

Nomina a Responsabile del Trattamento

TRA

FONDAZIONE DOMENICO BERNACCHI GERLI ARIOLI ONLUS, in persona del legale rappresentante, **GIUSEPPE BASSI**, nato a Seveso (MI) il 5/1/1946, residente a Gavirate (VA), via Case Nuove n. 6, C.F. BSSGPP46A05I709Z, con sede legale in **GAVIRATE (VA), VIA G. FERRARI n. 11, P. IVA 01485670127** e **CODICE FISCALE 83002910129**, nella sua qualità di Titolare del trattamento dei dati personali
(di seguito "**Titolare**")

E

La società **MYGO S.r.l.**, con sede legale in Roma, Piazza Crati n. 20, Codice Fiscale, Partita Iva e Codice Fiscale 14356531005, nella sua qualità di Responsabile del trattamento dei dati personali
(di seguito "**MYGO**", il "**Responsabile**")

FONDAZIONE DOMENICO BERNACCHI GERLI ARIOLI ONLUS e **MYGO**

sono collettivamente definite le "**Parti**"

premessi che

- ai sensi del contratto concluso tra il Titolare e il Responsabile (il "**Contratto**"), il Responsabile fornisce al Titolare i servizi indicati nel Contratto (i "**Servizi**");
- ai fini della fornitura dei Servizi, il Responsabile può ricevere, avere accesso e trattare le informazioni del Titolare che possono essere considerate dati personali ai sensi del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016, sulla protezione dei dati personali e sulla libera circolazione di tali dati (il "**Regolamento**") e altre leggi e disposizioni sulla protezione dei dati applicabili (i "**Dati**");
- che **FONDAZIONE DOMENICO BERNACCHI GERLI ARIOLI ONLUS** intende conformarsi alle disposizioni del Regolamento, provvedendo, in questa fase, alla nomina di un Responsabile del trattamento dei dati ai sensi dell'art. 28 del Regolamento;
- il Responsabile possiede competenze e conoscenze tecniche in relazione alle finalità e ai metodi delle operazioni di trattamento, le misure di sicurezza da adottare per garantire la riservatezza, l'integrità e la completezza dei dati trattati e le disposizioni relative alla protezione dei dati personali;
- che, quanto al significato della terminologia tecnico-giuridica usata nel presente atto di nomina, le seguenti qualifiche o definizioni sono individuate, vanno interpretate, ed eventualmente integrate, sulla base ed in conformità delle corrispondenti qualifiche o definizioni generali contenute nell'art.4, co. 1, del Regolamento:
 - "**Titolare**": *"la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali"*;
 - "**Responsabile**": MYGO ovvero *"la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento"*;
 - "**Interessato**": la persona fisica - identificata o identificabile - a cui si riferiscono i dati, in particolare i dipendenti e i collaboratori del Titolare nonché ogni altra persona fisica della quale il Titolare tratti i dati personali sulla scorta di una delle basi giuridiche del trattamento di cui al Regolamento;
 - "**Dato personale**": qualunque informazione riguardante l'Interessato, ovvero *"qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale"*;
 - "**Trattamento**": *"qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o 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"*;
 - "**Le persone autorizzate al trattamento dei dati personali**" o "**Incaricati**": le persone fisiche autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;
 - "**Categorie particolari di dati personali**": dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.

TUTTO CIÒ PREMESSO

al fine di fornire adeguate misure di salvaguardia rispetto al trattamento dei dati personali e dei diritti libertà fondamentali dell'individuo, le Parti convengono quanto segue.

1. Oggetto del trattamento:

Con il presente atto di nomina (la "**Nomina**"), il Titolare affida al Responsabile, che accetta, l'incarico di effettuare, per suo conto, le operazioni di trattamento dei Dati personali funzionali alla corretta esecuzione del Contratto e impartisce le necessarie istruzioni come di seguito specificati.

Salvo ove diversamente specificato nel presente atto di nomina, la durata del trattamento coinciderà con la durata di vigenza del Contratto.

