impegna altresì a non installare nessun software sugli apparati, ad esclusione dei PC forniti con il servizio White Box.

Art. 2 - Rinnovo tecnologico apparati

2.1 SERVIZI OFFERTI

Halley garantisce il rinnovo tecnologico degli apparati (ove presenti) tramite la loro sostituzione parziale o completa in caso di obsolescenza, previa verifica delle condizioni degli apparati da parte di Halley stessa.

2.2 IMPEGNI HALLEY

Halley si impegna a mantenere sempre ottimali le performance di software e apparati (ove presenti), rinnovandoli e/o riconfigurandoli tutte le volte che si rende necessario.

2.3 IMPEGNI DEL CLIENTE

Il Cliente si impegna a custodire e conservare sempre gli apparati e/o i software (ove presenti) con la diligenza del buon padre di famiglia, nel rispetto di quanto disposto dall'art. *"Uso e conservazione degli apparati"*.

Art. 3 - Uso e conservazione degli apparati

3.1 SERVIZI OFFERTI

Halley si impegna a consegnare (ove necessari) apparati in buone condizioni per l'erogazione dei servizi, e opportunamente dimensionati in relazione alla quantità dei dati e al contesto del Cliente.

3.2 IMPEGNI HALLEY

In caso di malfunzionamento degli apparati Halley provvederà tempestivamente alla risoluzione del problema.

3.3 IMPEGNI DEL CLIENTE

Il Cliente si impegna a preservare l'integrità di tutti gli apparati eventualmente forniti, con la diligenza del buon padre di famiglia, utilizzando anche misure di sicurezza fisica, al fine di far fronte ad eventi straordinari dovuti a cause naturali o provocati da terzi (es. distruzione o furto).

In nessun caso Halley potrà essere ritenuta responsabile per la distruzione, il deterioramento o la perdita degli apparati, i cui obblighi di custodia, manutenzione e conservazione ricadono unicamente sul Cliente.

In caso di distruzione, deterioramento o perdita degli apparati a causa di negligenza, imprudenza e imperizia del Cliente, quest'ultimo sarà tenuto a rimborsare ad Halley il valore di mercato degli apparati.

Art. 4 - Configurazione rete e connettività

4.1 RETE LAN E CONNETTIVITA'

Il Cliente si impegna a non modificare la configurazione di rete e apparati di rete (es. indirizzi IP, switch, ecc...) della rete LAN e della connettività (es. accesso internet, router, ecc...).

Qualora fosse necessario, il Cliente si impegna a segnalare ad Halley con congruo anticipo (almeno 7 giorni) variazioni della LAN e/o del fornitore internet.

Il Cliente si impegna altresì a non spostare le cartelle e i percorsi di rete, delle procedure e dei dati Halley.

Art. 5 - Controllo funzionalità da remoto

5.1 SERVIZI OFFERTI

Halley garantisce il costante e continuo monitoraggio da remoto tramite un apposito pannello di controllo (Dashboard) che evidenzia lo stato di funzionamento dei servizi offerti.

Il monitoraggio di alcuni servizi necessita di un apparato dedicato, chiamato concentratore, che permette di avere hardware e software aggiornati.

Halley monitorizza il funzionamento degli apparati e dei servizi offerti.

5.2 IMPEGNI HALLEY

Halley si impegna a ripristinare il completo monitoraggio in caso di malfunzionamento del pannello di controllo e ad intervenire negli apparati e nei software (ove presenti) sia da remoto che presso Cliente, se necessario.

5.3 IMPEGNI DEL CLIENTE

Il Cliente si impegna a consentire e a non ostacolare in alcun modo il monitoraggio di cui sopra in accordo con Halley.

5.4 PRIVACY

Halley monitorizza da remoto il funzionamento dei servizi offerti senza poter in alcun modo avere conoscenza dei siti internet a cui il Cliente accede o tenta di accedere né tantomeno dei software installati dal Cliente nei PC.

