

CONTRATTO per il TRATTAMENTO dei DATI personali

Data processing addendum (ex art. 28 GDPR)

Versione 04.04.2024

Il presente **Contratto per il Trattamento dei Dati** (di seguito anche **DPA**), è parte integrante delle **Condizioni Generali di Servizio** stipulate tra:

- **VHosting Solution s.r.l.** (di seguito anche **VHS**), partita IVA IT06439660827, con sede in Via San Vito, 18 (20123) Milano, Italia, Punti di contatto:

Supporto Commerciale:

E-Mail: info@vhosting.com – H24

PEC: posta@pec.vhosting-it.com – Solo comunicazioni tramite PEC

Servizio Recall: +39 091 5642185 – Dal Lunedì al Venerdì (10:00/14:00 16:00/20:00)

Supporto Tecnico:

Helpdesk: <https://clients.vhosting.com> – H24

(quale Responsabile esterno del trattamento) e

- **il Cliente** (in qualità di Titolare del trattamento).

Scopo del presente Contratto è di definire le condizioni in base alle quali **VHosting Solution s.r.l.**, quale **RESPONSABILE DEL TRATTAMENTO** (di seguito **Responsabile**) in ossequio agli artt. 4 e 28 del Regolamento europeo 679/2016 (GDPR), tratta, nel rispetto delle istruzioni del Cliente, i dati personali per conto del **Cliente**, nonché gli oneri e le responsabilità conseguenti al trattamento dei dati personali.

Indice generale

Definizioni e interpretazione	2
1. Oggetto e Ruoli del trattamento	4
2. Trattamento dei dati personali	4
3. Limitazioni all'utilizzo dei dati personali	5
4. Durata del trattamento e restituzione dati per cessazione del Servizio	5
5. Luogo del trattamento e meccanismi di trasferimento extra SEE dei dati	6
7. Obblighi del Responsabile del trattamento (VHS).....	6
7.2. Verifiche da parte delle Autorità	7
7.3. Aggiornamento e certificazioni	7
7.5. Registro delle attività di trattamento	7
7.5. Obbligo di riservatezza	8
7.6. Portabilità e migrazione.....	8
7.7. Assistenza al Cliente in relazione all'esercizio dei diritti delle Persone Interessate	8
7.8. Assistenza al Cliente in relazione ai propri diritti.....	8
8. Obblighi del Cliente e limitazioni	9
9. Clausola di esenzione	9
10. Subappalto del trattamento dei Dati Personali	10
11. Verifiche e Controlli (Audit)	10
12. Ripartizione delle responsabilità	11
13. Misure tecnico-organizzative e di sicurezza	12
14. Disposizioni Finali	13
Allegato 1: Misure tecnico-organizzative	14

Definizioni e interpretazione

Le premesse costituiscono parte integrante del presente DPA. Nel DPA i seguenti termini ed espressioni avranno il significato associato ad essi qui di seguito:

Amministratore di sistema: il soggetto che ai sensi della presente procedura e sulla base delle indicazioni di volta in volta impartite dal Titolare, dai Responsabili e dal DPO (ove nominato), garantisce l'effettiva predisposizione e implementazione di adeguate misure di sicurezza sui sistemi informatici, con particolare riguardo ai dati personali. Il titolare può riservarsi tale ruolo.

Archivio: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico.

Autorità Garante: l'Autorità denominata Garante per la protezione dei dati personali di cui all'articolo 153 del Codice Privacy, che, tra l'altro, controlla se i Trattamenti siano effettuati nel rispetto della disciplina di legge applicabile.

Autorizzato al trattamento: la persona fisica che elabora o utilizza materialmente i dati personali sulla base delle istruzioni ricevute dal titolare che lo nomina. L'Autorizzato può essere un dipendente o un collaboratore, ma può anche essere nominato tra soggetti esterni all'impresa (es. il soggetto deputato alle riparazioni dei computer aziendali).

Base giuridica del trattamento: è ciò che autorizza legalmente il trattamento, in assenza della quale il trattamento è illecito. Il titolare del trattamento ha l'obbligo di valutare quale sia la base giuridica più idonea rispetto al trattamento che intende porre in essere, e questo prima di iniziare il trattamento. Cioè, non è libero di scegliere la base giuridica che preferisce, ma deve rispettare le condizioni previste dal GDPR in relazione alle caratteristiche di ciascuna delle basi indicate nell'art. 6, ed essere sempre in grado di dimostrare la correttezza della scelta fatta. Ogni base giuridica, infatti, obbedisce a condizioni specifiche, e ha differenti conseguenze sui diritti delle persone. Ovviamente non esiste una gerarchia tra le diverse basi giuridiche.

Le basi giuridiche sono:

- consenso;
- adempimento obblighi contrattuali e precontrattuali;
- obblighi di legge cui è soggetto il titolare del trattamento;
- interessi vitali della persona interessata o di terzi;
- legittimo interesse prevalente del titolare o di terzi cui i dati vengono comunicati.

La base giuridica va indicata nell'informativa rivolta agli utenti.

Per il trattamento dei dati di cui all'art. 9 (dati sensibili), oltre ad individuare una corretta base giuridica, occorre fare riferimento alle condizioni previste nell'articolo indicato.

Dato personale: qualsiasi tipo di informazione che da sola o collegata ad altre può portare all'identificazione del soggetto a cui afferisce (**Interessato**). Si considera identificabile la persona fisica che può essere identificata anche indirettamente, tramite, ad esempio, uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale. Quindi un dato si definisce personale anche se da solo non è in grado di portare all'identificazione dell'Interessato, ma in collegamento con altri dati consenta tale l'identificazione. Dato personale può quindi essere anche un semplice dato valutativo, il quale viene collegato al soggetto fisico solo tramite la connessione con un altro dato. Esempi di dati personali: foto, nome, data di nascita, codice fiscale, dati di localizzazione, indirizzo IP, numero conto corrente. Include, a titolo puramente esemplificativo, tutti i dati forniti, archiviati, inviati, ricevuti o altrimenti elaborati, o creati dal Cliente, o dall'Utente Finale in relazione alla fruizione dei Servizi, nella misura in cui siano oggetto di trattamento da parte del Fornitore, sulla base del Contratto.

Dati a trattamento speciale ex art. 9 GDPR (o particolare): sono quelli che una volta si definivano dati sensibili, e comprendono i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati,

associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, i dati personali idonei a rivelare lo stato di salute e la vita sessuale, e i dati biometrici.

