Accordo sul trattamento dei dati tra titolare e responsabile

Tra

Il Dirigente Scolastico Dott.ssa Giuliana Atzeni C.F. TZNGLN63H59H501H, legale rappresentante dell'ISTITUTO COMPRENSIVO GIOVANNI PAOLO II C.F. 97197210582 p.t. di seguito titolare del trattamento o semplicemente TITOLARE, da una parte

e

Server Plan srl unipersonale con sede in Via G. Leopardi, 22 – 03043 – Cassino (FR), P. Iva 02495250603 – REA 156549 in persona del legale rappresentate p.t., De Luca Claudio, di seguito responsabile del trattamento, o semplicemente RESPONSABILE dall'altra

PREMESSO

- che la Server Plan è leader per i servizi hosting, VPS, Cloud, Server Dedicati e Registrazione domini ed è una realtà consolidata del web hosting italiano. Attualmente è:
  - Registrar accreditato per la Registration Authority Italiana per la registrazione dei domini .it;
  - Registrar accreditato presso l'ICANN per la registrazione dei domini .com, .net, .org, .info, biz e delle nuove estensioni;
  - Registrar accreditato presso l'Eurid per la registrazione dei domini .eu;
  - Registrar accreditato presso LIR (Local Internet Registry) per l'Italia dal RIPE per la gestione di risorse internet (indirizzi IP, Reverse Delegation).

  Fornisce i seguenti servizi: registrazione domini, trasferimento domini, web Hosting, powermail, pec, cloud, Vps, Hosting rivenditore, Server dedicati, Certificati SSL.

  Ha ottenuto le seguenti certificazioni: ISO 9001:2008 - ISO 27001:2013. Applica il codice di condotta CISPE Cloud Infrastructure Services Providers in Europe), che promuove l'armonizzazione delle normative sulla sicurezza e la protezione dei dati archiviati su piattaforma Cloud in ambito UE.

- che tra le parti sussiste un contratto di erogazione di servizi relativo a:

Tipologia di servizi	**Barrare**
Hosting e servizi annessi Server dedicati, VPS, cloud e servizi annessi	X
Registrazione nomi a dominio	X
Certificati digitali Email	X X
Pec	

I.OGGETTO

Le presenti pattuizioni hanno ad oggetto la disciplina delle condizioni alle quali il RESPONSABILE, per conto del Titolare, si impegna ad effettuare le operazioni di trattamento dei dati e delle informazioni personali come definiti di seguito.

Nell'ambito dei loro rapporti contrattuali, le parti si obbligano a rispettare la normativa vigente e applicabile al trattamento dei dati personali, e in particolare il REGOLAMENTO UE 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016, applicabile dal 25 maggio 2018, di seguito anche semplicemente Regolamento

II. DESCRIZIONE DEI TRATTAMENTI DELEGATI AL RESPONSABILE

Il Responsabile è autorizzato a trattare per conto del Titolare i dati personali necessari a prestare il servizio fornito, relativo alla gestione e manutenzione del sistema informative.

Ai suoi incaricati, siano essi interni o esterni all'organizzazione, viene prescritto di non effettuare alcun trattamento sui dati personali contenuti negli strumenti elettronici, fatta unicamente eccezione per i trattamenti di carattere temporaneo strettamente necessari per effettuare la gestione o manutenzione dei sistemi (a titolo esemplificativo attività connesse alla gestione dei backup, aggiornamenti automatici dei sistemi operativi e dei pannelli, richieste di supporto del cliente, interventi sul sistema di virtualizzazione, richieste di restore, upgrade hw, sostituzioni parti hw difettose, migrazione del sistema a seguito di richieste di upgrade hw).

La natura delle operazioni di trattamento poste in essere e la tipologia di dati è:

a) Dati personali la cui trasmissione è implicita nell'utilizzo di protocolli di comunicazione internet

Si tratta di dati che non vengono raccolti per essere associati a soggetti identificati, ma che per loro stessa natura potrebbero, attraverso elaborazioni ed associazioni con dati detenuti da terzi, permettere di identificare gli utenti (es. indirizzi IP).

FINALITA': tali dati vengono trattati per il corretto funzionamento del sito di Server Plan e dei servizi forniti e sono acquisiti da sistemi informatici e procedure software nel corso del loro normale esercizio.

Tali dati vengono utilizzati solamente per informazioni statistiche anonime relative all'utilizzo del servizio e per verificarne il corretto funzionamento.

b) Dati connessi alla registrazione di nomi a dominio

Si tratta di dati identificativi e di contatto che possono essere comunicati a terze parti sempre esclusivamente per le suddette finalità (Autorità di registrazione nazionali ed estere).

Al termine della registrazione del dominio i dati forniti, secondo quanto previsto da ciascuno dei Registri di competenza, verranno pubblicati sul WHOIS (pubblico database che contiene tutti i dati degli intestatari dei nomi a dominio).

Tali dati verranno conservati per la durata di 6 mesi a decorrere dalla cancellazione del nome a dominio cui fanno riferimento, salvo che la conservazione ulteriore non venga imposta con ordine di un'autorità giudiziaria o amministrativa.

FINALITA': registrazione di nomi di dominio

c) trasferimento dei dati personali al di fuori dello Spazio Economico Europeo

Al fine di poter erogare alcuni servizi disciplinati nel contratto (come le registrazioni di nomi a dominio internazionali ed il rilascio di certificati digitali di sicurezza), Il titolare autorizza il Responsabile esterno, al trasferimento dei dati personali a terze parti al di fuori dello Spazio Economico Europeo.