2. Tipi di dati personali, categorie di interessati, finalità del trattamento

Il Trattamento avrà per oggetto e finalità quanto segue:

- a) Tipo di dati personali: nome, cognome, indirizzo email;
- b) Categorie di interessati: i dipendenti e i collaboratori del Titolare nonché ogni altra persona fisica della quale il Titolare tratti i dati personali sulla scorta di una delle basi giuridiche del trattamento di cui al Regolamento;
- c) Finalità del trattamento: **esecuzione del Contratto ed espletamento dei Servizi ivi previsti con particolare riferimento alla** comunicazione tracciata da parte del Titolare ai propri dipendenti e collaboratori.

3. Natura del trattamento:

Salvo le istruzioni particolari di seguito indicate e quanto previsto all'art. 4 che segue, il Responsabile è autorizzato, su richiesta del Titolare, a porre in essere le seguenti attività:

- raccolta;
- elaborazione;
- memorizzazione su supporti elettronici;
- stampa;
- registrazione;
- organizzazione;
- strutturazione;
- conservazione;
- adattamento o la modifica;
- estrazione;
- consultazione;
- uso;
- comunicazione mediante trasmissione;
- raffronto o l'interconnessione;
- diffusione o qualsiasi altra forma di messa a disposizione;
- limitazione;
- cancellazione o la distruzione;
- altro;

nei limiti del consenso prestato dagli interessati del trattamento, le istruzioni di trattamento fornite dal Titolare ed in funzione del corretto espletamento dei Servizi.

4. Istruzioni al e obblighi del Responsabile

Il Responsabile si obbliga a osservare, e far osservare ai propri dipendenti e collaboratori, le seguenti istruzioni in materia di trattamento dei dati personali:

- a) trattare i dati personali in modo lecito, secondo correttezza, nel rispetto di quanto disposto dal Regolamento, dalla normativa nazionale in materia di protezione dei dati personali applicabile, dalle disposizioni, decisioni e/o regolamenti, provvedimenti e decisioni adottati dalle Autorità Garanti per la protezione dei dati personali, tra cui i Provvedimenti dell'Autorità Garante per la Protezione dei dati Personali italiana (il "**Garante**"), e dal Gruppo di lavoro costituito ex Articolo 29 della Direttiva 95/46 CE del 13 luglio 2011 / Comitato europeo per la protezione dei dati;
- b) **garantire il rispetto delle disposizioni di cui all'art. 28 del Regolamento;**
- c) **individuare e designare gli Incaricati e fornire loro le relative istruzioni, coerenti al presente atto di nomina, per un corretto e lecito trattamento dei Dati personali;**
- d) **vigilare sull'operato degli Incaricati;**