Decisione di Adeguatezza indica una decisione della Commissione Europea sulla base dell'Articolo 45(3) del GDPR in merito al fatto che le leggi di un certo paese garantiscano un adeguato livello di protezione, come previsto dalla Legislazione in materia di Protezione dei Dati Personali.

Informativa: l'informativa è una comunicazione rivolta all'interessato che ha lo scopo di informare il cittadino, anche prima che diventi interessato (cioè prima che inizi il trattamento), sulle finalità e le modalità dei trattamenti operati dal Titolare del trattamento. Essa è condizione non tanto del rispetto del diritto individuale ad essere informato, quanto del dovere del Titolare del trattamento di assicurare la trasparenza e correttezza dei trattamenti fin dalla fase di progettazione dei trattamenti stessi, e di essere in grado di dimostrarlo in qualunque momento (principio di *accountability*).

Interessato al trattamento: il soggetto persona fisica a cui afferiscono i dati trattati, che può essere identificato direttamente o indirettamente attraverso i detti dati, e che può esercitare i diritti previsti dalle norme europee e nazionali. Interessato è anche il dipendente.

Legislazione in materia di Protezione dei Dati Personali indica il GDPR, e ogni eventuale ulteriore norma e/o regolamento di attuazione emanati ai sensi del GDPR o comunque vigenti in Italia in materia di protezione dei Dati Personali, nonché ogni provvedimento vincolante che risulti emanato dalle autorità di controllo competenti in materia di protezione dei Dati Personali (es. Garante per la protezione dei dati personali) e conservi efficacia vincolante (ivi inclusi i requisiti delle Autorizzazioni generali al trattamento dei dati sensibili e giudiziari, se applicabili e ove mantengano la propria efficacia vincolante successivamente al 25 maggio 2018).

Misure di sicurezza: il complesso delle misure tecniche e organizzative, comprese le misure informatiche, adottate per ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati personali, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

Registro dei trattamenti: documento istituito per censire e individuare tutti i trattamenti posti in essere dall'azienda.

Responsabile del trattamento: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento. Generalmente è un fornitore di servizi. Tra titolare e responsabile deve sempre sussistere un contratto che regola i rapporti.

Richiesta indica una richiesta di accesso di un Interessato, una richiesta di cancellazione o correzione dei Dati Personali, o una richiesta di esercizio di uno degli altri diritti previsti dal GDPR;

Responsabile Ulteriore del Trattamento indica qualunque subappaltatore cui il Fornitore abbia subappaltato uno qualsiasi degli obblighi assunti contrattualmente e che, nell'adempiere tali obblighi, potrebbe dover raccogliere, accedere, ricevere, conservare o altrimenti trattare Dati Personali.

Riservatezza delle informazioni: si intende come la proprietà delle informazioni di essere accessibili e utilizzabili su richiesta solo da un soggetto autorizzato.

Servizio/i indica il servizio o i servizi oggetto dei Contratti sottoscritti tempo per tempo tra il Cliente e il Fornitore.

Titolare del trattamento: il soggetto che assume le decisioni in ordine alle finalità e alle modalità del trattamento dei dati personali nonché agli strumenti utilizzati, ivi compresi gli atti di nomina delle figure aziendali preposte e il sistema di regole e procedure da seguire.

Trattamento dei dati personali: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati, applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento, la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione. Anche la semplice consultazione (cioè vedere il dato) è trattamento.

Utente Finale si intende l'eventuale fruitore finale del Servizio, Titolare del Trattamento;

Violazione della Sicurezza dei Dati Personali o anche Data Breach, indica la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai Dati Personali occorsa su sistemi gestiti dal Fornitore o comunque sui quali il Fornitore abbia un controllo.

Per le finalità del presente Contratto, i termini “Interessato”, “Trattamento”, “Titolare del trattamento”, “Responsabile del trattamento”, “Trasferimento” e “Misure tecnico-organizzative adeguate” saranno interpretati in conformità alla Legislazione in materia di Protezione dei Dati Personali applicabile.

1. Oggetto e Ruoli del trattamento

1.1. Le Parti riconoscono e convengono che VHS agisce quale Responsabile del trattamento in relazione ai Dati Personali e il Cliente agisce quale Titolare del trattamento dei Dati Personali.

1.2. Qualora il Cliente svolga operazioni di trattamento per conto di altro Titolare, il Cliente potrà agire a sua volta quale Responsabile del trattamento. In tal caso, il Cliente garantisce che le istruzioni impartite e le attività intraprese in relazione al trattamento dei Dati Personali, inclusa la designazione, da parte del Cliente, di VHS quale ulteriore Responsabile del trattamento derivante dalla stipulazione del presente Contratto è stata autorizzata dal relativo Titolare del trattamento e si impegna ad esibire a VHS, dietro sua semplice richiesta scritta, la documentazione attestante quanto sopra. Il ruolo di VHS in tale caso sarà di Sub-Responsabile del trattamento dei dati personali.

1.3. 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.

2. Trattamento dei dati personali

2.1. Con la stipulazione del presente Contratto il Cliente affida a VHS l'incarico di trattare i Dati Personali ai fini della prestazione dei Servizi, così come meglio dettagliato nelle Condizioni Generali e Speciali del Contratto.

2.2. VHS si impegna a conformarsi alle Istruzioni e ad elaborare i dati personali forniti dal Cliente solo in base a dette Istruzioni e alle condizioni stabilite nel presente Contratto. Qualora il Cliente richieda variazioni rispetto alle Istruzioni iniziali, il Fornitore valuterà gli aspetti di fattibilità e concorderà con il Cliente le predette variazioni ed i costi connessi.

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

2.4. Il trattamento dei dati da parte di VHS avviene per le seguenti finalità:

- fornitura del servizio richiesto dal Cliente in base al Contratto e alle Condizioni Generali e Speciali;
- supporto e assistenza al Cliente;
- verifica del funzionamento corretto del servizio;
- verifica della sicurezza del servizio e dei dati stessi;
- adempimento degli obblighi imposti dalle leggi o dalle prassi di settore.