In nessun caso, pertanto, Halley potrà essere ritenuta responsabile circa l'uso del PC e dei software installati dal Cliente.

Art. 6 - Gestione sicurezza accessi

6.1 MISURE DI SICUREZZA CONTRO INTRUSIONI ED ACCESSI ABUSIVI

In attuazione delle misure di sicurezza di cui al D.lgs 196/2003 e s.m.i. e al Regolamento UE 679/2016, Halley si impegna a rendere ragionevolmente sicuri gli accessi e le attività svolte sugli apparati mediante l'utilizzo di un collegamento criptato con protocolli internazionali di sicurezza, le cui credenziali di accesso sono in possesso ed uso esclusivo degli operatori Halley che ne assicurano la custodia e la segretezza. Dette credenziali non contengono riferimenti agevolmente riconducibili agli operatori e sono modificate da questi ultimi almeno ogni sei mesi.

L'eventuale accesso da parte di tecnici o operatori Halley a dati contenuti nel server, nei PC o negli apparati di Backup (ove presenti) del Cliente avviene esclusivamente per provvedere alla manutenzione ordinaria e/o straordinaria da remoto e dunque unicamente per scopi di assistenza tecnica.

6.2 SICUREZZA FIREWALL

Halley si impegna ad aprire le porte in uscita (LAN to WAN) del proprio firewall (ove necessario) esclusivamente verso i propri indirizzi.

Nel caso in cui il firewall sia di altro fornitore, Halley si impegna a comunicare le suddette porte.

Art. 7 - Assistenza hardware (in presenza di apparati)

7.1 Servizi offerti

7.1.1 GARANZIA DEL CORRETTO FUNZIONAMENTO

Halley garantisce l'assistenza hardware telefonica, in teleassistenza e presso Cliente degli apparati (specificati nell'allegato), per tutti i casi in cui si renda necessaria.

7.1.2 IL CANONE COMPRENDE I SEGUENTI SERVIZI

- Sostituzione dei componenti;
- Manodopera dei tecnici presso Cliente

7.1.3 SERVIZI PRESSO CLIENTE

A seguito di rilevazioni dello stato di non funzionamento degli apparati, non risolvibili nè telefonicamente né da remoto, Halley effettuerà presso il Cliente interventi di manutenzione correttiva allo scopo di ripristinare le buone condizioni di funzionamento, salvo le condizioni previste nell'art. "Servizi non inclusi". Sono incluse uscite illimitate del tecnico presso il Cliente.

7.1.4 TEMPI D'INTERVENTO

Ad eccezione del servizio Cloud, in cui la continuità di servizio è prossima al 100% su base annua, l'intervento verrà effettuato dal personale tecnico Halley con un tempo massimo di 8 ore lavorative per il Server e 24 ore lavorative per il gruppo di continuità (secondo l'orario di lavoro Halley).

I tempi d'intervento decorrono dal momento della rilevazione.

7.1.5 GUASTI CAUSATI DA FULMINI

E' inclusa l'assistenza (materiali e manodopera) per guasti causati da fulmini.

7.2 Clausola per la manutenzione

7.2.1 MANUTENZIONE

Halley, a propria discrezione, avrà la facoltà di applicare modifiche tecniche durante gli interventi per la manutenzione.

Halley provvederà al reperimento dei materiali necessari per le operazioni di manutenzione (riparazione e/o sostituzione), come pure alle attrezzature, alla documentazione e agli apparati ritenuti necessari per la corretta effettuazione delle operazioni.

I servizi di manutenzione comprenderanno la riparazione e/o sostituzione provvisoria o definitiva dei componenti con materiali di qualità equivalente o superiore, secondo quanto ritenuto necessario da Halley, e verranno eseguiti in conformità alle norme e procedure di manutenzione in vigore.

I componenti forniti in sostituzione si intenderanno permutati con i componenti sostituiti; questi ultimi, una volta rimossi dagli apparati, resteranno di proprietà della Halley.