In particolare:

- per i domini di competenza dell'ICANN (Internet Corporation for Assigned Names and Numbers) e su consiglio dell'ICANN, una copia dei dati forniti viene depositata anche presso la società Denic Services GMBH and co, Inc a titolo di garanzia (entrambe le società hanno sede negli Stati Uniti);
- per i domini di competenza del registro GMO Registry i dati vengono trasmessi a Tokyo - Giappone (in cui ha sede il registro);
- per i domini di competenza del registro InternetX i dati vengono trasmessi a negli Stati Uniti (in cui ha sede il registro);

- per i domini di competenza del registro Godaddy.com i dati vengono trasmessi a negli Stati Uniti (in cui ha sede il registro);
- per i domini di competenza del registro GRS Domains i dati vengono trasmessi a Gibilterrra (in cui ha sede il registro);
- per i domini di competenza di P.D.R. SOLUTIONS i dati vengono trasmessi negli Stati Uniti (in cui ha sede la società);
- per i domini di competenza del registro Public Internet Registry (PIR) i dati vengono trasmessi a Reston - Stati Uniti (in cui ha sede il registro);
- per i domini di competenza di Verisign i dati vengono trasmessi a Reston - Stati Uniti (in cui ha sede la società);
- per i domini di competenza di Onlinenic i dati vengono trasmessi in California - Stati Uniti (in cui ha sede la società)
- per i domini di competenza del registro Registry Services, LLC) i dati vengono trasmessi negli Stati Uniti (in cui ha sede il registro);
- per i domini di competenza del registro TUCOWS SERVICES i dati vengono trasmessi in Canada (in cui ha sede il registro);

Nelle suddette circostanze le società destinatarie dei dati ci garantiscono standard di protezione, grazie ad opportune misure tecniche, organizzative e giuridiche.

La categorie di dati che formano oggetto del trattamento sono:

Tipologie di dati trattati	**Barrare**
Dati comuni relativi a clienti/utenti	x
Dati comuni relativi a fornitori	
Dati comuni relativi al personale, o candidati	
Dati comuni relativi ad altri soggetti	x
Particolari categorie di dati relativi a clienti/utenti	
Particolari categorie di dati relativi al personale, o candidati	
Particolari categorie di dati relativi a fornitori	
Particolari categorie di dati relativi ad altri soggetti	
Dati derivanti da attività di profilazione relativi a dipendenti o candidati	
Dati derivanti da attività di profilazione relativi a clienti o utenti	
Dati derivanti da attività di profilazione relativi ad altri soggetti	
Dati relativi allo svolgimento di attività economica o commerciale	x
Dati relativi a decisioni automatizzate	
Dati da sistemi di Videosorveglianza	
Dati relativi a carte di credito	

Dati relativi alla trasmissione su rete una rete telefonica o telematica	x
Dati relativi al traffico telematico o telefonico	

Categorie di dati personali	**Barrare**
Dati identificativi (nome e cognome)	x
Dati anagrafici (data di nascita, luogo di nascita indirizzo, residenza)	x
Dati di contatto (numero di tel. fisso o cell., email, indirizzo per posta cartacea)	x
Informazioni demografiche (genere, età)	x
Dati dei documenti di identità (n. carta di identità o fotocopia)	x
Curricula	
Dati di connessione (log o ip)	x
Dati di geolocalizzazione	
Numero di identificazione	x
Identificativo online	x
Dati giudiziari relativi a condanne penali	
Dati che rivelano l'origine razziale o etnica	
Dati che rivelano le opinioni politiche	
Dati che rivelano convinzioni religiose o filosofiche (idem)	
Dati che rivelano l'appartenenza sindacale	
Dati genetici	
Dati biometrici	
Dati relativi alla salute	
Dati relativi alla vita sessuale	
Dati relativi all'orientamento sessuale	

III. DURATA DELL'ACCORDO

Il presente accordo entrerà in vigore tra le parti dalla sottoscrizione per una durata pari a quella del servizio sostanziale offerto dal Responsabile aderito dal Titolare che giustifica il trattamento da parte del Responsabile.

IV. OBBLIGHI DEL TITOLARE DEL TRATTAMENTO NEI CONFRONTI DEL RESPONSABILE

Il titolare del trattamento si obbliga a:

- fornire al responsabile del trattamento dei dati personali quanto indicato al n. II del presente accordo;

- documentare per iscritto tutte le istruzioni riguardanti il trattamento dei dati da parte del responsabile;
- assicurare, sin d'ora e per tutta la durata del trattamento, il rispetto degli obblighi previsti dal Regolamento da parte del responsabile;
- supervisionare il trattamento, compresa la realizzazione degli audit e le ispezioni col contributo del responsabile.

V. OBBLIGHI DEL RESPONSABILE

Il Responsabile si impegna innanzi al Titolare a:

1. Trattare i dati personali per le sole finalità oggetto del trattamento;

2. Trattare i dati personali in conformità alle istruzioni scritte del titolare, allegate al presente contratto; se il responsabile ritiene che un'istruzione ricevuta dal titolare rappresenti una violazione del Regolamento generale sulla protezione dei dati, o del diritto dell'Unione europea o del diritto di uno Stato membro, egli informa tempestivamente il titolare del trattamento.

3. garantire la riservatezza dei dati personali trattati nell'ambito del presente contratto;

4. assicurare che le persone autorizzate a trattare i dati a carattere personale in virtù del presente contratto:
   - si impegnino a rispettare la riservatezza o siano sottoposte a un idoneo obbligo legale di riservatezza
   - ricevano le istruzioni necessarie a mantenere la protezione dei dati a carattere personale.

5. Tener conto, per quanto riguarda strumenti, prodotti, applicazioni o servizi, dei principi della privacy sin dalla progettazione (privacy by design) e della privacy per impostazione predefinita (privacy by default).

6. Sub-responsabili - Autorizzazione generale

Il Responsabile può ricorrere a un altro responsabile del trattamento (d'ora innanzi sub-responsabile) per l'esecuzione di specifiche attività di trattamento. In questo caso egli informa preventivamente e per iscritto il titolare di tutte le modifiche riguardanti l'aggiunta o la sostituzione dei sub responsabili. Tali informazioni devono indicare chiaramente le attività di trattamento effettuate dal sub-responsabile, l'identità e i recapiti del sub responsabile, e la data del contratto relativo al sub-trattamento. Il titolare del trattamento dispone di un periodo di 15 giorni a far data dal ricevimento delle informazioni per presentare le proprie obiezioni. Il sub trattamento non può avere inizio sino a che il termine indicato non sia spirato senza che il titolare abbia presentato obiezioni.

