



Autore	Ufficio Privacy Zucchetti Spa
Approvazione	Alessandro Zucchi

Versione Revisione

Versione	Autore	Consultazione DPO	Data emissione	Motivo della revisione
0.0	Ufficio Privacy	28/11/2024	03/12/2024	Prima emissione
1.0	Ufficio Privacy	18/06/2025	18/06/2025	Inserito Partner PAR-TEC quale fornitore di attività di assistenza sistemistica estesa H24. Aggiornato nome rappresentante legale.
2.0	Ufficio Privacy	07/01/2026	07/01/2026	Variazione indirizzo sede Zucchetti Spa ed inserita Z Holding Spa come DPO

PARERE DPO
OK.



SOSTENIBILE.CLOUD

RESPONSABILE DEL TRATTAMENTO					
Denominazione	Zucchetti Spa				
Partita Iva	05006900962				
Indirizzo	Piazza Mino Zucchetti,1				
Città	Lodi	Cap	26900	PV	LO
Legale Rappresentante	Alessandro Zucchetti preposto della società CONVERTENDO SRL, Legale rappresentante di Zucchetti SPA				
STRUTTURA ORGANIZZATIVA					
Divisione	Commercialisti	Responsabile Divisione	Mario Pedrazzini		
Area	Post-Vendita	Responsabile Reparto	Germana Meomartini		
INCARICATI DEL TRATTAMENTO					
Addetti analisi, sviluppo, controllo qualità, help desk, consulenti applicativi, sistemisti					
DATI DI CONTATTO					
Responsabile del trattamento	Zucchetti Spa	ufficio.privacy@zucchetti.it	03715941		
Responsabile protezione dati (DPO)	Z Holding Spa	dpo@zucchetti.it	03715943191		
DESCRIZIONE					
Sostenibile.cloud rappresenta una suite di servizi digitali per le imprese per sviluppare, monitorare e rendicontare la loro sostenibilità aziendale. Il Servizio è descritto all'interno della documentazione tecnica e del contratto di servizio e assistenza La Suite è sviluppata dal produttore Sostenibile.cloud che, nell’ambito dell’erogazione del servizio potrebbe svolgere assistenza di II livello nei confronti del Cliente. Zucchetti, erogherà il servizio e svolgerà assistenza di I livello.					
FINALITA' DEL TRATTAMENTO					
La finalità del trattamento è quella di erogare i servizi di assistenza e manutenzione al Titolare.					
CATEGORIA INTERESSATI					
- Dipendenti e collaboratori del Cliente Titolare del Trattamento - Clienti e Fornitori del Cliente Titolare del Trattamento - Soci e Amministratori del Cliente Titolare del Trattamento					
CATEGORIE DI DATI PERSONALI					
Dati personali inseriti dal Cliente all'interno del software: - Dati identificativi - Indirizzi e-mail dei collaboratori e di terzi - Dati finanziari - Dati relativi alle attività di assistenza Non è previsto il trattamento di particolari categorie di dati e di dati giudiziari (artt. 9 e 10 del GDPR).					
CATEGORIA DI DESTINATARI A CUI I DATI POTRANNO ESSERE COMUNICATI					



Fornitori di Servizi Cloud Aziende del gruppo Zucchetti Subappaltatori PAR-TEC S.p.A. quale partner fornitore di attività di assistenza sistemistica estesa H24
--

TRASFERIMENTO DATI ALL'ESTERO

No

TERMINI PER LA CANCELLAZIONE DEI DATI
--

90 giorni decorrenti dalla cessazione del contratto



DESCRIZIONE GENERALE DELLE MISURE DI SICUREZZA TECNICHE E ORGANIZZATIVE

1. MISURE DI SICUREZZA IMPLEMENTATE NEI SOFTWARE

Le misure di sicurezza configurabili nel sistema applicativo sono:

- *Gestione credenziali di accesso*
- User name: l'accesso al sistema avviene solo attraverso l'identificazione univoca del soggetto che vi accede. Nel sistema ci sono delle credenziali amministrative riservate ai tecnici di Sostenibile.cloud finalizzate alla configurazione, all'assistenza ed al mantenimento del software
- L'utente registrato in fase di contrattualizzazione ("master"), avrà la possibilità di creare altri utenti dipendenti dal proprio account ("collaboratori", "read only"). Questi utenti saranno identificati univocamente all'interno del sistema. Le regole di complessità / scadenza / gestione password saranno uguali per tutte le tipologie di utente.
- L'utente "master" avrà la facoltà di assegnare / revocare agli utenti "read only" e "collaboratori" diritti di visibilità e modifica sui dati delle aziende di sua competenza.
- L'utente "master" avrà la facoltà di disattivare gli account a lui legati. Le informazioni legate agli account disattivati, rimarranno comunque nel sistema fino alla cancellazione dell'account "master"
- L'utente "master" continuerà ad avere diritti di visibilità sui dati delle aziende di sua competenza, anche se assegnate ad utenti "collaboratori" o "read only".
- Password: le regole di complessità della password sono preimpostate e prevedono:
 - lunghezza minima 8 caratteri
 - almeno un carattere minuscolo
 - almeno un carattere maiuscolo
 - almeno un carattere speciale
 - almeno un numero
 - diversa dalle ultime 4 utilizzate
 - diversa da username
 - diversa da emailLa password ha validità 180 giorni, trascorsi i quali il sistema chiederà la modifica prima di eseguire l'accesso.
- Disattivazione/disabilitazione credenziali: Le credenziali verranno automaticamente disattivate trascorsi 15 giorni dalla scadenza del contratto e cancellate trascorsi 3 mesi.
 - *Minimizzazione:*
- Profili di autorizzazione: il cliente può configurare l'accesso ai dati aziendali trattati nel sistema a seconda delle attività svolte dagli utenti.
 - *Identificazione di chi ha trattato i dati:*
- Strumenti di log: E' attivo un log della procedura con cui sono registrati gli accessi alla procedura stessa e alle singole funzioni che la compongono con il tipo di operazione eseguita. Il cliente può ottenere l'elenco completo dei log per un range di date chiedendolo direttamente a Sostenibile.cloud.
I log vengono conservati nel sistema per 30 giorni, trascorsi i quali sono automaticamente cancellati.
- Presenza di utenze di servizio per personale di assistenza: Coloro che eseguono assistenza e manutenzione sulla procedura hanno utenze nominali.



- *Tecniche di crittografia:*
- Crittografia delle password: viene registrato un hash delle password con l'algoritmo bcrypt aggiungendo un "salt" di applicazione ed un "salt" di utente
 - *Diritti degli interessati:*
- Diritti degli interessati: il cliente potrà agire direttamente sul Portale Sostenibile.cloud, facendo le operazioni necessarie (cancellando l'anagrafica, aggiornamento, modifica). Se del caso potrà essere contattata l'assistenza per ricevere supporto.



2. RESPONSABILE DEL TRATTAMENTO:

MISURE DI SICUREZZA IMPLEMENTATE PER I SERVIZI DI ASSISTENZA DI PRIMO LIVELLO IN CAPO A ZUCCHETTI

ASSISTENZA ON SITE

Gli addetti Zucchetti accedono presso la struttura del Titolare per fare formazione od effettuare attività tecnica di manutenzione.

In questo caso gli addetti Zucchetti lavorano come se facessero parte della struttura del Titolare ed adottano tutte le procedure di sicurezze implementate dallo stesso. I Titolari potranno generare utenze individuali per l'accesso ai loro sistemi, oppure potranno far accedere in affiancamento per formare il loro personale.