7.3 Servizi non inclusi

7.3.1 CAUSE DI ESCLUSIONE

Nel caso di non funzionamento degli apparati, provocato da cause diverse ed estranee dal loro normale uso ed usura, il ripristino non è coperto e saranno applicate le tariffe di listino, ad eccezione del servizio Cloud.

Si citano, a puro titolo di esempio, i seguenti casi:

- a) negligenze o uso errato degli apparati o degli accessori operativi;
- b) guasti nell'alimentazione di rete elettrica, negli impianti di condizionamento dell'aria o di controllo dell'umidità o simili;
- c) guasti causati da incuria e/o accumuli di polvere;
- d) guasti derivanti da cause accidentali di qualsiasi genere ed origine e/o da calamità naturali (incendi, inondazioni e allagamenti, terremoti, altri eventi atmosferici, ecc.) ad eccezione dei guasti di cui all'art.

"Guasti causati da fulmini";

- e) interventi non portati a buon fine a causa di scioperi o per eventi imputabili al Cliente;
- f) uso di accessori operativi non autorizzati;
- g) guasti causati da modifiche effettuate da personale non Halley;
- h) guasti causati dal non funzionamento di materiali non inclusi.

Non è inclusa la fornitura di accessori operativi (es. batterie di tastiere e mouse) ove presenti.
Nel servizio Gestione Stampe sono inclusi invece i toner.

Nel servizio Cloud le cause di esclusione sono:

- malfunzionamenti della linea internet del Cliente;
- guasti derivanti da cause accidentali di qualsiasi genere ed origine e/o calamità naturali (es. terremoti, altri eventi atmosferici, etc.).

Art. 8 - Assistenza sistemistica

8.1 Servizi offerti

8.1.1 GARANZIA DELLA CORRETTA IMPOSTAZIONE DEL SISTEMA

L'assistenza sistemistica garantisce il ripristino di tutte le funzionalità dell'intero sistema: rigenerazioni del sistema operativo, configurazione periferiche, ottimizzazioni del sistema, ecc..

A differenza dell'assistenza hardware, che garantisce solo la riparazione o la sostituzione di un determinato componente, l'assistenza sistemistica permette non solo di far funzionare quel componente, ma di ottimizzarne risorse e capacità.

La sistemistica è l'indispensabile ponte di collegamento tra hardware e software, senza il quale né l'uno né l'altro potrebbero funzionare.

8.1.2 IL CANONE COMPRENDE I SEGUENTI SERVIZI

L'assistenza sistemistica copre tutte quelle attività che non sono competenza tipica né dei servizi hardware né dei servizi software. I servizi forniti, esclusivamente sugli apparati specificati in allegato, sono:

- Ripristino copie Halley;
- Ripristino configurazione server;
- Gestione e configurazione del sistema operativo;
- Reinstallazione sistema operativo;
- Ripristino configurazione PC;
- Ripristino configurazioni periferiche (es. gruppo di continuità, stampanti, firewall, ecc..);
- Ripristino accessi e attività da remoto (es. collegamenti criptati);
- Ripristino configurazioni di rete.

8.1.3 SERVIZI PRESSO IL CLIENTE

A seguito di rilevazioni dello stato di non funzionamento degli apparati, non risolvibili né telefonicamente né da remoto, Halley effettuerà presso il Cliente interventi di manutenzione correttiva allo scopo di ripristinare le buone condizioni di funzionamento, salvo le condizioni previste dall'art. "Servizi non inclusi".

Sono incluse uscite illimitate del tecnico presso il Cliente.

8.1.4 TEMPI D'INTERVENTO

Ad eccezione del servizio Cloud, in cui la continuità di servizio è prossima al 100% su base annua, l'intervento verrà effettuato dal personale tecnico Halley con un tempo massimo di 8 ore lavorative per il Server e 24 ore lavorative per gli altri apparati, ove presenti, (secondo l'orario di lavoro Halley). I tempi d'intervento decorrono dal momento della rilevazione.