Il sub-responsabile è tenuto a rispettare gli obblighi del presente contratto per conto e secondo le istruzioni del titolare del trattamento. E' compito del Responsabile assicurare che il sub-responsabile presenti le medesime garanzie sufficienti in ordine alla messa in atto delle misure tecniche e organizzative adeguate in modo che il trattamento soddisfi i requisiti del Regolamento generale sulla protezione dei dati.
Se il sub-responsabile del trattamento omette di adempiere i suoi obblighi in materia di protezione -dei dati, il Responsabile iniziale conserva nei confronti del titolare la piena responsabilità per l'adempimento degli obblighi del sub-responsabile.

7. Diritto degli interessati all'informativa

E' compito del titolare del trattamento fornire l'informativa agli interessati del trattamento al momento in cui i dati sono raccolti.

8. Esercizio dei diritti da parte degli interessati

Nella misura del possibile il responsabile del trattamento deve aiutare il titolare del trattamento ad adempiere ai propri obblighi di fornire riscontro alle richieste degli interessati in ordine al diritto d'accesso, di rettifica, di cancellazione e di opposizione, alla limitazione del trattamento, diritto alla portabilità dei dati, diritto a opporsi a una decisione individuale automatizzata (compresa la profilazione).
Quando gli interessati si rivolgano al responsabile per l'esercizio dei loro diritti, il responsabile deve inviare queste richieste, non appena vengono ricevute, per posta elettronica, all'indirizzo di posta elettronica indicato in calce al presente accordo (allegato B). Ove il Titolare non provveda a tale incombente il Responsabile è libero da ogni obbligo.

9. Notifica delle violazioni dei dati personali

Il Responsabile comunica al Titolare del trattamento tutte le violazioni di dati a carattere personale nel **termine massimo di 48 ore** dal momento in cui è venuto a conoscenza della violazione, con le seguenti modalità: comunicazione all'indirizzo di posta elettronica indicato nell'allegato B al presente contratto.

Tale comunicazione è accompagnata dalla notizia della messa a disposizione (ove possibile) di tutta la documentazione utile (la cui modalità di trasmissione verrà concordata tra le parti) al fine di permettere al titolare del trattamento, di provvedere, se necessario, alla notifica di tale violazione all'Autorità di Controllo competente nei termini di legge.

10. Ausilio del responsabile per il rispetto, da parte del Titolare, degli obblighi gravanti sul Titolare stesso

Il responsabile aiuta il titolare del trattamento nell'effettuazione della valutazione di impatto sulla protezione dei dati personali.

Il responsabile del trattamento aiuta il titolare del trattamento nell'effettuazione della consultazione preventiva rivolta all'Autorità di controllo

11. Misure di sicurezza

Il responsabile si obbliga, ai sensi dell'articolo 32, a mettere in atto le misure di sicurezza descritte nell'allegato "Sicurezza 2018" che il Titolare dichiara adeguate e conformi alle istruzioni da impartire.

Il Titolare delega al responsabile l'adozione di misure diverse rispetto a quelle descritte nell'allegato "Sicurezza 2018" a condizione che il responsabile rispetti i parametri definiti dall'articolo 32 del Regolamento. Il responsabile, se applicabili e congrue, si obbliga a mettere in atto le misure di sicurezza seguenti:

- la pseudonimizzazione e la cifratura dei dati personali;
- misure che abbiano la capacità di assicurare su base permanente la riservatezza;
- l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
- misure che abbiano la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
- una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento;

12. Sorte dei dati

Al termine della prestazione del servizio relativo al trattamento dei dati il responsabile si obbliga a restituire tutti i dati personali al titolare del trattamento, salvo che questi gli ordini di distruggerli.

La restituzione si accompagna alla distruzione di tutte le copie esistenti nel sistema informatico del responsabile.

13. Responsabile per la protezione dei dati (Data Protection Officer, DPO o RPD)

Il responsabile del trattamento comunica al Titolare il nome e i recapiti del suo responsabile per la protezione dei dati (DPO o RPD) mediante compilazione del form in calce alla presente scrittura.

14. Registro delle attività di trattamento

Il Responsabile dichiara di tenere per iscritto un registro di tutte le attività di trattamento effettuate per conto del titolare comprendente tutti gli elementi elencati a tal fine dall'articolo 30 del Regolamento.

15. Documentazione

Il responsabile mette a disposizione del titolare del trattamento la documentazione necessaria a dimostrare il rispetto di tutti i suoi obblighi, e per consentire gli audit, comprese le ispezioni, al titolare del trattamento o altro soggetto da questi a tal fine incaricato, e contribuire agli audit.

V Clausole finali

Le premesse e gli allegati fanno parte integrante del presente accordo.

ROMA, 30/05/2025

Il Dirigente Scolastico

Dott.ssa Giuliana Atzeni

Documento firmato digitalmente ai sensi del CAD e norme ad esso connesso

ALLEGATO A – DATI DI CONTATTO

Nominativo del DPO di ServerPlan	**Dati di contatto**
Avv. Maria Leda Piedimonte	Email: dpo@messaggipec.it Telefono: 3392493238

Nominativo del DPO del Titolare (se applicabile)	**Dati di contatto**

ALLEGATO B - RECAPITI

Recapiti del Titolare per le comunicazioni previste nel presente accordo	Dati di contatto
Data Breach	
Istanze di accesso	
Autorità Garante o Altra Autorità	

Recapiti del Responsabile per le comunicazioni previste nel presente accordo	Dati di contatto
Data Breach	Pec: gdpr@messaggipec.it Telefono: 07763924 int. 2
Istanze di accesso	Pec: gdpr@messaggipec.it Telefono: 07763924 int. 2
Autorità Garante o Altra Autorità	Pec: gdpr@messaggipec.it Telefono: 07763924 int. 2

ALLEGATO C – "Sub-responsabili"

Il Responsabile è autorizzato a sub-appaltare parte delle operazioni di trattamento ai seguenti sub-responsabili (siano essi o meno appartenenti al Gruppo del Responsabile)

La seguente tabella mappa i sub-responsabili ingaggiati dal Responsabile.