Qualora durante l'attività di assistenza l'addetto Zucchetti abbia la necessità di prelevare archivi o DB di cui necessita per risolvere le problematiche evidenziate è necessario che informi il Titolare e registri tale attività sulla Nota di Intervento:

Al termine dell'attività presso gli uffici Zucchetti sarà informato il Titolare sulla soluzione adottata e sulla successiva cancellazione dell'archivio.

Qualora vi fosse la necessità di conservare gli archivi per il tempo necessario al collaudo della soluzione adottata, dovrà essere informato il Titolare sul tempo massimo di conservazione di tali archivi.

ASSISTENZA TELEFONICA

Non presenta problemi da un punto di vista di trattamento di dati personali. Non sono trasmessi dati o archivi e la comunicazione rimane verbale.

ASSISTENZA TRAMITE EMAIL/TICKETS WEB

Nell'assistenza tramite email i tecnici Zucchetti inseriranno sempre nel testo del messaggio il disclaimer per rendere edotto il Titolare dell'informativa sintetica e dei recapiti a cui potrà rivolgersi per esercitare i suoi diritti o i diritti dei suoi interessati.

L'addetto Zucchetti non è autorizzato a farsi mandare le credenziali di accesso del Titolare via email né tantomeno potrà salvarle sullo strumento di ticketing.

Qualora un Titolare invii le credenziali di accesso al suo ambiente senza richiesta del tecnico Zucchetti è necessario che lo stesso risponda che non è autorizzato ad accedere ai sistemi con credenziali di altri utenti in quanto questa modalità viola il GDPR. Quindi il tecnico Zucchetti dovrà richiedere credenziali individuali oppure collegamento da remoto tramite strumenti a ciò dedicati.

I tecnici Zucchetti firmeranno ogni email con nome e cognome e l'informazione sarà salvata nello strumento di ticketing.

ASSISTENZA ATTRAVERSO LA RICEZIONE DI DATA BASE DEI CLIENTI

Qualora per risolvere il problema segnalato dal Titolare fosse necessario farsi mandare la base dati o altri files o query contenenti dati personali è necessario comunicare al Titolare o l'area ftp su cui dovrà caricare i file oppure per i Titolari con l'ambiente installato sul ns. data center, richiedere l'autorizzazione per far effettuare la copia ai nostri sistemisti.

Area FTP

L'area ftp sarà impostata affinché il Titolare veda solo l'upload. Il download sarà visualizzato solo dal gruppo di assistenza a cui la richiesta di assistenza è stata effettuata.

Tre giorni dopo la data di pubblicazione una routine cancellerà i file caricati in area ftp.



Area SharePoint

Essendo diventato Office 365 strumento aziendale anche di collaboration ogni utente Zucchetti ha a disposizione Sharepoint che può utilizzare anche tale strumento per la condivisione dei documenti e file in genere coi clienti.

L'azienda al fine di tutelare la privacy del dipendente non entrerà nel merito dello sharepoint individuale, pertanto, una volta che il cliente ha scaricato i files, l'operatore avrà anche la responsabilità della relativa cancellazione.

Scaricamento archivi tramite wetransfer o link di collegamento su ambienti del Titolare

In questo caso la gestione è in carico al Titolare che fornirà le credenziali per accedere all'ambiente dove risiedono gli archivi.

L'assistenza dovrà scaricarli in dischi di rete non soggetti a backup e cancellarli al termine dell'attività come nelle altre ipotesi.

Autorizzazione di backup da parte dei nostri sistemisti

L'archivio ricevuto viene scaricato su una directory del gruppo di assistenza non soggetta a backup.

L'assistenza di primo livello trasmette il db all'assistenza di 2 livello. L'assistenza di 2 livello procederà alle analisi di cui il problema necessita e poi cancellerà gli archivi ricevuti.

In ogni caso l'assistenza che ha in carico il problema, sia essa di primo o secondo livello, al termine dell'attività, cancellerà gli archivi ricevuti.