Art. 9 - Adeguamento alle normative vigenti in materia di sicurezza e privacy

Com'è noto, anche ai trattamenti di dati personali riguardanti le persone fisiche effettuati dalle Pubbliche Amministrazioni, si applicano le disposizioni del Regolamento UE 679/2016 (GDPR) e del D.Lgs. 196/2003 (Codice in materia di protezione dei dati personali) e s.m.i. che prevedono specifiche garanzie in materia di protezione dei dati per quanto concerne le misure di sicurezza da adottare in particolare al fine di ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati personali e di accessi non autorizzati alle informazioni.

Nel quadro dei generali obblighi di cui alla citata normativa, tutti i servizi contenuti nella presente offerta sono strutturati in modo tale da garantire il rispetto delle misure di sicurezza in materia di trattamento dei dati personali.

Mediante l'adozione dei servizi oggetto della presente offerta, Halley garantisce al Cliente l'adeguamento alle normative vigenti, assicurando, a seconda dei servizi acquistati, salvataggio e protezione dei dati contenuti nei server e negli apparati, controlli e misure antivirus e antimalware, accesso ragionevolmente sicuro e controllato ad internet, nonché la riduzione del rischio di intrusioni ed accessi abusivi ai dati.

Art. 10 - Adeguamento al Regolamento Comunitario GDPR

Il Regolamento Europeo GDPR ha introdotto - tra le altre cose - il principio dell'accountability (responsabilizzazione nella traduzione italiana), individuando nel Titolare il soggetto competente a garantire il rispetto dei principi posti dalla nuova disciplina in tema di trattamento dei dati personali.

In particolare l'art. 24 del Regolamento prevede che tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il Titolare del trattamento debba mettere in atto misure tecniche e organizzative adeguate per garantire ed essere in grado di dimostrare, che il trattamento sia effettuato conformemente al Regolamento.

Halley garantisce servizi ed interventi "privacy compliance" e supporta il Cliente nell'adeguamento alla normativa comunitaria offrendo servizi in grado di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico nonché in grado di garantire un livello di sicurezza adeguato contro i rischi di distruzione, perdita, modifica e accesso in modo abusivo o illegale a dati personali trasmessi, conservati o comunque trattati, come richiesto dal GDPR.

Art. 11 - Tempi di consegna

L'erogazione del servizio viene prevista con termine massimo entro 60 giorni dalla data di ricevimento della copia della delibera di acquisto e del materiale necessario all'evasione dell'ordine. Si potranno protrarre i tempi nei mesi di dicembre e gennaio, in considerazione della chiusura dei nostri fornitori.

Art. 12 - Fatturazione e pagamenti

I prezzi sono validi per le seguenti modalità di pagamento: 30 gg. l'importo una tantum dalla data di attivazione del servizio, ed il canone come pattuito in fase di offerta.

Art. 13 - Validità dell'offerta

La presente offerta è valida 60 giorni, l'azienda si riserva di verificare l'accettazione ricevuta oltre i termini.

Art. 14 - Nomina a Responsabile del trattamento

Il Cliente, accettando la presente offerta, per i servizi ivi indicati, nomina Halley Informatica s.r.l quale Responsabile per il trattamento dei dati, con la descrizione dettagliata dei compiti ed oneri ai quali sarà tenuta in virtù di tale ruolo per tutta la durata della offerta.

Per effetto della presente nomina, che annulla e sostituisce ogni altra eventuale precedente nomina, Halley è autorizzata esclusivamente al trattamento dei dati personali e/o particolari forniti dal Titolare del Trattamento (di seguito anche "Cliente") nella misura e nei limiti necessari all'esecuzione delle attività ad essa assegnate.

Halley ha il potere di compiere tutte le attività necessarie per assicurare il rispetto delle vigenti disposizioni in materia nonché il compito di organizzare, gestire e supervisionare tutte le operazioni di trattamento dei dati personali ad essa comunicati dal Cliente ai fini dell'esecuzione delle attività oggetto della presente offerta.