Paese in cui è stabilito il Titolare	Responsabile	Sub-responsabili
Italia	Italia	Italia, Irlanda, Regno Unito, Belgio, Giappone, Stati Uniti, isole Vergini Britanniche, Isole Cayman

Sub-responsabile
Registrazione dei domini • Centralnic LTD - 4th Floor, Saddlers House,44 Gutter Lane, London, EC2V 6AE - United Kingdom • CONSIGLIO NAZIONALE DELLE RICERCHE - Via Giuseppe Moruzzi, 1 56124 – PISA – Italia • DENIC Services GmbH & Co. KG - Heinrich-Hertz-Str. 5 64295 Darmstadt Germany • EURID VZW - Telecomlaan 9 - 1831 Diegem – BELGIUM • GODADDY.COM, LLC - 2155 E GoDaddy Way, Tempe, Arizona 85284 United States • GMO REGISTRY - Cerulean Tower 9-12F-26-1 Sakuragaokacho-Shibuya ku, Tokyo, Japan • GLOBAL REGISTRY SERVOCES LTD - 327 Main Street- Gibraltar, GX11 1AA • INTERNET X CORP - 777 Brickell Avenue, Suite 500-Miami, FL 33131, USA • IDENTITY DIGITAL INC. - 10500 NE 8th St Ste 750 Bellevue, WA 98004 United States • IDENTITY DIGITAL LTD - Ground Floor Le Pole House Ship Street Great Ship Street Great Ireland • ONLINENIC INC - 3027 Teagarden St. San Leandro, CA 94577, USA • PUBLIC INTERNET REGISTRY - 1775 Wiehle Avenue, Suite 100-Reston VA 20190 • PDR SOLUTIONS - 10 Corporate Drive Burlington-01803 Massachusetts, United States • REGISTRY SERVICES LLC - 100 S Mill Avenue Suite 1600 AZ 85281 • 96 Mowat Ave Toronto, ON M6K 3M1 Canada • TUCOWS REGISTRY SERVICES - 96 Mowat Ave Toronto, ON M6K 3M1 Canada • VERISIGN INC - ON BEHALF OF VNDS LLC-PO BOX # 404326-ATLANTA GA 30384- UNITED STATES • INTERNET CORPORATION FOR ASSIGNED NAMES AND NUMBERS - 12025

Waterfront Drive Suite 300-Los Angeles, CA 90094-2536-USA

Certificati digitali

- DIGICERT INC - Unit 21, 12 Beckett Way Park West Business Park - D12 C9YE Dublin 12 - Ireland

PEC

- NAMIRIAL S.P.A. - VIA CADUTI SUL LAVORO, 4 -SENIGALLIA AN -60019

Restano esclusi i servizi non forniti dal Responsabile e soggetti a separati accordi tra il Sub-responsabile e il Titolare.

La tabella dei sub-responsabili verrà aggiornata di volta in volta e il Titolare verrà notificato di conseguenza in modo che possa opporsi all'impiego di nuovi sub-responsabili.

ALLEGATO D
MODELLO PER LA COMUNICAZIONE DELLA VIOLAZIONE DEI DATI DAL RESPONSABILE AL TITOLARE (AI FINI DEL C.D. "DATA BREACH")

Denominazione (nome della ditta o azienda o ragione sociale)

_____

indirizzo di posta elettronica o pec indicato nell'accordo sul trattamento

_____@_____

Sito web _____

REFERENTI:

Cognome _____

Nome_____

Telefono fisso _____ cell. _____

indirizzo di posta elettronica ulteriore

_____@_____

Denominazione della/e banca/banche dati oggetto di data breach e breve descrizione della violazione dei dati personali ivi trattati

_____
_____
_____
_____
_____
_____

Quando si è verificata la violazione dei dati personali trattati nell'ambito della banca dati?

[ ] Il _____
[ ] Tra il _____ e il _____
[ ] In un tempo non ancora determinato
[ ] E' possibile che sia ancora in corso

Dove è avvenuta la violazione dei dati? (Specificare se sia avvenuta a seguito di smarrimento di dispositivi o di supporti portatili)

_____
_____
_____
_____
_____
_____

Modalità di esposizione al rischio - Tipo di violazione

[ ] Lettura (presumibilmente i dati non sono stati copiati)
[ ] Copia (i dati sono ancora presenti sui sistemi del titolare)
[ ] Alterazione (i dati sono presenti sui sistemi ma sono stati alterati)
[ ] Cancellazione (i dati non sono più sui sistemi del titolare e non li ha neppure l'autore della violazione)
[ ] Furto (i dati non sono più sui sistemi del titolare e li ha l'autore della violazione)
[ ] Altro :

_____

Dispositivo oggetto della violazione

[ ] Computer
[ ] Rete
[ ] Dispositivo mobile
[ ] File o parte di un file
[ ] Strumento di backup
[ ] Documento cartaceo
[ ] Altro :

_____

Sintetica descrizione dei sistemi di elaborazione o di memorizzazione dei dati coinvolti, con indicazione della loro ubicazione:

_____
_____
_____
_____
_____
_____

Quante persone sono state colpite dalla violazione dei dati personali trattati nell'ambito della banca dati?

[ ] N. _____ persone
[ ] Circa _____ persone
[ ] Un numero (ancora) sconosciuto di persone

Che tipo di dati sono oggetto di violazione?