- e) consentire l'accesso degli Incaricati ai soli Dati personali la cui conoscenza sia strettamente necessaria per adempiere ai compiti loro assegnati, imponendo agli stessi, negli atti di designazione, il rispetto dell'obbligo di riservatezza in merito ai Dati trattati;
- f) effettuare le operazioni di trattamento dei Dati unicamente per **finalità** inerenti all'esecuzione del rapporto contrattuale, con divieto esplicito di utilizzare tali dati per scopi o finalità diversi da quelli indicati nel Contratto;
- g) non cedere, trasferire, comunicare e/o fornire copia, totale o parziale, in qualsiasi modo e sotto qualsiasi formato, dei Dati Personali a terzi, se non su specifica autorizzazione scritta del Titolare;
- h) in caso di necessità di ricorrere a terzi **sub-fornitori** al fine del corretto adempimento delle operazioni di trattamento, il Responsabile si obbliga a:
 - i. ottenere l'autorizzazione preventiva del Titolare;
 - ii. fornire idonee istruzioni di trattamento, imponendo il pieno ed incondizionato rispetto delle misure di cui alla presente clausola;
 - iii. prevedere garanzie idonee per garantire l'attuazione di misure tecniche ed organizzative adeguate a far garantire il rispetto della vigente normativa e del Regolamento;
 - iv. vigilare sull'operato dei terzi sub-fornitori;
 - v. nel caso in cui un sub-fornitore sia stabilito al di fuori dell'UE / SEE in un paese che non fornisce un livello adeguato di protezione dei dati, il Responsabile del trattamento dovrà (a) garantire che il titolare del trattamento e il sub-fornitore sottoscrivano un accordo per il trattamento dei dati basato sulle Clausole Contrattuali Standard per il Trasferimento di Dati Personali ai Responsabili stabiliti in Paesi Terzi ai sensi della Decisione della Commissione 2010/87 / UE del 5 febbraio 2010, oppure (b) fornire al Titolare del trattamento informazioni sulla certificazione del subfornitore, il ai sensi del Privacy Shield e regolarmente, almeno una volta l'anno, confermare che la certificazione è ancora valida, o (c) fornire al Titolare del Trattamento altre informazioni e documentazione sul meccanismo relativo ai trasferimenti internazionali dei dati ai sensi dell'articolo 46 del Regolamento utilizzato per trasferire legittimamente i dati del Titolare al subfornitore.
- i) attenersi alle **istruzioni** di volta in volta ricevute dal Titolare al fine di conservare i dati per un tempo non eccedente quello necessario per gli scopi per il quale i dati stessi sono stati raccolti;
- j) collaborare con il Titolare al fine di **garantire** all'interessato che ne faccia richiesta l'effettivo esercizio dei **diritti** previsti dagli artt. da 15 a 22 del Regolamento;
- k) fornire al Titolare tutte le informazioni utili ai fini della tenuta del proprio Registro ove richiesto e redatto dal Titolare sempre che MYGO abbia deciso di dotarsene;
- l) assistere il Titolare qualora questo intenda effettuare una **valutazione di impatto** sulla protezione dei dati personali ai sensi dell'art. 35 del Regolamento relativa ad un trattamento svolto dal Responsabile per conto del Titolare;
- m) adottare i provvedimenti tecnici e di buon senso per predisporre un sistema di **sicurezza** idoneo a rispettare le prescrizioni degli artt. 32 e ss. del Regolamento per prevenire e/o evitare i rischi connessi al trattamento. In particolare, ai sensi del Regolamento, il Responsabile si obbliga, tenuto conto dello stato dell'arte, a mettere in atto misure tecniche ed organizzative adeguate a garantire un livello adeguato di sicurezza dei Dati personali trattati. Tali misure includono, a titolo esemplificativo e non esaustivo, le misure minime indicate nell' **Allegato 1**;
- n) adottare le misure ed adempiere alle prescrizioni di cui al Provvedimento del Garante del 27 novembre 2008 - *Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema* (il "Provvedimento");
- o) consentire al Titolare l'esercizio del potere di **controllo**, ai sensi del Regolamento, al fine di verificare il rispetto delle istruzioni di trattamento fornite e, in generale, del Regolamento;
- p) effettuare un monitoraggio periodico ed eventuale adeguamento (ove necessario) delle misure di sicurezza fisiche, tecniche e organizzative adottate. Nel caso di modifica o integrazione della normativa in materia di protezione dei dati applicabile, il Responsabile dovrà conformarsi alle nuove norme e implementare, ove necessario, le misure di sicurezza richieste;
- q) non trasferire, senza previa comunicazione e autorizzazione dal Titolare, i dati personali al di fuori del territorio della UE/SEE. Nel caso in cui il Titolare autorizzi tale trasferimento, il Responsabile dovrà implementare la documentazione e le azioni richieste dal Titolare per assicurare che il trasferimento avvenga in conformità al Regolamento e alle altre normative nazionali applicabili in materia di protezione dei dati personali;
- r) nel caso di trattamento di categorie speciali di dati ai sensi del Regolamento e/o dati personali relativi a condanne penali e reati, il Responsabile dovrà osservare i relativi requisiti stabiliti dal Regolamento e dalle altre normative nazionali applicabili, incluse le misure di sicurezza, e dovrà assicurare la conformità alle norme anche non espressamente richiamate nella presente nomina;