In conformità a quanto prescritto dal Codice Privacy e dal Regolamento n. 679/2016 relativamente ai dati personali ed alle modalità di trattamento, si precisa che Halley è tenuta a:

- a) svolgere le attività oggetto della offerta in conformità alle disposizioni previste dal Regolamento (UE) 679/2016 e, nello specifico, ai principi enunciati dall'art. 5 GDPR, del cui rispetto il Responsabile dev'essere competente, nonché in conformità ai provvedimenti emanati dal Garante per la protezione dei dati personali e, in generale, alla normativa, europea o statale;
- b) attenersi al divieto di comunicazione dei dati personali salvo il caso in cui ciò si renda necessario per l'adempimento dell'incarico affidato mediante offerta dal Cliente al Responsabile. In tal caso il Cliente autorizza l'eventuale comunicazione dei dati personali a terzi, che dovranno a loro volta essere regolarmente nominati Responsabili del trattamento, esclusivamente al fine di adempiere agli obblighi contrattuali o al fine di ottemperare a specifici obblighi disposti da leggi o regolamenti applicabili al Responsabile;
- c) rispettare le condizioni di cui all'art. 28, paragrafi 2 e 4, GDPR per ricorrere ad un altro Responsabile del trattamento; in particolare, il Responsabile, qualora ricorra ad altro Responsabile per l'esecuzione di specifiche attività di trattamento per conto del Cliente, è consapevole che l'altro Responsabile dovrà sottostare agli stessi obblighi previsti nella presente nomina;
- d) attenersi al divieto di diffusione nonché al divieto di utilizzo autonomo dei dati personali per finalità diverse rispetto a quelle specificate nella presente nomina;
- e) garantire che, all'interno della sua organizzazione e sotto la sua autorità, i dati personali siano trattati soltanto da persone appositamente incaricate e individuate come autorizzate al trattamento, le quali si siano impegnate a trattare e custodire in modo sicuro e riservato i dati loro affidati. Le persone autorizzate al trattamento devono, inoltre, essere istruite, anche per iscritto, e formate con aggiornamento periodico su quanto richiesto dalla normativa in materia di protezione dei dati ed in particolare sui rischi che incombono sui dati e sulle misure disponibili per prevenire eventi dannosi;
- f) adottare le misure richieste ai sensi dell'art. 32 GDPR;
- g) coadiuvare ed assistere il Titolare, nell'ambito dei servizi oggetto della presente scrittura, nel dar seguito alle richieste per l'esercizio dei diritti dell'interessato di cui agli artt. da 15 a 22 GDPR;
- h) assistere il Titolare nel garantire il rispetto degli obblighi di cui agli artt. da 32 a 36 GDPR, ed in particolare:
 - nella predisposizione delle misure di sicurezza da adottare a protezione dei dati;
 - nel dare notizia e documentare al Cliente le eventuali violazioni subite, senza ingiustificato ritardo dalla scoperta delle stesse. A tal fine il Responsabile si impegna a comunicare, per iscritto, nel momento in cui ne è venuto a conoscenza, ogni violazione dei dati personali subita da sé o da qualsivoglia Sub-responsabile;

- nello svolgere, ove necessario, una valutazione d'impatto sulla protezione dei dati e una consultazione preventiva dell'Autorità di Controllo (Garante per la protezione dei dati personali);
- i) restituire e/o cancellare i dati personali al termine del trattamento oggetto del rapporto in essere, eliminando qualunque copia – in formato cartaceo e/o elettronico – sia stata fatta dagli stessi, salvo diverso obbligo di legge. E' fatto salvo il diritto del Responsabile di trattare i dati personali anche successivamente alla data di cessazione al solo ed esclusivo fine di ottemperare a specifici obblighi disposti da leggi o regolamenti applicabili al Responsabile, nei limiti e per la durata da questi previsti;
- j) mettere a disposizione del Cliente tutte le informazioni necessarie per dimostrare il rispetto degli obblighi previsti dal GDPR, e ai sensi dell'art. 31 GDPR, cooperare, su richiesta, con l'autorità di controllo;
- k) redigere il registro delle categorie di attività di trattamento, in conformità a quanto richiesto dall'art 30 GDPR;
- l) non trasferire i dati personali trattati per conto del Cliente verso un Paese terzo o un'organizzazione internazionale.