[ ] Dati anagrafici/codice fiscale
[ ] Dati di accesso e di identificazione (user name, password, customer ID, altro)
[ ] Dati relativi a minori
[ ] 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
[ ] Dati personali idonei a rivelare lo stato di salute e la vita sessuale
[ ] Dati giudiziari
[ ] Copia per immagine su supporto informatico di documenti analogici
[ ] Ancora sconosciuto
[ ] Altro :

Conseguenze sull'interessato:

[ ] Danni fisici o psicologici gravi o morte (Molto Alto)
[ ] Discriminazione (Alto
[ ] Danno per la reputazione (Alto)
[ ] Impossibilità di esercitare diritti, accedere a servizi, godere di opportunità (Alto)
[ ] Perdite finanziarie (Alto)
[ ] furto di identità (Medio)
[ ] Perdita di controllo dei dati (Medio)
[ ] Disagi significativi (difficoltà derivanti da costi aggiuntivi diniego di accesso a servizi aziendali, timore, stress) (Medio)
[ ] Svantaggi minori e disagi(tempo perso per reinserire i dati, irritazione o fastidio) (Basso)

_____
_____

Livello di gravità della violazione dei dati personali trattati nell'ambito della banca dati (secondo le valutazioni del titolare)?

[ ] Basso/trascurabile (B)
[ ] Medio (M)
[ ] Alto (A)
[ ] Molto alto (MA)

Misure tecniche e organizzative applicate ai dati oggetto di violazione

_____
_____

Si ritiene che la violazione vada comunicata anche agli interessati?

Sì, perché

_____

No, perché

_____

Qual è il contenuto della comunicazione da rendere agli interessati?

_____
_____
_____
_____
_____

_____

Quali misure tecnologiche e organizzative sono state assunte per contenere la violazione dei dati e prevenire simili violazioni future?

_____

_____

Allegato E

Istruzioni generali impartite dal Titolare al Responsabile del Trattamento

Il Responsabile è tenuto ad adottare le seguenti misure di sicurezza:

- individuare per iscritto le persone fisiche autorizzate al trattamento, anche per settori e nel rispetto della propria normativa nazionale. Contestualmente alla designazione, il Responsabile si fa carico di fornire adeguate istruzioni scritte alle persone autorizzate al trattamento circa le modalità del trattamento, in ottemperanza a quanto disposto dalla legge e dal presente accordo. A titolo esemplificativo e non esaustivo, il Responsabile, nel designare per iscritto le persone autorizzate al trattamento, dovrà prescrivere che essi abbiano accesso ai soli dati personali la cui conoscenza sia strettamente necessaria per adempiere ai compiti loro assegnati.
- Il trattamento di dati personali con strumenti elettronici deve essere consentito agli incaricati dotati di credenziali di autenticazione che consentano il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti.
- Le credenziali di autenticazione devono consistere in un codice per l'identificazione dell'incaricato associato a una parola chiave riservata conosciuta solamente dal medesimo oppure in un dispositivo di autenticazione in possesso e uso esclusivo dell'incaricato, eventualmente associato a un codice identificativo o a una parola chiave.
  - Le credenziali di autenticazione devono essere associate ai soggetti autorizzati individualmente
  - Con le istruzioni impartite agli incaricati deve essere prescritto di adottare le necessarie cautele per assicurare la segretezza della componente riservata della credenziale e la diligente custodia dei dispositivi in possesso ed uso esclusivo dell'incaricato.
- La parola chiave, quando è prevista dal sistema di autenticazione, deve essere composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito; essa non contiene riferimenti agevolmente riconducibili all'incaricato e deve essere modificata da quest'ultimo al primo utilizzo e, successivamente, almeno ogni sei mesi. In caso di trattamento di dati sensibili e di dati giudiziari la parola chiave è modificata almeno ogni tre mesi.
- Il codice per l'identificazione, laddove utilizzato, non può essere assegnato ad altri incaricati, neppure in tempi diversi.
- Le credenziali di autenticazione non utilizzate da almeno sei mesi devono essere disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica.
- Le credenziali devono essere disattivate anche in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali.
- Devono essere impartite istruzioni agli incaricati per non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento.
- Quando per gli incaricati sono individuati profili di autorizzazione di ambito diverso deve essere utilizzato un sistema di autorizzazione.
- I profili di autorizzazione, per ciascun incaricato o per classi omogenee di incaricati, devono essere individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento.
- Periodicamente, e comunque almeno annualmente, deve essere verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione.
- I dati personali devono essere protetti contro il rischio di intrusione e dell'azione di programmi di cui all'art. 615-*quinquies* del codice penale italiano, mediante l'attivazione di idonei strumenti elettronici da aggiornare regolarmente.
- Gli aggiornamenti periodici dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti devono essere effettuati tempestivamente.
- Agli incaricati devono essere impartite istruzioni organizzative e tecniche che prevedono il salvataggio dei dati con frequenza almeno settimanale.
- I dati che comportano rischi particolari devono essere protetti contro l'accesso abusivo, di cui all'art. 615-*ter* del codice penale, mediante l'utilizzo di idonei strumenti elettronici.
- Agli incaricati devono essere impartite istruzioni organizzative e tecniche per la custodia e l'uso dei supporti rimovibili su cui sono memorizzati i dati al fine di evitare accessi non autorizzati e trattamenti non consentiti.

- I supporti rimovibili contenenti dati che comportano rischi particolari, se non utilizzati, devono essere distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri incaricati, non autorizzati al trattamento degli stessi dati, se le informazioni precedentemente in essi contenute non sono intelligibili e tecnicamente in alcun modo ricostruibili.
- Devono essere 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 e non superiori a sette giorni.
- I dati che comportano rischi particolari contenuti in elenchi, registri o banche di dati, tenuti con l'ausilio di strumenti elettronici, devono essere trattati con tecniche di cifratura o mediante l'utilizzazione di codici identificativi o di altre soluzioni che, considerato il numero e la natura dei dati trattati, li rendono temporaneamente inintelligibili anche a chi è autorizzato ad accedervi e permettono di identificare gli interessati solo in caso di necessità.