L'assistenza che ha in carico la gestione, terminata l'attività dovrà cancellare gli archivi ricevuti dal disco condiviso e da eventuali supporti di memorizzazione locali.

Qualora vi fosse la necessità di mantenere gli archivi sarà mandata una email al Titolare che ne darà l'autorizzazione.

Gli archivi dei Titolari non potranno mai essere trasmessi a gruppi di lavoro differenti rispetto a quelli finalizzati alla risoluzione del problema segnalato dal Titolare.

L'unica possibilità che i tecnici hanno per conservare gli archivi senza la previa autorizzazione del Titolare è l'anonimizzazione degli stessi.

ASSISTENZA ATTRAVERSO LA NECESSITÀ DI AVERE IL BACKUP DEI CLIENTI DI UN SERVIZIO DATA CENTER

Qualora i dati personali del Titolare siano su sistema Zucchetti/Data center, in nessun caso l'assistenza di 1 livello potrà richiedere il backup ai sistemisti di Data Center se non previa autorizzazione del Titolare stesso.

I sistemisti non potranno estrarre nessun backup dei Titolari per esigenze e finalità differenti rispetto al fornire assistenza agli stessi; ad esempio non potranno essere effettuati backup indirizzati alla produzione per l'esecuzione di test.

ASSISTENZA ATTRAVERSO COLLEGAMENTO DA REMOTO ATTRAVERSO STRUMENTI A CIO' DEDICATI

Questa modalità di collegamento sugli strumenti dei clienti garantisce la privacy in quanto:

- Il collegamento è sempre richiesto dal cliente
- Le credenziali di accesso sono sempre individuali
- Il cliente ci fa accedere ad un ambiente con profilo di autorizzazione da lui scelto per farci eseguire le attività di assistenza
- Il cliente può sconnetterci quando desidera.

Attraverso tali strumenti è possibile far accedere anche l'assistenza di 2 livello alla stessa sessione da noi aperta. In questo caso il cliente ne ha l'evidenza perché fornita dallo strumento e quindi accetta implicitamente tale modalità.

È essenziale utilizzare i nostri strumenti in quanto licenziati e personalizzati con tutta la documentazione che deve essere prodotta dalla legge sul trattamento dei dati personali.



Solo in casi eccezionali e dopo attenta valutazione del responsabile e dell'ufficio privacy è possibile utilizzare altri strumenti di connessione che si comportano in modo uguale.

Si precisa che non sarà possibile registrare i collegamenti da remoto in diretta, qualora fosse strettamente necessario e solo su base progettuale, sarà possibile valutare con il responsabile eventuali eccezioni, previa sottoscrizione della relativa manleva.

ASSISTENZA ATTRAVERSO COLLEGAMENTO DA REMOTO SU IP PUBBLICI OPPURE TRAMITE VPN

Qualora l'attività di assistenza debba essere svolta su sistemi cloud su IP pubblici oppure tramite VPN o accessi privati è necessario che gli addetti Zucchetti entrino nei sistemi dei Titolari:

- Previa autorizzazione del cliente
- Previa ricezione delle credenziali individuali e le stesse siano state attivate per il tempo necessario all'esecuzione delle attività richieste
- al termine dell'attività siano disattivate le credenziali da parte del Titolare

Regole che riguardano gli ambienti dei Titolari, in qualsiasi forma di delivery (Saas/Paas/On Premise) riferite a:

- creazione utenze per consulenti applicativi;
- creazione utenze per personale di assistenza.

Consulenti applicativi

Per effettuare tutte le attività di start up sull'ambiente del Titolare è necessario che venga appositamente creata un'utenza all'interno del sistema come di seguito indicato:

- ZU_+ prime 3 lettere del cognome + prime 3 lettere del nome
- nella descrizione (nome completo) apporre: Utente Zucchetti

In questo modo il Cliente potrà riconoscere la provenienza dell'utenza stessa.