3. Limitazioni all'utilizzo dei dati personali

3.1. Nell'elaborare i Dati Personali ai fini della prestazione dei Servizi, VHS si impegna a eseguire il trattamento dei Dati Personali:

- soltanto nella misura e con le modalità necessarie per erogare i Servizi o per adempiere opportunamente i propri obblighi, previsti dal Contratto e dal presente DPA ovvero imposti dalla

legge o da un organo di vigilanza o controllo competente. In tale ultima circostanza VHS ne informerà il Cliente (salvo il caso in cui ciò sia vietato dalla legge per ragioni di pubblico interesse) mediante comunicazione trasmessa all'email di contatto fornita dal Cliente in sede di stipula;

- in conformità alle Istruzioni del Cliente.

3.2. Il Personale di VHS che accede, o comunque tratta i Dati Personali, è preposto al trattamento di tali dati sulla base di idonee autorizzazioni e ha ricevuto le necessarie istruzioni in merito al trattamento dei dati personali. Tale personale è altresì vincolato da obblighi di riservatezza.

3.3. Oggetto del trattamento sono i dati personali inviati dal Cliente nel corso dell'utilizzo dei servizi, la cui tipologia ed entità è determinata e controllata esclusivamente dal Cliente medesimo.

3.4. Il Cliente riconosce che VHS inoltre è obbligato a raccogliere una serie di informazioni del Cliente per obblighi legali e/o da mettere eventualmente a disposizione delle autorità. Il Cliente si impegna a fornire queste informazioni e a tenerle costantemente aggiornate.

3.5. Il Cliente è il solo responsabile per la selezione dei Servizi a seconda delle condizioni richieste per il trattamento dei dati, ivi compreso il trattamento di dati soggetti a prescrizioni specifiche (es. dati sanitari) per i quali occorrono più elevati standard di sicurezza. È responsabilità del Cliente selezionare i Servizi accuratamente in particolare quando il trattamento presenta elevati rischi per i diritti delle persone fisiche.

4. Durata del trattamento e restituzione dati per cessazione del Servizio

4.1. Il trattamento dei dati personali sarà effettuato fino alla scadenza del contratto stipulato col Cliente, così come previsto dalle Condizioni Generali di Contratto e/o dai listini online, o comunque fino al verificarsi di condizioni che rendono impossibile continuare l'esecuzione del contratto (es. mancato pagamento). Alla scadenza i dati forniti dal Cliente o elaborati tramite i Servizi di VHS saranno messi a disposizione del Cliente (tramite procedure di download automatizzato) per il periodo indicato nel Contratto e successivamente cancellati dai server di VHS oppure solo cancellati a scelta del Cliente, a meno che non sia previsto un obbligo legale di conservazione dei dati (es. garanzia, motivi fiscali).

4.2. Il Cliente è consapevole ed accetta che per l'eliminazione o cancellazione completa dei dati del Cliente potrebbe occorrere un periodo variabile fino a 30 giorni.

4.3. Qualsiasi prova e documentazione intesa a dimostrare il corretto trattamento dei dati in conformità con i requisiti contrattuali e altri requisiti applicabili sarà conservata da VHS anche oltre la fine del contratto e fino alla scadenza dei termini previsti dalle leggi vigenti per eventuali azioni giudiziarie.

5. Luogo del trattamento e meccanismi di trasferimento extra SEE dei dati

5.1. I dati sono trattati presso la sede di VHS e presso i Data Center. Sia la sede che i Data Center si trovano nel SEE (Spazio Economico Europeo). Il Fornitore si riserva il diritto di aggiornare le sedi di trattamento dei dati se necessario. Le informazioni sulla localizzazione dei Data Center sono disponibili sul sito web ([Lista Data Center](#)).

5.2. VHS non trasferirà i Dati Personali al di fuori dello SEE se non in accordo con il Cliente o a seguito di richiesta del Cliente anche eventualmente effettuata tramite le impostazioni del Servizio (es. utilizzo di servizi di analytics). L'eventuale trasferimento di dati personali al di fuori dello SEE è ammesso a condizione che il paese di destinazione garantisca un livello di protezione adeguato oppure esistano specifiche decisioni di adeguatezza emanate dalla Commissione europea o clausole contrattuali utilizzate dal Cliente.

5.3. Qualora un servizio selezionato dal Cliente implichi un trasferimento di dati al di fuori dello SEE, e ciò comporti la sottoscrizione di apposita clausola o DPA con il servizio in questione, tale sottoscrizione dovrà essere operata dal Cliente quale Titolare del suo trattamento.

5.4. VHS si riserva il diritto di stipulare Clausole Contrattuali Standard (SCC) con l'importatore dei dati per consentire il trasferimento dei dati personali qualora il Cliente comunichi espressamente l'intenzione di avviare trasferimenti con paesi al di fuori del SEE autorizzandolo a stipulare le Clausole con l'importatore dei dati e dichiarando di disporre di tutte le autorizzazioni necessarie.

7. Obblighi del Responsabile del trattamento (VHS)

7.1. VHS si impegna a:

- a) trattare i Dati Personali immessi e utilizzati dal Cliente per i Servizi unicamente nella misura necessaria e proporzionata allo scopo di fornire tali Servizi;
- b) trattare i dati solo tramite Autorizzati al trattamento che operano in base alle istruzioni fornite, verificando che applichino le prescrizioni di sicurezza e riservatezza dei dati, assicurandosi che siano a conoscenza delle norme a tutela dei dati personali, provvedendo alla loro formazione e al loro aggiornamento, prescrivendo che abbiano accesso ai soli dati strettamente necessari per adempiere ai compiti loro assegnati;
- c) non accedere né utilizzare i Dati Personali per qualunque altro scopo se non quello strettamente necessario per lo svolgimento dei Servizi (in particolare in riferimento alle finalità di gestione delle Violazioni) o per l'Assistenza ai Servizi o per la Manutenzione dei Servizi e dei Software;
- d) adottare le misure tecniche e organizzative adeguate e conformi agli standard di settore per garantire la sicurezza dei Dati Personali nella fornitura dei Servizi;
- e) fornire Servizi improntati ai principi di minimizzazione del trattamento (*privacy by design & by default*), fermo restando che è responsabilità esclusiva del Cliente, o dell'Utente Finale, se Titolare del Trattamento, assicurare che il trattamento sia condotto poi concretamente nel rispetto di detti principi e verificare che le misure tecniche e organizzative di un Servizio soddisfano i requisiti di conformità della Società, ivi inclusi i requisiti previsti dalla Legislazione in materia di protezione dei dati personali;
- f) garantire che i dipendenti di VHS autorizzati al trattamento dei Dati Personali in base al Contratto siano vincolati da un obbligo di riservatezza e ricevano una formazione adeguata in merito alla tutela di tali dati;
- g) informare il Cliente qualora, in base alle informazioni a sua disposizione, ritenga che un'istruzione del Cliente stesso violi il GDPR o altre disposizioni per la tutela dei dati dell'Unione europea o di uno Stato membro dell'UE;
- h) in caso di ricevimento di richieste da parte di un'Autorità competente e relative ai Dati Personali trattati, informare il Cliente (fatto salvo quando proibito dalle normative vigenti o da un'ingiunzione di un'autorità competente), nonché limitare la comunicazione dei dati a quanto l'Autorità abbia espressamente richiesto.
- i) in generale VHS presterà assistenza al Cliente e coopererà nei modi previsti dalle leggi e precisati di seguito al fine di consentire al Cliente il rispetto degli obblighi previsti dalla Legislazione in materia di Protezione dei Dati Personali.