- In ordine alla dismissione della strumentazione informatica, il Responsabile deve osservare almeno le procedure prescritte dal Garante Privacy nel provvedimento del 13 ottobre 2008 in materia di dismissione di pc e dispositivi elettronici contenenti banche dati, attivando gli opportuni accorgimenti tecnici idonei a cancellare in maniera definitiva i dati personali ivi memorizzati così da garantire la loro non intelligibilità, o modalità e sistemi equivalenti.

Il Responsabile è inoltre tenuto a:

- vincolare le persone autorizzate al trattamento alla riservatezza o ad un adeguato obbligo legale di riservatezza, mediante apposito e valido accordo di riservatezza o non divulgazione, anche per il periodo successivo all'estinzione del rapporto di collaborazione intrattenuto con il Responsabile, in relazione alle operazioni di trattamento da esse eseguite.
- garantire la sicurezza del Data Base e/o delle operazioni di elaborazione ed archiviazione e il salvataggio disposto in via automatica del Sistema informatico.
- risolvere i problemi di funzionalità del software di gestione del Data Base;
- per quanto concerne i trattamenti effettuati per fornire il Servizio dalle persone autorizzate al trattamento con mansioni di "Amministratore di Sistema", il Responsabile è tenuto altresì al rispetto delle previsioni pro tempore applicabili relative alla disciplina sugli amministratori di sistema contenute nel provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008 modificato in base al provvedimento del 25 giugno 2009. Il Responsabile, in particolare, si impegna a conservare direttamente e specificamente gli estremi identificativi delle persone fisiche preposte quali amministratori di sistema, e a fornirli prontamente al Titolare su richiesta del medesimo.

In ordine al trasferimento in Paesi terzi, il Responsabile è tenuto a:

- adottare adeguate garanzie qualora il trattamento comporti il trasferimento dei dati in Paesi Terzi.

Allegato F - “Sicurezza”

I sistemi informativi di Server Plan si basano su una rete locale utilizzata per tutte le attività.
L’accesso a internet è controllato mediante un firewall che filtra le comunicazioni secondo le regole decise.
Tutti i computer sono dotati di antivirus e sistema di backup giornaliero automatici.
Si dispone delle seguenti attrezzature:
- elaboratori con accesso a internet
- stampanti
- armadio in cui sono allocati 2 server
- Impianto di video sorveglianza

Sono installati i seguenti impianti di video sorveglianza:
un impianto atto a tutelare la sicurezza interna, è installato all’ingresso della Server Plan.

Procedure per gli incaricati del trattamento dei dati
Il trattamento dei dati viene effettuato solo da soggetti che hanno ricevuto un formale incarico mediante designazione per iscritto di ogni singolo incaricato, con la quale si individua puntualmente l’ambito del trattamento consentito. Oltre alle istruzioni generali, su come devono essere trattati i dati personali, agli incaricati vengono fornite esplicite istruzioni in merito ai seguenti punti aventi specifica attinenza con la sicurezza:

- Procedura da seguire per la classificazione dei dati, al fine di distinguere quelli giudiziari per garantire la sicurezza dei quali occorrono maggiori cautele, rispetto a quanto previsto per i dati di natura comune;
- Modalità di reperimento dei documenti contenenti i dati personali e modalità da osservare per la custodia degli stessi e la loro archiviazione al termine dello svolgimento del lavoro per il quale è stato necessario utilizzare i documenti;
- Modalità per elaborare e custodire le password necessarie per accedere agli elaboratori elettronici ed i dati in essi contenuti, nonché per fornire una copia al preposto alla custodia della parola chiave;
- Prescrizione di non lasciare incustoditi ed accessibili gli strumenti elettronici
- Screen – server con password
- Procedure e modalità di utilizzo degli strumenti e di programmi atti a proteggere i sistemi informativi
- Procedure per il salvataggio dei dati
- Modalità di custodia ed utilizzo dei supporti removibili contenenti dati personali;
- Dovere di aggiornarsi, utilizzando il materiale e gli strumenti forniti dal Titolare, sulle misure di sicurezza.

Soggetti incaricati alla gestione e manutenzione del sistema informativo
Il supporto tecnico per la manutenzione degli strumenti elettronici viene svolto dagli stessi tecnici dipendenti della Server Plan srl unipersonale.
Le lettere di incarico o di designazione degli incaricati, nonché quelle di nomina dei responsabili, vengono raccolte in modo ordinato. In tal modo il Titolare dispone di un quadro chiaro di chi fa cosa (mansionario privacy), nell’ambito del trattamento dei dati personali.
Periodicamente, con cadenza almeno annuale, si procede ad aggiornare la definizione dei dati cui gli incaricati sono autorizzati ad accedere e dei trattamenti che sono autorizzati a porre in essere, al fine di verificare la sussistenza delle condizioni che giustificano tali autorizzazioni.
La stessa operazione viene compiuta per le autorizzazioni rilasciate ai soggetti incaricati della gestione o manutenzione degli strumenti elettronici.
Sono previsti interventi formativi degli incaricati del trattamento, finalizzati a renderli edotti dei seguenti aspetti:

- Profili della disciplina sulla protezione dei dati personali, che appaiono più rilevanti per l’attività svolta dagli incaricati e delle conseguenti responsabilità che ne derivano
- Rischi che incombono sui dati

- Misure disponibili per prevenire eventi dannosi
- Modalità per aggiornarsi sulle misure di sicurezza adottate dal titolare

Tali interventi formativi sono programmati in modo tale da dare luogo al verificarsi di una delle seguenti circostanze:

- Già al momento dell'ingresso in servizio
- In occasione di cambiamenti di mansioni
- In occasione della introduzione di nuovi significativi strumenti

Analisi dei rischi

I rischi che incombono sui dati sono essenzialmente rappresentanti da:

Calamità naturali

1. Perdita di dati conseguenti ad allagamento
2. Perdita di dati conseguenti ad incendio

Minacce intenzionali

1. Accessi non consentiti:

- Accesso, furto, manomissione di dati su supporti cartacei e supporti informatici
- Accessi non autorizzati
- Perdita di dati dovuta a virus o altra intrusione informatica

Minacce involontarie

1. Black out elettrico
2. Malfunzionamenti del software
3. Malfunzionamenti dell'hardware

Misure atte a garantire l'integrità e la disponibilità dei dati

a. Calamità naturali:

1. Perdita di dati conseguente ad allagamento

Per ciò che concerne il rischio di perdita di dati da allagamento, considerata la posizione del fabbricato della sede della Server Plan, si esclude che, salvo eventi imprevedibili e del tutto eccezionali, detto rischio possa verificarsi.