Sotto il profilo della responsabilità per i danni cagionati dal Responsabile, si richiamano gli artt. 82, 83 e 84 GDPR; in particolare:

- A)** in caso di danni derivanti dal trattamento, il Responsabile ne risponderà qualora non abbia adempiuto agli obblighi imposti dalla normativa vigente in materia di trattamento dei dati personali specificatamente diretti ai Responsabili del trattamento dei dati personali; ne risponderà altresì qualora abbia agito in modo difforme o contrario alle presenti istruzioni impartite dal Titolare del trattamento (art. 82, paragr. 2, GDPR);
- B)** il Titolare ed il Responsabile sono privi di responsabilità soltanto qualora l'evento dannoso non sia in alcun modo a loro imputabile (art. 82, paragr. 3, GDPR);
- C)** il Titolare ed il Responsabile sono responsabili in solido per l'intero ammontare del danno, qualora siano entrambi coinvolti nel medesimo trattamento e risultino corresponsabili del danno cagionato dal trattamento stesso (art. 82, paragr. 4, GDPR);
- D)** qualora vi sia responsabilità in solido, il Titolare o il Responsabile che abbia interamente risarcito il danno ha il diritto di reclamare dal corresponsabile la quota di risarcimento corrispondente alla parte di responsabilità in capo a quest'ultimo (art. 82, paragr. 5, GDPR).

Sono a carico del Cliente tutti gli obblighi stabiliti dalla normativa nei confronti degli interessati, compresi, a titolo meramente esemplificativo, gli obblighi di informazione, gli obblighi relativi al conferimento del consenso, gli obblighi relativi all'esercizio dei diritti degli interessati.

Nessun corrispettivo è dovuto dal Cliente al Responsabile per l'espletamento della funzione.

L'atto di nomina avrà durata pari alla offerta e la sua efficacia cesserà alla data in cui la offerta verrà meno per qualsivoglia motivo.

Nel caso in cui, in qualsiasi momento, una delle disposizioni della presente nomina sia o diventi invalida o inapplicabile, tale disposizione sarà considerata autonomamente rispetto alla presente nomina e, se possibile, sostituita da una disposizione legittima e, ove consentito, non influenza la validità o l'applicabilità di alcuna altra disposizione della presente nomina.

Per tutto quanto non espressamente specificato, il Responsabile si atterrà a quanto previsto dal Regolamento (UE) 679/2016, al Codice Privacy e a successive disposizioni normative in materia di protezione dei dati personali.

Art. 15 - Norme finali

15.1 Per quanto non espressamente disciplinato nella presente offerta si richiamano le norme del Codice Civile.

Art. 16 - Informativa sul trattamento dei dati

Halley Informatica s.r.l. tutela la riservatezza dei dati personali forniti dal Cliente e garantisce ad essi la protezione necessaria da ogni evento che possa metterli a rischio di violazione.

Come previsto dall'art. 13 del Regolamento UE n. 679/2016 ("GDPR"), qui di seguito si forniscono al Cliente le informazioni richieste dalla legge in relazione al trattamento dei dati personali.

La presente informativa è fornita non solo per adempiere agli obblighi di legge in materia di protezione dei dati personali previsti dal GDPR, ma anche perché Halley crede che la tutela dei dati personali sia un valore fondamentale della propria attività e vuole fornire al Cliente ogni informazione che possa aiutarlo a tutelare la privacy dei suoi dati e a controllare l'utilizzo che ne viene fatto.