7.2. Verifiche da parte delle Autorità

7.2.1. Eventuali verifiche, controlli o indagini da parte dell'Autorità di controllo (Garante Privacy) relative ai trattamenti operati per conto del Cliente, saranno comunicate nel più breve tempo possibile al Cliente all'indirizzo mail indicato in sede di Contratto. Il Responsabile si obbliga a cooperare e assistere il Cliente in casi di verifiche, controlli o indagini sul Cliente stesso, fornendo ogni informazione utile o necessaria riguardo al trattamento dei dati personali.

7.2.2. Entrambe le parti si obbligano a cooperare con le Autorità al meglio in caso di verifica, controlli o indagini da parte delle Autorità.

7.2.3. In caso di verifiche da parte dell'Autorità di controllo con riferimento al trattamento dati del Cliente, il Cliente si impegna a tenere indenne il Responsabile da spese o eventuali costi.

7.3. Aggiornamento e certificazioni

7.3.1. Il Responsabile si obbliga a curare l'aggiornamento delle proprie competenze specifiche e a tenersi aggiornato in merito a codici di condotta e alle certificazioni approvate dalle autorità di controllo e verificate dagli istituti di certificazione.

7.5. Registro delle attività di trattamento

7.5.1. Il Responsabile dichiara di tenere per iscritto un registro di tutte le categorie di attività di trattamento effettuate per conto del Titolare del trattamento e che comprendono:

- nome e dati del Cliente e, se applicabile, del Responsabile della protezione dei dati (DPO);
- categorie di trattamenti effettuati per conto del Cliente;
- se applicabili, i trasferimenti di dati a carattere personale verso un paese terzo o ad una organizzazione internazionale e, nel caso di trasferimenti previsti dall'articolo 49, paragrafo 1, secondo comma del GDPR, i documenti che attestano l'esistenza di opportune garanzie;
- per quanto possibile, una descrizione generale delle misure di sicurezza tecniche ed organizzative;
- gli strumenti che permettono di garantire la riservatezza, l'integrità, la disponibilità e la resilienza costanti dei sistemi e dei servizi di trattamento;
- gli strumenti che permettono di ristabilire la disponibilità dei dati a carattere personale e l'accesso a questi nei tempi appropriati in caso di incidente fisico o tecnico;
- la procedura che mira a testare, ad analizzare ed a valutare regolarmente l'efficacia delle misure tecniche ed organizzative per assicurare la sicurezza del trattamento.

7.5.2. Il Cliente si impegna a fornire per iscritto tutte le istruzioni necessarie per il trattamento dei dati, e tutte le informazioni necessarie per la creazione e la corretta tenuta dei registri del Responsabile sulle attività di trattamento dei dati. Il Cliente resta l'unico responsabile per le informazioni trattate e le istruzioni comunicate nel caso siano non corrette o incomplete.

7.5. Obbligo di riservatezza

7.5.1. Il Responsabile è vincolato dall'obbligo di riservatezza, anche dopo la cessazione del contratto, con riferimento a tutti i dati trattati per conto del Cliente, come anche il personale autorizzato al trattamento, per il quale l'obbligo permane anche dopo la cessazione del rapporto di lavoro.

7.5.2. Il personale viene istruito in merito agli obblighi particolari relativi alla protezione dei dati derivanti dal presente mandato, nonché dalle leggi in materia di protezione dei dati personali. Il Responsabile vigila sull'osservanza delle istruzioni e degli obblighi imposti.

7.5.3. Tale obbligo di riservatezza non si applica nel caso in cui il Cliente abbia autorizzato la fornitura di informazioni a terzi, oppure laddove la fornitura delle informazioni a terzi sia ragionevolmente necessaria in considerazione della natura delle istruzioni e dell'attuazione di questo Accordo per l'elaborazione dei dati, o se vi è l'obbligo legale di rendere l'informazione disponibile a terzi.

7.6. Portabilità e migrazione

7.6.1. Il Cliente prende atto che, in caso di Richieste di portabilità dei Dati Personali avanzate dai rispettivi Interessati, e solo in relazione ai Servizi che generano Dati Personali rilevanti a tal fine, VHS presterà assistenza al Cliente mettendo a disposizione le informazioni necessarie per estrarre i

dati richiesti in formato conforme a quanto previsto dalla Legislazione in materia di Protezione dei Dati Personali.

7.7. Assistenza al Cliente in relazione all'esercizio dei diritti delle Persone Interessate

7.7.1. Qualora le persone interessate esercitino tale diritto presso il Responsabile del trattamento presentandogli la relativa richiesta, il Responsabile del trattamento inoltrerà tempestivamente tali richieste al Titolare al contatto (es. email) indicato in sede di stipula del Contratto.

7.7.2. Il Responsabile si impegna per quanto possibile ad assistere il Cliente nell'adempimento dell'obbligo di evadere le richieste di esercizio dei diritti degli interessati. I sistemi software (es. posta, posta certificata) sono progettati per facilitare il compito del Cliente. Il Responsabile rimane a disposizione del Cliente per ulteriori eventuali informazioni. Nel caso il Cliente richiedesse servizi aggiuntivi (es. il trattamento diretto da parte del Responsabile) per l'evasione delle richieste degli interessati, tali forniture dovranno essere oggetto di separato accordo.