- s) comunicare al Titolare senza ritardo, comunque entro e non oltre le 24 ore, e per iscritto ogni **"Violazione dei dati personali"** ("*data breach*"), da intendersi quale *"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 trasmessi, conservati o comunque trattati"*. In particolare il Responsabile garantirà il rispetto delle prescrizioni di cui all'art. 33 del Regolamento e fornirà al Titolare una descrizione dettagliata:
- i. della Violazione verificatasi,
 - ii. dei Dati personali interessati (comprensivi delle categorie e del numero approssimativo degli interessati),
 - iii. delle categorie e del numero approssimativo delle registrazioni dei dati personali interessati,
 - iv. delle probabili conseguenze della Violazione,
 - v. nonché ogni ulteriore informazione e/o documentazione richiesta dal Titolare, non appena disponibili;
- t) informare prontamente il Titolare circa ogni richiesta del Garante o altra autorità;
- u) attenersi ad ogni ulteriore istruzione di volta in volta ricevuta dal Titolare in merito al trattamento dei dati personali;
- v) rendere tempestivamente al Titolare ogni informazione in ordine a qualsiasi questione rilevante ai sensi e per gli effetti del Regolamento a ogni altra normativa applicabile in materia di protezione dei dati personali.
- w) il Responsabile ha diritto di informare immediatamente il Titolare qualora, a suo parere, una delle istruzioni fornite dal Titolare stesso, o di cui al presente atto, violi il Regolamento o altre disposizioni, nazionali o dell'Unione Europea, in materia di protezione di dati.
- x) il Responsabile riconosce che le credenziali di autenticazione (come user-id e password) e, in generale, qualsiasi codice di identificazione e accesso fornito per accedere e trattare i Dati ai fini dei servizi di cui al Contratto, devono essere utilizzati solo nella misura necessaria per fornire tali servizi e in conformità con le istruzioni, le regole e le procedure esistenti del Titolare. Il Responsabile riconosce che tali credenziali e codici sono confidenziali e segreti e devono essere archiviati in modo tale da impedire l'accesso non autorizzato e non devono essere divulgati a terzi, salvo che siano necessari dal punto di vista funzionale per la fornitura dei servizi e in conformità con la Nomina e con le istruzioni del Titolare.

Il Responsabile, con la sottoscrizione della presente Nomina, accetta la Nomina a Responsabile, conferma la diretta ed approfondita conoscenza degli obblighi che si assume in relazione al dettato della normativa richiamata, si impegna a procedere al trattamento dei dati personali correttamente ed in modo lecito, in conformità al Contratto e all'incarico ricevuto.

Resta inteso tra le Parti che il corrispettivo pattuito tra le parti per la prestazione dei servizi di cui al Contratto deve intendersi comprensivo anche della remunerazione dell'attività di Responsabile del trattamento.

5. Durata

La Nomina sarà efficace per l'intera durata del Contratto, comprese eventuali estensioni e rinnovi. In caso di cessazione del Contratto per qualsiasi motivo, la Nomina sarà automaticamente revocata. Qualsiasi revoca della Nomina non avrà alcun effetto sulla validità e l'efficacia delle altre clausole del Contratto e sull'adempimento degli obblighi contrattuali del Responsabile del trattamento. In caso di revoca della Nomina per qualsiasi motivo, il Titolare ed il Responsabile coopereranno al fine di assicurare che i Dati vengano trattati in conformità alle normative in materia di dati personali applicabili e il Regolamento.

Il Responsabile dovrà inoltre restituire tempestivamente al Titolare o a soggetti terzi indicati per iscritto dal Titolare tutta la documentazione e i dispositivi contenenti i Dati trattati o acquisiti durante l'esecuzione del Contratto e qualsiasi copia correlata, in qualsiasi formato, inclusa ogni copia detenuta da terzi che hanno collaborato con il Responsabile per fornire i servizi oggetto del Contratto.

Su richiesta scritta del Titolare, il Responsabile dovrà distruggere detta documentazione. In caso di effettiva e tecnica impossibilità di cancellare i Dati trattati per via elettronica secondo quanto sopra, il Responsabile dovrà adottare tutte le misure necessarie per rendere i Dati non accessibili, non recuperabili e non modificabili e qualsiasi uso correlato dovrà essere severamente vietato.

6. Garanzie del Titolare in rapporto al trattamento dei dati

Il Titolare garantisce che il trattamento dei dati, compreso il loro trasferimento in formato cartaceo o elettronico presso il Responsabile, è effettuato e continuerà ad essere effettuato nel pieno rispetto di tutte le disposizioni vigenti in materia.

In particolare, il Titolare dichiara e garantisce la legittimità delle modalità di raccolta dei dati trattati dal Responsabile per conto del Titolare nell'esecuzione del Contratto, il regolare assolvimento degli obblighi

normativi posti a carico del Titolare nei confronti degli Interessati, nonché la coerenza alle norme previste in materia dei trattamenti su di essi effettuati e si impegna, pertanto, a tenere indenne il Responsabile per ogni conseguenza dannosa che dovesse derivare a carico di quest'ultimo a causa dell'inadempimento a tali dichiarazioni.