Chi siamo e quali dati trattiamo

Halley Informatica s.r.l. in persona del Legale Rappresentante, con sede legale in Via Circonvallazione, 131 – 62024 Matelica (MC), C.F. e P.Iva 00384350435, mail: halley@halley.it, pec: halleyinformatica@legalmail.it, tel: 0737.781211 tratta i dati personali e/o "particolari" (ovvero, secondo quanto previsto dall'art. 9 del GDPR, i dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona) forniti dal Cliente.

Responsabile della Protezione dei Dati

Halley Informatica s.r.l. ha nominato un Responsabile della protezione dei dati ("Data Protection Officer" o "DPO"), che il Cliente potrà contattare per l'esercizio dei Suoi diritti, nonché per ricevere qualsiasi informazione relativa agli stessi e/o alla presente Informativa:

- scrivendo a HALLEY INFORMATICA S.r.l, Via Circonvallazione, 131 – 62024 Matelica (MC), – Att.ne Data Protection Officer;
- inviando una e-mail all'indirizzo halley@halley.it – Att.ne Data Protection Officer;
- inviando un messaggio di posta elettronica certificata all'indirizzo PEC halleyinformatica@legalmail.it – Att.ne Data Protection Officer.

Tipi di dati trattati e finalità del trattamento

Halley tratta i dati personali e/o particolari forniti dal Cliente, esclusivamente per la fornitura dei servizi prescelti, per gestire ed eseguire le richieste di contatto inoltrate dal Cliente, fornire assistenza, adempiere agli obblighi di legge e regolamentari cui Halley è tenuta in funzione dell'attività esercitata. In nessun caso Halley rivende a terzi i dati personali forniti dal Cliente, né li utilizza per finalità non dichiarate.

Base Giuridica del Trattamento

Base giuridica di tali trattamenti è l'adempimento delle prestazioni inerenti al rapporto instaurato mediante offerta, il rispetto di obblighi di legge ed il legittimo interesse di Halley Informatica s.r.l. ad effettuare trattamenti necessari a tali finalità.

Luogo del trattamento

I dati personali e/o particolari forniti dal Cliente sono conservati in archivi cartacei, informatici e telematici situati in Italia, dove trova applicazione il GDPR.

Comunicazione a terzi e categorie di destinatari

La comunicazione dei dati personali dell'Interessato può avvenire nei confronti delle società del Gruppo Halley e di terzi la cui attività è necessaria per l'espletamento delle attività inerenti al rapporto instaurato

nonchè per rispondere a determinati obblighi di legge. Detti terzi sono stati regolarmente nominati Responsabili del Trattamento ai sensi dell'art 28 del Regolamento UE 679/2016 e l'elenco aggiornato è consultabile nel sito www.halley.it nella sezione "privacy".

Facoltatività del conferimento dei dati personali

La raccolta ed il trattamento dei dati personali è necessaria per dar seguito alle prestazioni richieste nonché all'erogazione dei Servizi richiesti. Qualora il Cliente non fornisca i dati personali degli interessati, Halley non potrà dar seguito ai trattamenti legati alla gestione delle prestazioni richieste e/o alla offerta, né agli adempimenti che da essi dipendono.

Modalità del trattamento

Il trattamento dei dati personali e/o particolari forniti dal Cliente avverrà in maniera lecita e corretta mediante strumenti automatizzati, informatici e telematici, con logiche strettamente correlate alle finalità indicate e, comunque, con modalità idonee a garantirne la sicurezza e la riservatezza in conformità alle disposizioni previste dall'articolo 32 GDPR.

Tempo di conservazione dei dati

A meno che il Cliente non esprima esplicitamente la propria volontà di rimuoverli, i dati personali degli Interessati saranno conservati fino a che saranno necessari rispetto alle legittime finalità per le quali sono stati forniti ovvero per il periodo di durata della offerta. E' fatto salvo il diritto di Halley di trattare i dati personali anche successivamente alla data di cessazione della offerta al solo ed esclusivo fine di ottemperare a specifici obblighi disposti da leggi o regolamenti alla stessa applicabili, nei limiti e per la durata da questi previsti.