7.8. Assistenza al Cliente in relazione ai propri diritti

7.8.1. VHS, tenuto conto della natura dei Dati Personali e delle informazioni ad esso disponibili, fornirà ragionevole assistenza al Cliente nel rendere disponibili informazioni utili per consentire al Cliente l'effettuazione di valutazioni di impatto sulla protezione dei Dati Personali (DPIA) nei casi previsti dalla legge. In tal caso VHS renderà disponibili informazioni di carattere generale in base al Servizio, quali le informazioni contenute nel Contratto e nei DPA relative ai Servizi interessati. 7.8.2. Eventuali richieste di assistenza personalizzate potranno essere soggette al pagamento di un corrispettivo da parte del Cliente.

7.8.3. Resta inteso che è responsabilità e onere esclusivo del Cliente, 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.

7.8.4. VHS si riserva il diritto, a sua esclusiva discrezione e in ossequio alle leggi vigenti, di rifiutare la divulgazione di qualsiasi informazione che possa essere critica per la sua attività, o che possa costituire una violazione di norme statali o clausole contrattuali o di riservatezza o che comunque possano ledere i diritti di terzi. Al Cliente non verrà concesso l'accesso a dati o informazioni di altri Clienti, o comunque a informazioni non rilevanti per il Cliente.

7.8.5. I registri e le misurazioni fornite da VHS sono considerati autentici a meno che il Cliente non fornisca prove convincenti del contrario.

8. Obblighi del Cliente e limitazioni

8.1. Il Cliente, quale Titolare del Trattamento dei Dati Personali, è responsabile della liceità della raccolta, elaborazione e utilizzo dei dati nonché per la tutela dei diritti degli interessati (cioè i suoi clienti o utenti). Il Cliente si impegna ad assolvere a tutti gli obblighi posti in capo al Titolare del Trattamento (e, nei casi in cui tali obblighi sono in capo all'Utente Finale, garantisce che analoghi obblighi sono imposti a carico dell'Utente Finale) dalla Legislazione in materia di Protezione dei Dati Personali, ivi inclusi gli **obblighi di informativa nei confronti degli Interessati**. Il Cliente si impegna inoltre a garantire che il trattamento dei Dati Personali effettuato mediante l'utilizzo dei Servizi avvenga solo in presenza di **idonea base giuridica** e dei requisiti per l'eventuale trattamento di dati ex art. 9 GDPR.

8.2. Il Cliente si impegna a impartire a VHS Istruzioni conformi alla normativa e a utilizzare i Servizi in modo conforme alla Legislazione in materia di Protezione dei Dati Personali e solo per trattare Dati Personali che siano stati raccolti in conformità alla Legislazione in materia di Protezione dei

Dati Personali. Si impegna altresì a tenere indenne VHS da eventuali richieste legali relative alla non conformità della sua informativa agli utenti/interessati del trattamento e/o della raccolta del consenso.

8.3. E' onere esclusivo del Cliente provvedere alla gestione dei Dati Personali in conformità alle Richieste avanzate dagli Interessati, e pertanto provvedere ad esempio agli eventuali aggiornamenti, integrazioni, rettifiche e cancellazioni dei Dati Personali.

8.6. E' onere del Cliente mantenere attiva la email di contatto fornita alla stipula del Contratto.

8.7. Il Cliente prende atto che, ai sensi dell'art. 30 del GDPR, VHS 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 VHS agisce e che tali informazioni devono essere rese disponibili all'autorità competente, su richiesta. Pertanto, quando richiesto, il Cliente si impegna a dare a VHS i dati identificativi e di contatto sopra indicati con le modalità individuate da VHS nel tempo e a mantenere aggiornate tali informazioni tramite i medesimi canali.

8.8. Spetta al Cliente valutare se il suo trattamento comporta un elevato rischio per i diritti o la libertà di persone fisiche, se si tratta di decisioni automatizzate con conseguenze legali sugli Interessati, monitoraggio sistematico, trattamento di dati a trattamento speciale (ex art. 9 GDPR), e quindi se si rende necessaria una Valutazione di Impatto del Trattamento (DPIA). L'eventuale DPIA dovrà essere portata a conoscenza di VHS. Spetta altresì al Cliente valutare se il suo trattamento comporta la nomina di un Data Protection Officer (DPO). L'eventuale nomina dovrà essere portata a conoscenza di VHS.

8.9. Spetta al Cliente valutare la sussistenza di un obbligo di comunicazione agli Interessati o di notifica alle Autorità di controllo (Garante della Privacy) della violazione della sicurezza o dei dati (Data Breach).

9. Clausola di esenzione

9.1. I dati verranno trattati dal Fornitore con mezzi automatizzati e comunque secondo modalità che non comportano la conoscenza effettiva di attività o di informazioni o fatti o circostanze descritti nelle informazioni trattate. Si applicano, quindi, le esenzioni di cui alla direttiva 2000/31/CE e al D.Lgs 70/2003 e successive modifiche.

9.2. Il Cliente Titolare si impegna comunque a tenere indenne VHS da eventuali azioni legali conseguenti alla commissione di illeciti da parte di clienti/utenti del Cliente derivanti dall'uso di dati personali senza idonea base giuridica oppure in violazione delle leggi (es. diffamazione).

10. Subappalto del trattamento dei Dati Personali

10.1. Con la sottoscrizione del [Contratto di fornitura dei Servizi](#) il Cliente accetta che il Responsabile utilizzi anche soggetti esterni per la fornitura di servizi specializzati connessi alla prestazione richiesta.

10.2. Il Cliente autorizza il Responsabile a subappaltare i suoi obblighi relativi al trattamento dei dati personali a **Sub-Responsabili (ulteriori Responsabili del trattamento)** senza necessità di approvazione preventiva qualora il rapporto tra Responsabile e sub-Responsabile sia contrattualizzato con obblighi analoghi a quelli previsti dal presente contratto e quindi conforme a quanto previsto dall'art. 28, par. 2-4 del GDPR.

10.2.1. In tale contesto, i Sub-Responsabili possono avere sede anche al di fuori dello SEE qualora essi siano vincolati da un contratto ai sensi dell'art. 28 e siano stipulate adeguate garanzie per il trasferimento dei dati ai sensi dall'art. 46 GDPR.

10.3. I Sub-Responsabili di VHS saranno comunque vincolati alle istruzioni di cui al presente Contratto, e in particolare il Sub-Responsabile accederà ai dati solo nella misura richiesta per adempiere alle obbligazioni assunte in base al Contratto, assumendo a sua volta gli obblighi di cui all'art. 28 GDPR.