7. Disposizioni finali

L'eventuale tolleranza di comportamenti posti in essere da una o entrambe le parti in violazione delle disposizioni contenute nella presente nomina non costituisce rinuncia ai diritti derivanti dalle disposizioni violate né al diritto di esigere l'esatto adempimento delle obbligazioni e il rispetto di tutti i termini e le condizioni previste nella nomina stessa.

Il Titolare e il Responsabile convengono che la nullità o l'inefficacia di singole disposizioni o clausole della presente nomina non comporterà la nullità o l'inefficacia dell'intera nomina.

La presente nomina è regolata dalla legge italiana.

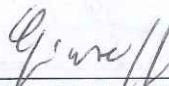
Per qualsiasi controversia inerente la validità, l'interpretazione, l'esecuzione o la risoluzione della presente nomina sarà territorialmente competente, in via esclusiva, il Tribunale di Roma.

Gavirate, lì 18 dicembre 2023

Roma, lì 18 dicembre 2023

Titolare

Responsabile
MYGO S.R.L.


Giuseppe Bassi
Presidente




Davide Caizzo
Amministratore Delegato

ALLEGATO 1

Misure di sicurezza

Fatta salva la responsabilità ed il dovere del Responsabile di valutare e adottare ogni ulteriore misura tecnica e organizzativa adeguata per garantire che il trattamento posto in essere avvenga nel rispetto dei requisiti richiesti dal Regolamento ed assicuri la protezione dei diritti degli Interessati, il presente allegato descrive le misure minime di sicurezza che devono essere adottate dal Responsabile del trattamento (ove applicabile).

Misure di sicurezza	Commenti
Mettere in sicurezza lo stabile che ospita l'infrastruttura IT utilizzata per elaborare e trasferire i dati	I dati della piattaforma My Governance sono conservati sui server Europei di AWS Amazon, ad eccezione di quelli di My Whistleblowing che, invece, sono sui server Europei di Microsoft Azure
Limitare il numero di soggetti autorizzati ad accedere ai dati e all'infrastruttura IT utilizzata per elaborare e trasferire i dati	La società che fa manutenzione alla piattaforma è stata debitamente individuata come Amministratore di Sistema
Assicurare un approvvigionamento energetico continuo all'infrastruttura IT utilizzata per elaborare i dati, in particolare dotandola di sistemi energetici di emergenza	Grazie alla società terza che garantisce la continuità del Data Center (DC) si assicurerà un approvvigionamento energetico continuo all'infrastruttura IT utilizzata per elaborare i dati, in particolare dotandola di sistemi energetici di emergenza
Assicurare che l'accesso ai dati avvenga in maniera controllata	L'accesso ai dati può avvenire solo in maniera controllata, grazie agli alti standard di sicurezza con cui viene protetto il DC e alla criptazione dei dati
Assicurare che i dati siano protetti da perdita o distruzione accidentale	Per assicurare che i dati siano protetti da perdita o distruzione accidentale si utilizzano copie di backup dislocate in posizioni geografiche differenti. Tale livello di protezione ridurrà al minimo la possibilità di perdita e comunque nel caso dovesse avvenire sarà sicuramente molto limitata.
Assegnare ad ogni soggetto coinvolto nel trattamento delle credenziali di autenticazione composte da un codice per l'identificazione (" User ID ") associato a una parola chiave (" password ")	Ogni soggetto coinvolto nel trattamento delle credenziali di autenticazione composte da un codice per l'identificazione (" User ID ") associato a una parola chiave (" password ") secondo gli standard migliori oggi presenti sul mercato. Password con sicurezze minime garantite
La password riservata, conosciuta solamente dall'assegnatario (" Utente ") deve avere quantomeno le seguenti caratteristiche: 1. essere composta da almeno 8 caratteri; 2. contenere lettere maiuscole e minuscole in combinazione con 3. numero o caratteri speciali; 4. non deve contenere lo User ID; 5. deve essere obbligatoriamente modificata al primo utilizzo e dopo il 6. reset della password; 7. deve essere modificata almeno ogni 60 giorni.	La password di accesso dovrà rispettare quantomeno i seguenti requisiti: <ul style="list-style-type: none">• almeno 8 caratteri• almeno una lettera maiuscola• almeno una lettera minuscola• almeno un simbolo speciale• almeno un numero Al quinto tentativo errato di inserimento di una password l'utenza verrà bloccata per 30 minuti.