Diritti degli interessati

In relazione ai trattamenti descritti nella presente Informativa, Halley si impegna a coadiuvare ed assistere il Titolare, nell'ambito dei servizi oggetto della presente offerta, nel dar seguito alle richieste per l'esercizio dei diritti degli Interessati ai sensi degli articoli da 15 a 21 del GDPR e, in particolare, il diritto di:

- ottenere conferma che sia o meno in corso un trattamento di dati personali che li riguardano e, in tal caso, ottenere l'accesso ai Suoi dati personali – compresa una copia degli stessi – e la comunicazione, tra le altre, delle seguenti informazioni: finalità del trattamento, categorie di dati personali trattati, destinatari cui questi sono stati o saranno comunicati, periodo di conservazione dei dati, diritti dell'interessato (diritto di accesso – articolo 15 GDPR);
- ottenere, senza ingiustificato ritardo, la rettifica dei dati personali inesatti che li riguardano e/o l'integrazione dei dati personali incompleti (diritto di rettifica – articolo 16 GDPR);
- ottenere, senza ingiustificato ritardo, la cancellazione dei dati personali che li riguardano (diritto alla cancellazione – articolo 17 GDPR);
- ottenere la limitazione del trattamento (diritto di limitazione di trattamento – articolo 18 GDPR);
- ricevere in un formato strutturato, di uso comune e leggibile da un dispositivo automatico, i dati personali che li riguardano, trasmetterli a un altro titolare e/o responsabile senza impedimenti e, ove tecnicamente fattibile, ottenere che i Suoi dati personali siano trasmessi direttamente dalla Società ad altro titolare e/o responsabile, qualora il trattamento si basi sul consenso e sia effettuato con mezzi automatizzati (diritto alla portabilità dei dati – articolo 20 GDPR);
- opporsi al trattamento dei dati personali che li riguardano, salvo che sussistano motivi legittimi per il Titolare di continuare il trattamento (diritto di opposizione – articolo 21 GDPR);
- proporre reclamo all'Autorità Garante per la protezione dei dati personali, Piazza di Montecitorio n. 121, 00186, Roma (RM).

Per l'esercizio dei citati diritti, per la revoca del consenso o per ricevere ulteriori informazioni in ordine al suddetto trattamento, il Cliente potrà contattare Halley Informatica s.r.l scrivendo al seguente indirizzo

e-mail halley@halley.it o all'indirizzo postale presso la sede di Halley Informatica s.r.l, in Via Circonvallazione, 131 – 62024 Matelica (MC).

La richiesta sarà riscontrata nel minor tempo possibile e, comunque, nei termini di cui al GDPR, ovvero entro un mese, salvo casi di particolare complessità, per cui potrebbe impiegarsi massimo 3 mesi. In ogni caso Halley provvederà a spiegare al Cliente il motivo dell'attesa entro un mese dalla sua richiesta. L'esito della richiesta verrà fornito per iscritto o su formato elettronico.

Si informa il Cliente che qualora Halley nutra dubbi circa l'identità della persona fisica che presenta la richiesta, potrà richiedere ulteriori informazioni necessarie a confermare la sua identità.

L'esercizio dei diritti è gratuito ai sensi dell'articolo 12 GDPR. Tuttavia, nel caso di richieste manifestamente infondate o eccessive, anche per la loro ripetitività, Halley potrebbe addebitare al Cliente un contributo spese ragionevole, alla luce dei costi amministrativi sostenuti per gestire la richiesta, o negare la soddisfazione della richiesta.

VERIFICA (Responsabile Processo Offerta Hardware) Data: 12/05/2020 Firma: Stefano Marzocchi	CONVALIDA (Responsabile Sistema Gestione Qualità) Data: 12/05/2020 Firma: Romina Crescentini
--	---