10.4. Se il Sub-Responsabile non adempie alle proprie obbligazioni in materia di protezione dei dati, il Responsabile del trattamento risponderà nei confronti del Cliente per il trattamento operato dal Sub-Responsabile, salvo differente ripartizione tra Responsabile e Sub-Responsabile.

10.5. Qualora il Cliente avesse ragionevole motivo di opporsi a Sub-Responsabili aggiuntivi, deve comunicare a VHS per iscritto i motivi della sua opposizione. Se il Cliente si oppone ai Sub-Responsabili aggiuntivi deve interrompere l'uso dei Servizi applicabili. L'opposizione deve essere comunicata entro 15 giorni dalla eventuale comunicazione dell'avvio del rapporto col Sub-Responsabile e specificare nel dettaglio il motivo dell'opposizione. VHS non sarà comunque obbligato a rinunciare al Sub-Responsabile opposto, ma il Cliente avrà il diritto di recedere dal Contratto di fornitura.

10.6. Non si devono intendere quali rapporti di subappalto i servizi cui il Responsabile ricorre presso terzi quale prestazione accessoria per supportare la fornitura del servizio, come ad esempio servizi di telecomunicazione, manutenzione e assistenza utente, addetti alle pulizie, spedizione, ecc... Tuttavia, ai fini della garanzia della protezione e della sicurezza dei dati del Committente, il Responsabile è tenuto, anche in caso di prestazioni accessorie demandate a terzi, a stipulare accordi contrattuali adeguati e conformi alla legge e ad adottare le opportune misure di controllo e sicurezza.

10.7. A richiesta il Titolare fornirà un elenco dettagliato dei sub-Responsabili.

11. Verifiche e Controlli (Audit)

11.1. VHS si riserva la facoltà di sottoporre 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. VHS avrà la facoltà di incaricare dei professionisti indipendenti per lo svolgimento di *audit* secondo standard internazionali e/o *best practice*. I Report, che costituiscono informazioni confidenziali del Fornitore, potranno essere resi disponibili al Cliente per consentirgli di verificare la conformità di VHS agli obblighi di sicurezza di cui al presente Contratto.

11.2. Nei casi previsti dall'art. Precedente il Cliente concorda che il proprio diritto di verifica sarà esercitato attraverso la verifica dei Report eventualmente messi a disposizione da VHS.

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

11.4. Nel caso di cui al precedente punto 11.3, il Cliente dovrà previamente inviare richiesta scritta e motivata a VHS. Successivamente alla richiesta di *audit* o ispezione VHS e il Cliente 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 Cliente e coloro che effettuano le verifiche e i costi che VHS potrà addebitare per tali verifiche e che saranno determinati in relazione all'estensione e alla durata delle attività di verifica.

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

11.6. Il Cliente si impegna a corrispondere a VHS gli eventuali costi calcolati e comunicati al Cliente nella fase di cui al precedente punto 11.4, con le modalità e nei tempi ivi concordati. Restano a carico esclusivo del Cliente i costi delle attività di verifica dallo stesso commissionate a terzi.

11.7. L'ispezione deve essere eseguita senza interferire in modo irragionevole con le attività aziendali di VHS.

11.8. Le attività di verifica che interessino eventuali Responsabili Ulteriori dovranno essere svolte nel rispetto delle regole di accesso e delle politiche di sicurezza dei Responsabili Ulteriori.

11.9. VHS potrà, in alternativa all'audit, provare la conformità alle norme e la validità delle misure organizzative e tecniche, a mezzo adesione a Codici di condotta ai sensi dell'art. 40 GDPR, o tramite strumenti equivalenti (es. certificazioni).

12. Ripartizione delle responsabilità

12.1. Il Responsabile del trattamento risponde unicamente del trattamento dei dati personali effettuato ai sensi del presente Accordo e non di ulteriori trattamenti di dati personali, inclusi, a titolo esemplificativo ma non esaustivo, trattamenti per scopi non segnalati dal Titolare ed elaborati da terze parti. Risponde solo dei danni causati a seguito di mancato rispetto degli obblighi di cui al GDPR o normativa nazionale con riferimento ai Responsabili del trattamento, o della violazione delle legittime istruzioni scritte fornite dal Cliente.

12.2. Richiedendo la fornitura del servizio di cui al Contratto, il Cliente dichiara e garantisce di avere un'idonea base legale per elaborare i dati personali, e che i contenuti non sono illegali e non violano alcun diritto di terzi (anche con riferimento a normative settoriali ulteriori, come quelle in materia di proprietà intellettuale). Dichiara altresì che i dati da lui trasmessi sono pertinenti e non eccedenti rispetto alle finalità per le quali sono stati raccolti. Il Cliente si impegna ad indennizzare il 12.3. Responsabile con riferimento a tutti i reclami o azioni legali di terzi relativi alla elaborazione di dati personali illecita o illegittima dipendente dal Cliente stesso o da utenti/clienti del Cliente.

12.4. Qualora il Responsabile e il Cliente siano coinvolti in una procedura relativa all'esecuzione del presente Accordo, il Cliente si farà carico di indennizzare per la totalità l'interessato e solo in seconda battuta si rivarrà sul Responsabile per la eventuale parte di responsabilità dell'Azienda.

12.5. Fatti salvi i limiti inderogabili di legge, VHS sarà tenuto a risarcire il Cliente in caso di violazione del presente Contratto entro i limiti massimi convenuti nel Contratto (Condizioni Generali).

13. Misure tecnico-organizzative e di sicurezza

13.1. Nell'eseguire il trattamento dei Dati Personali ai fini della prestazione dei Servizi VHS si impegna ad adottare misure tecnico-organizzative adeguate per evitare il trattamento illecito o non autorizzato, la distruzione accidentale o illecita, il danneggiamento, la perdita accidentale, l'alterazione e la divulgazione non autorizzata di, o l'accesso ai, Dati Personali, come descritte nell'**Allegato 1** al presente Contratto ("**Misure tecnico-organizzative e di sicurezza**").