Assicurare che lo User ID assegnato ad un Utente non possa essere assegnato ad un altro incaricato in tempi diversi	Questo deve essere garantito dal Titolare in quanto lo user ID è l'indirizzo email
Assicurarsi che le credenziali vengano disattivate in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali	Questo dovrà essere eseguito dal Titolare che provvederà a rimuovere gli utenti dall'anagrafica. Tali utenti avranno in ogni caso accesso ai documenti già approvati.
Assicurare che: i. quando per gli incaricati sono individuati profili di autorizzazione di ambito diverso venga utilizzato un sistema di autorizzazione. ii. i profili di autorizzazione, per ciascun incaricato o per classi omogenee di incaricati, siano individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento. iii. periodicamente, e comunque almeno annualmente, verificare la sussistenza delle condizioni per la conservazione dei profili di autorizzazione	Confermato
Proteggere i dati il rischio di intrusione e dell'azione di programmi di cui all'art. 615-quinquies del codice penale: i. mediante l'attivazione di idonei strumenti elettronici da aggiornare con cadenza quotidiana; ii. effettuare aggiornamenti periodici dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti su base quotidiana	Confermato
Assicurare che il trattamento avvenga utilizzando software (ivi incluso il sistema operativo, il middleware e le applicazioni) dotati di funzioni di sicurezza all'avanguardia	Confermato
Assicurare che sia effettuato un back-up almeno con frequenza quotidiana	Grazie alla società terza proprietaria dei server si assicurerà che sia effettuato un back-up almeno con frequenza quotidiana
Assicurare che i dati possano essere recuperati entro un determinato termine massimo (non più di 7 giorni)	Sì
Garantire che i dati utilizzati per l'autenticazione siano protetti con efficaci misure di sicurezza crittografica	Sì
Assicurarsi che i dati trasferiti siano protetti utilizzando procedure di crittografia aggiornate	Sì
Le categorie particolari di dati personali sono protette utilizzando procedure di crittografia aggiornate	Normalmente non vengono trattate categorie particolari di dati personali ma in ogni caso i dati in nostro possesso sono sempre crittografati
Assicurarsi che sia possibile verificare e stabilire se e chi ha avuto accesso o ha inserito, ha modificato o cancellato i dati nei sistemi di elaborazione dati. I log devono essere disponibili per almeno un anno	Confermato
Garantire che siano regolarmente eseguiti test di vulnerabilità e di penetrazione	Cadenza annuale

Qualora una violazione o vulnerabilità sia identificata nell'ambito del trattamento o in qualsiasi sistema utilizzato per fornire i servizi del Responsabile, informare immediatamente il Titolare del trattamento in merito all'evento e alle misure adottare per porvi rimedio	Sì
Garantire che l'accesso ai dati sia limitato ai soli dati necessari per effettuare le operazioni di trattamento.	Sì by default
Limitare il numero di Incaricati autorizzati a svolgere attività connesse al trattamento dei dati	Sì by default
Erogare apposita formazione nei confronti degli Incaricati con riferimento alla normativa vigente in materia di tutela dei dati personali, alle misure di sicurezza	Sì
Mantenere una lista aggiornata degli Incaricati	Presente
Mantenere una copia di riserva aggiornata dei dati e del software utilizzato per il trattamento	Presente
Garantire che i Dati vengano archiviati applicando misure idonee a proteggerli da accessi non autorizzati, modifiche, danni e distruzione	Presente
Assicurarsi che i dati vengano cancellati in modo irreversibile in caso di sostituzione o riutilizzo dell'hardware	Sì by default
Escludere o limitare le copie dei dati (incluse le stampe) e assicurare la corretta distruzione dopo l'utilizzo	Sì by default
Proteggere i documenti cartacei contenenti dati utilizzati durante l'elaborazione al momento della stampa, archiviazione, distruzione e scambio	Non viene utilizzato alcun documento cartaceo
Garantire la sicurezza della rete su cui viene eseguito il trattamento (sistema firewall, proxy, sistemi di rilevamento delle intrusioni o altri dispositivi attivi o passivi)	Presente