Ad ogni modo le attrezzature informatiche sono state tutte rialzate da terra.

2. Perdita di dati conseguente ad incendio

Per ciò che concerne la perdita di dati conseguente ad incendio si precisa che sono state attuate tutte le misure previste dall'attuale legislazione in materia di prevenzione incendi, inclusa la verifica periodica dell'impianto elettrico, dell'impianto di riciclo dell'aria e di condizionamento

Si precisa, inoltre, che la posizione degli estintori risulta da appositi segnali affissi nei locali della sede della Server Plan.

b) Minacce intenzionali

1. accessi non consentiti

- accesso, furto, manomissione

Si evidenzia che:

- Gli ingressi della sede sono protetti da doppia serratura
- I locali nei quali si svolge il trattamento sono protetti da ingresso di allarme e ingresso sorvegliato da telecamere a circuito chiuso.

Gli incaricati devono custodire in modo appropriato gli atti, i documenti ed i supporti contenenti dati personali, loro affidati per lo svolgimento delle mansioni lavorative.

Eventuali copie di documenti, di scritti, di appunti, di tabulati di prova, ecc, vengono distrutti al termine del loro utilizzo.

E' fatto espresso divieto di utilizzare carta riciclata per stampare documenti da consegnare a terzi.

Cautele particolari sono previste per gli atti, documenti e supporti contenenti dati giudiziari:

agli incaricati viene in questi casi prescritto di provvedere al controllo ed alla custodia in modo tale che ai dati non possano accedere persone prive di autorizzazione.

- accesso, furto manomissione di dati su supporti informatici

La Server Plan ha attivato ed è correntemente funzionante un sistema di autenticazione per ognuno degli incaricati che trattano dati personali:

- Si associa un codice per identificazione dell'incaricato (username) attribuito da chi amministra il sistema, ad una parola chiave riservata (password), conosciuta solamente

dall'incaricato. Che provvederà ad elaborarla, mantenerla riservata e modificarla periodicamente.

- Per l'attribuzione e la gestione delle credenziali per l'autenticazione si utilizzano i seguenti criteri:
- Ad ogni incaricato esse vengono assegnate o associate individualmente, per cui non è ammesso che due o più incaricati possano accedere agli strumenti elettronici utilizzando le medesime credenziali.
- Il codice per l'identificazione (username) attribuito all'incaricato da chi amministra i sistemi, è univoco; esso non può essere assegnato ad altri incaricati neppure in tempi diversi.
- Viene segnalato agli incaricati che la lunghezza della password da utilizzare non deve essere inferiore ad 8 caratteri, salvo limitazioni tecniche nei software in uso
- Agli incaricati è prescritto di utilizzare alcuni accorgimenti nell'elaborazione delle password:
- esse non devono contenere riferimenti agevolmente riconducibili all'interessato (non solo nomi, cognomi, soprannomi, ma neppure date di nascita proprie, dei figli e di amici), né consistere in nomi noti anche di fantasia (Pippo, Pluto, Paperino..)
- Buona norma è che dei caratteri che costituiscono la password , da un quarto alla metà sia di natura numerica.
- La password non deve essere comunicata a nessuno (non solo soggetti esterni, ma neppure persone appartenenti all'organizzazione, siano essi colleghi, responsabili del trattamento, amministratori di sistema o titolari)
- Nei casi di prolungata assenza o impedimento dell'incaricato, che renda indispensabile o indifferibile per esclusive necessità di operatività e di sicurezza del sistema, potrebbe, però, rendersi necessario disporre della password dell'incaricato per accedere agli strumenti ed ai dati.

A tal fine, agli incaricati sono state fornite istruzioni scritte affinchè essi:
scrivano la parola chiave su un foglio di carta da inserire in una busta che deve essere chiusa e sigillata;
consegnino la busta a chi custodisce le copie delle parole chiave, il cui nominativo viene loro indicato al momento dell'attribuzione della password.
Solo al verificarsi delle condizioni sopra esposte che rendono necessario accedere allo strumento elettronico, utilizzando la copia della parola chiave, il titolare o un responsabile potranno richiedere la busta che la contiene a chi la custodisce.
Dell'accesso effettuato si dovrà provvedere ad informare tempestivamente l'incaricato cui appartiene la parola chiave.
Viene segnalato ad ogni incaricato la necessità di cambiare la password almeno ogni 6 mesi.
Al verificarsi dei seguenti casi è prevista la disattivazione delle credenziali di autenticazione:

- Immediatamente nel caso in cui l'incaricato perda la qualità che gli consentiva di accedere allo strumento;
- In ogni caso entro 6 mesi di mancato utilizzo

Il sistema di identificazione ed autenticazione è operativo anche sui computer portatili, sui cellulari che possono gestire e contenere dati personali.
Per quanto concerne i supporti removibili (chiavette, hard disk e removibili) contenenti i dati personali, la norma impone particolari cautele sono nel caso in cui essi contengano dati giudiziari.
Tuttavia, il titolare del sistema ha vietato categoricamente l'uso degli stessi nell'ambiente lavorativo.