13.1.1. L'Allegato 1 contiene misure di protezione degli archivi dati commisurate al livello dei rischi presenti con riferimento ai Dati Personali per consentire la riservatezza, integrità, disponibilità e la resilienza dei sistemi e dei Servizi di VHS, nonché misure per consentire il tempestivo ripristino degli accessi ai Dati Personali in caso di Violazione della Sicurezza dei Dati Personali, e misure per testare l'efficacia nel tempo di dette misure. Le misure di sicurezza sono state progettate in conformità delle norme in materia e dei principi di protezione per impostazione predefinita (*privacy by design e by default*, ai sensi dell'art. 25 GDPR).

13.2. Il Cliente dà atto ed accetta che, tenuto conto dello stato dell'arte, dei costi di implementazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità di trattamento dei Dati Personali, le procedure e i criteri di sicurezza implementati da VHS garantiscono un livello di protezione adeguato al rischio e proporzionato alle attività ed elaborazioni che vengono affidate a VHS.

13.3. VHS potrà aggiornare e modificare nel tempo le Misure di Sicurezza sopra indicate, fermo restando che tali aggiornamenti e modifiche non potranno mai comportare una riduzione del livello di sicurezza complessivo dei Servizi.

13.4. Qualora il Cliente richieda di adottare misure di sicurezza aggiuntive rispetto alle Misure di Sicurezza, VHS si riserva il diritto di valutarne la fattibilità e potrà applicare costi aggiuntivi a carico del Cliente per tale implementazione.

13.5. Il Cliente riconosce e accetta che VHS, tenuto conto della natura dei Dati Personali e delle informazioni disponibili a VHS stesso secondo quanto specificamente riportato nei relativi DPA – Condizioni Particolari, presterà assistenza al Cliente nel garantire il rispetto degli obblighi di sicurezza di cui agli artt. 32-34 del GDPR nei modi seguenti:

- implementando e mantenendo aggiornate le Misure di Sicurezza;
- conformandosi agli obblighi di legge e alle prassi di settore.

13.6. Qualora il prodotto o servizio consenta l'integrazione con applicativi di terze parti, VHS 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.

13.7. **MISURE DI SICUREZZA DEL CLIENTE** – Fermi restando gli obblighi in capo a VHS, il Cliente riconosce e accetta che, nella fruizione dei Servizi, rimane responsabilità esclusiva del Cliente 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.

13.8. A tal fine il Cliente si impegna ad utilizzare i Servizi e le funzionalità di trattamento dei Dati Personali in modo da garantire un livello di protezione adeguato al rischio effettivo.

13.9. Il Cliente si impegna altresì ad adottare tutte le misure idonee per proteggere le credenziali di autenticazione, i sistemi e i dispositivi utilizzati dal Cliente o dai fruitori presso l'Utente Finale per accedere ai Servizi, e per effettuare i salvataggi e backup dei Dati Personali al fine di garantire il ripristino dei Dati Personali nel rispetto delle norme di legge.

13.10. Resta escluso qualsiasi obbligo o responsabilità in capo a VHS circa la protezione dei Dati Personali che il Cliente o l'Utente Finale, se applicabile, conservino o trasferiscano fuori dai sistemi utilizzati da VHS e dai suoi Responsabili Ulteriori del Trattamento (ad esempio, in archivi cartacei, o presso propri data center).

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

- informerà senza ingiustificato ritardo il Cliente mediante comunicazione inoltrata all'email di contatto;
- adotterà misure ragionevoli per limitare i possibili danni e la sicurezza dei Dati Personali;
- fornirà al Cliente, 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 da VHS al Cliente per la gestione della Violazione di Sicurezza;
- considererà informazioni confidenziali ai sensi di quanto previsto nel Contratto, le informazioni attinenti alle eventuali Violazioni della Sicurezza, i relativi documenti, comunicati e avvisi e non comunicherà a terzi dati informazioni, fuori dai casi strettamente necessari all'assolvimento degli obblighi del Cliente derivanti dalla Legislazione in materia di Protezione dei Dati Personali senza il previo consenso scritto del Titolare del Trattamento.

13.11.1. È responsabilità esclusiva del Cliente adempiere, nei casi previsti dalla Legislazione in materia di Trattamento di Dati Personali, agli obblighi di notificazione della Violazione di Sicurezza ai terzi (all'Utente Finale qualora il Cliente sia un Responsabile del Trattamento) e, se il Cliente è Titolare del Trattamento, all'Autorità di controllo e agli interessati.

13.11.2. Resta inteso che la notificazione di una Violazione di Sicurezza o l'adozione di misure volte a gestire una Violazione di Sicurezza non costituisce riconoscimento di inadempimento o di responsabilità da parte del Fornitore in relazione a detta Violazione di Sicurezza.

13.12. Il Cliente dovrà comunicare tempestivamente a VHS eventuali utilizzi impropri degli account o delle credenziali di autenticazione oppure eventuali Violazioni di Sicurezza di cui abbia avuto conoscenza riguardanti i Servizi.

14. Disposizioni Finali

14.1. Il presente Contratto sostituisce qualsiasi altro accordo, contratto o intesa tra le Parti con riferimento al suo oggetto nonché qualsivoglia istruzione fornita in qualsiasi forma dal Cliente al Fornitore precedentemente alla data del presente Contratto in merito ai Dati Personali trattati nell'ambito dell'esecuzione del Contratto di Servizio.

14.2. Il presente Contratto potrà essere modificato da VHS dandone comunicazione scritta (anche via email o con l'ausilio di programmi informatici) al Cliente. In tal caso, il Cliente avrà il diritto di recedere dal Contratto con comunicazione scritta inviata a VHS a mezzo raccomandata con ricevuta di ricevimento nel termine di 15 giorni dal ricevimento della comunicazione del Fornitore. In mancanza di esercizio del diritto di recesso da parte del Cliente, nei termini e nei modi sopra indicati, le modifiche al presente Contratto si intenderanno da questi definitivamente conosciute e accettate e diverranno definitivamente efficaci e vincolanti.

14.3. In caso di conflitto tra le previsioni del presente Contratto e quanto previsto nel Contratto di Servizio o da altri contratti, accordi o documenti, prevarrà quanto previsto nel presente Contratto.

14.4. Per tutto ciò che non è regolamentato dal presente Contratto si deve fare riferimento alle norme europee e nazionali in materia di protezione dei dati personali, che le parti si impegnano a conoscere e rispettare.

Allegato1: Misure tecnico-organizzative

In aggiunta alle misure di sicurezza previste nel Contratto e nel DPA il Responsabile del Trattamento applica le seguenti misure di sicurezza organizzative.

Misure di sicurezza organizzative

Policy e Disciplinari utenti – tutti i dipendenti e in genere gli autorizzati con accesso ai sistemi informativi ha l'obbligo di conformarsi alle policy e ai disciplinari finalizzati a garantire comportamenti idonei ad assicurare il rispetto dei principi di riservatezza, disponibilità ed integrità dei dati nell'utilizzo delle risorse informatiche.

Autorizzazione accessi logici – sono impostati dei profili di accesso e autorizzazione nel rispetto del *least privilege* necessari all'esecuzione delle sole mansioni assegnate. I profili sono individuati e configurati anteriormente all'inizio del trattamento (*privacy by design & by default*), in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento.

Tali profili sono oggetto di controlli periodici finalizzati alla verifica della sussistenza delle condizioni per la conservazione dei profili attribuiti.

Gestione interventi di assistenza – gli interventi di assistenza sono regolamentati allo scopo di garantire l'esecuzione delle sole attività previste contrattualmente e impedire il trattamento eccessivo di dati personali la cui titolarità è in capo al Cliente o all'Utente Finale.

Incident Management – è prevista una specifica procedura di Incident Management allo scopo di garantire il ripristino delle normali operazioni di servizio nel più breve tempo possibile, garantendo il mantenimento dei livelli migliori di servizio.

Procedura Data Breach – è prevista una apposita procedura finalizzata alla gestione degli eventi e degli incidenti con un potenziale impatto sui dati personali che definisce ruoli e responsabilità, il processo di rilevazione (presunto o accertato), l'applicazione delle azioni di contrasto, la risposta e il contenimento dell'incidente-violazione nonché le modalità attraverso le quali effettuare le comunicazioni delle violazioni di dati personali al Cliente.

Procedura Gestione diritti degli Interessati – è prevista una apposita procedura per la Gestione corretta e conforme alle norme delle richieste pervenute dagli Interessati volta a impedire una divulgazione non autorizzata dei dati e una risposta celere e trasparente.

Formazione: VHS eroga periodicamente ai propri dipendenti coinvolti nelle attività di trattamento istruzioni e eventualmente corsi di formazione sulla corretta gestione dei dati personali.

Misure di sicurezza tecniche

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 periodicamente aggiornati in base alle migliori tecnologie disponibili.

Sicurezza linee di comunicazione - per quanto di propria competenza, sono adottati protocolli di comunicazione sicuri e in linea con la tecnologia.

Protezione da malware – i sistemi sono protetti contro il rischio derivante dall'azione di malware di ogni tipo, mediante l'installazione e aggiornamento costante di idonei strumenti.

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.

Sicurezza Password – le credenziali di accesso, le password e i token di autorizzazione e accesso ai sistemi sono gestiti conformemente alle best practice del settore. Ai soggetti ai quali sono attribuite le credenziali sono fornite puntuali istruzioni in relazione alle modalità da adottare per assicurarne la segretezza e impedire gli abusi.

Logging – i sistemi sono configurabili con modalità che consentono il tracciamento degli accessi e, ove appropriato, delle attività svolte in capo alle diverse tipologie di utenze (Amministratore, Super User, etc.) protetti da adeguate misure di sicurezza che ne garantiscono l'integrità.

Procedure di 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.

Ove gli accordi contrattuali lo prevedono è posto in uso un piano di continuità operativa integrato, ove necessario, con il piano di *disaster recovery* che garantiscono la disponibilità e l'accesso ai sistemi anche nel caso di eventi negativi di portata rilevante che dovessero perdurare nel tempo.

Vulnerability Assessment & Penetration Test – VHS effettua periodicamente attività di analisi delle vulnerabilità finalizzate a rilevare lo stato di esposizione alle vulnerabilità note, sia in relazione agli ambiti infrastrutturali sia a quelli applicativi, considerando i sistemi in esercizio o in fase di sviluppo. Ove ritenuto appropriato in relazione ai potenziali rischi identificati, tali verifiche sono integrate periodicamente con apposite tecniche di Penetration Test, mediante simulazioni di intrusione che utilizzano diversi scenari di attacco, con l'obiettivo di verificare il livello di sicurezza di applicazioni/sistemi/reti attraverso attività che mirano a sfruttare le vulnerabilità rilevate per eludere i meccanismi di sicurezza fisica/logica ed avere accesso agli stessi.

I risultati delle verifiche sono puntualmente e dettagliatamente esaminati per identificare e porre in essere i punti di miglioramento necessari a garantire l'elevato livello di sicurezza richiesto.

Amministratori di Sistema – Relativamente a tutti gli utenti che operano in qualità di Amministratori di Sistema, il cui elenco è mantenuto aggiornato e le cui funzioni attribuite sono opportunamente definite in appositi atti di nomina, è gestito un sistema di *log management* finalizzato al puntuale tracciamento delle attività svolte ed alla conservazione di tali dati con modalità idonee a consentirne ex post il monitoraggio. L'operato degli Amministratori di Sistema è sottoposto ad attività di verifica in modo da controllarne la rispondenza alle misure organizzative, tecniche e di sicurezza rispetto ai trattamenti dei dati personali previsti dalle norme vigenti.

Data Center – L'accesso fisico al Data Center è limitato ai soli soggetti autorizzati.

Per il dettaglio delle misure di sicurezza adottate con riferimento ai servizi di data center erogati dai Responsabili Ulteriori del Trattamento, così come individuati nei DPA Condizioni Speciali, si fa rinvio alle misure di sicurezza indicate descritte dai medesimi Responsabili Ulteriori e rese disponibili nei relativi siti istituzionali ai seguenti indirizzi (o a quelli che saranno successivamente resi disponibili dai Responsabili Ulteriori):

- Irideos (Milano): <https://irideos.it/cybersecurity/>
- Servereasy (Settimo Milanese): <https://www.servereasy.it/datacenter/>
- IT.Gate (Torino): <https://www.itgate.it/index.php/it/data-center.html>
- Aruba (Ponte San Pietro, Arezzo): <https://www.datacenter.it/home.aspx>
- Hetzner Online GmbH (Nuremberg, Falkenstein, Germania):
<https://cdn.hetzner.com/assets/Uploads/Sicherheit-en.pdf>
- Hetzner Online GmbH (Helsinki, Finlandia): <https://cdn.hetzner.com/assets/Uploads/Sicherheit-en.pdf>