1. Accessi non autorizzati

Per quanto concerne il rischio di accessi non autorizzati, non appare necessario prevedere profili di autorizzazione distinti per le diverse persone, in relazione alle limitate dimensioni della struttura del titolare ed al fatto che non si ravvisano ragioni di tutela della riservatezza tali da imporre che uno o più incaricati non possano accedere ad alcune tipologie di dati personali oggetto di trattamento.

1. Perdita di dati dovuta a virus o intrusioni informatiche

a. Virus

Per ciò che concerne la perdita di dati o di danneggiamento degli stessi dovuta a virus, si precisa che:

- I personal computer in dotazione alla sede sono dotati di programmi antivirus

b. Intrusione informatica

Relativamente all'intrusione informatica da parte di terzi, si precisa che è stato installato un firewall hardware le cui direttive ed indicazioni sono state fornite dal responsabile dell'area tecnica.

Anche in relazione a questo rischio non si registrano inconvenienti occorsi, sicchè si reputa il sistema di protezione rispondente alle necessità della sede.

c. Minacce involontarie

- Black out elettrico

La sede si è dotata di un gruppo di continuità per prevenire le conseguenze dei black out elettrici o dei picchi di sovra o sotto tensione elettrica.

- Malfunzionamento del software

A tal riguardo Server Plan si è da tempo dotata di programmi, che possiedono una funzionalità che consente l'aggiornamento automatico del sistema mediante l'installazione delle PATCH rilasciate dalla case madre volte a prevenire errori di protezione o malfunzionamento del software stesso.

Si ottempera così alla disposizione di legge che obbliga il titolare del trattamento a provvedere ad aggiornare con cadenza almeno annuale i software degli strumenti elettronici.

La suddetta cadenza annuale diviene semestrale per gli strumenti con i quali si trattano i dati giudiziari.

Malfunzionamenti hardware

La manutenzione degli strumenti elettronici a livello hardware viene svolta dagli stessi tecnici della Server Plan

1. Criteri e modalità di ripristino dei dati in seguito a distruzione o danneggiamento

Back up dati

Al fine di garantire non solo la integrità ma anche la pronta disponibilità dei dati, la Server Plan si è dotata dei seguenti strumenti e procedure di back up:

- Server esterno

Tutti i dati personali gestiti con strumenti elettronici nella sede vengono inclusi nella procedura di backup. La frequenza con cui vengono effettuate le copie di sicurezza è giornaliera.

Il tempo necessario per recuperare i dati delle copie di sicurezza, a fronte di una generica emergenza, viene stimato in poche ore dal verificarsi del possibile accadimento, comunque, ampiamente sotto il limite dei 7 giorni previsti dal punto 23 dell'all. B del D. Lgs 196/2003.

Il ripristino avviene mediante apposito programma di restore in dotazione all'unità preposta al backup.

Protezione dei contenuti

Attraverso le reti private virtuali è possibile connettere in modo sicuro sedi distaccate di un'azienda o singole postazioni. Grazie alla crittografia i dati viaggiano protetti anche su reti aperti come se si fosse all'interno di reti locali private. Attivando un firewall si ha a disposizione fino a 750 VPN native su tecnologia CISCO ASA.

Back orario

E' la scelta ideale per progetti con contenuti aggiornati di frequente. E' la garanzia di uno snapshot orario dei dati, immediatamente disponibile in farm per il ripristino completo del sistema.

Backup disponibili

I backup e restore sono eseguibili in qualsiasi momento grazie alla comoda interfaccia web accessibile via browser.

Il sito ed i contenuti saranno subito online in caso di accidentale perdita dei dati, con pochi semplici click.

Protezione dei dati con R1- Soft CDP

Il sistema più affidabile per i backup continui dei dati. Basato su R1- Soft, con backup orario si ha la semplicità del migliore pannello di controllo per tenere al sicuro i dati anche in maniera selettiva.

Sicurezza e disaster recovery

La vera garanzia di un backup e la rapidità e facilità di ripristino.
Con backup orario si può effettuare alla massima velocità il ripristino dell'intero file system o solamente del database a partire da qualsiasi snapshot disponibile.

Backup su server Dell

Gli snapshot vengono salvati su server Dell, la soluzione più avanzata sul mercato con le migliori performance per stabilità, sicurezza e velocità.

Web farm (ubicata in Roma – Via di Tor Cervara, 282/a)

Di seguito le principali caratteristiche dal datacenter ubicato in Italia.

- Webfarm fisicamente isolata
- Sistema di controllo degli accessi con badge e codice numerico a più livelli
- Armadio rack dedicato alla conservazione dei log con sistema di accesso biometrico
- Sistema di rilevamento antintrusione
- Presidio con agente di vigilanza H24 per 7 giorni su 7
- Telecamere a circuito chiuso e archiviazione digitale delle riprese
- Sistemi di rilevamento antifumo, antiincendio ed antiallagamento
- Trasformatori principali ridondanti al 100%
- Gruppi di continuità ridondati al 100%
- Gruppi elettronici con tempo di rilevazione minori di 10 secondi
- Armadi rack con doppia alimentazione e potere di interruzione del corto circuito al primo interruttore a monte del rack
- Impianto di condizionamento ridondato al 100%
- Climatizzazione completa in grado di mantenere un delta < 1°
- Singolo armadio rack con condizionamento forzato ed estrattore di calore dall'alto
- Continuità ed affidabilità di servizio oltre il 99, 99%
- Firewall di fornitori diversi per limitare i rischi dovuti alle potenziali vulnerabilità

Tutti i sistemi di supporto del datacenter sono ampliamente ridondati e dotati di sistema di monitoraggio che consentono una reazione tempestiva a qualsiasi anomalia e rendono esiguo il rischio di interruzione del servizio.

Sono, inoltre, protetti da sofisticati sistemi di sicurezza in grado di rilevare ed impedire tempestivamente qualsiasi intrusione dall'esterno.

Il Quality managment system della web farm è certificato ISO 9001, ISO 14001 , OH SAS 18001, SA 8000 e ISO 27001.