Es: per il soggetto Rossi Mario dovrà essere creata l'utenza: ZU_ROSMAR

Per la creazione dovrà essere coinvolto il Titolare, il quale dovrà essere guidato all'accesso e alla creazione dell'utenza precisando e condividendo con lui, i diritti che verranno assegnati a quest'ultima.

Personale di Help Desk

La creazione dell'utenza deve essere richiesta solo al Titolare che, attraverso l'amministratore di applicazione, potrà creare il nuovo utente.

Non deve mai essere utilizzato l'utente amministratore da parte degli operatori di assistenza.

Anche in questo caso, per la creazione delle utenze, valgono le regole di creazione esplicitate per i consulenti applicativi

Le utenze dovranno essere generate con la codifica: ZU_prime tre cognome_prime tre nome.

Nella descrizione dovrà essere inserito Zucchetti Utente

Creazione di utenze ZU_ per assistenza applicative/produzione

Nel caso in cui, grazie agli strumenti di monitoraggio, sia possibile riscontrare un problema dall'interno prima che le assistenze o il cliente/titolare lo segnalino, è possibile creare un'utenza ZU_ anche all'assistenza applicativa di riferimento o alla produzione secondo il seguente flusso:

- una volta rilevata la criticità, i sistemisti applicativi creano un ticket figlio verso il



relativo Centro Servizi, chiedendo all'assistenza applicativa (Zucchetti SPA o Partner) di effettuare le opportune verifiche confrontandosi se opportuno la loro produzione e/o cliente

- le verifiche applicative possono necessitare un'utenza zu_ e pertanto ne verrà richiesta la creazione ai Sistemisti Applicativi
- Al termine delle attività di verifica i Sistemisti Applicativi provvederanno a disabilitare l'utente zu_ creato per l'assistenza.

CONVERSIONI E PROGETTI DI START UP

Qualora si verifichino le seguenti casistiche:

- Conversione o start up con contratto
- Conversioni o startup senza contratto

Nel primo caso le attività sono finalizzate ad adempiere all'obbligazione contrattuale e pertanto lecite.

In questo caso è necessario redigere un documento di progetto in cui si convengono con il Titolare le modalità operative di esecuzione delle attività tra cui:

- Dati personali, archivi, base dati di cui necessita l'esecuzione delle attività
- Dettaglio delle operazioni da eseguire sui dati
- Identificazione del periodo entro cui sarà terminata tale attività
- La previsione di un collaudo in cui il Titolare proverà la conversione

I documenti che il Titolare ha sottoscritto per lo svolgimento di queste attività sono il contratto e la nomina a responsabile conferendo mandato a Zucchetti di svolgere tutte le attività necessarie all'erogazione del servizio. In questo caso non serve mandare al Titolare la lettera di incarico, in quanto la stessa viene fatta da Zucchetti, in qualità di responsabile, agli addetti Zucchetti.

Qualora non vi sia il contratto invece è necessario inviare al Titolare la nomina a responsabile al trattamento. Nella nomina dovrà essere previsto un termine di svolgimento e portata a termine dell'attività. Zucchetti provvederà ad incaricare gli addetti in qualità di responsabile.

Anche in questo caso è necessario prevedere una fase progettuale in cui condividere gli step sopra riportati. Al termine sarà anche in questo caso essenziale prevedere il collaudo.

Con il documento di collaudo, che dovrà essere sottoscritto dal Titolare, lo stesso ci dichiarerà che le attività da noi effettuate sono corrette e quindi ci autorizzerà a cancellare i suoi archivi.

Nel documento di collaudo dovranno essere inserite le seguenti indicazioni:

- Il lavoro svolto è conforme rispetto all'ambito contrattuale convenuto
- Il Titolare ha provato la conversione e dichiara che il prodotto funziona e tutte le funzioni sono state correttamente configurate e implementate
- Che non ci sono errori nei dati convertiti e che quindi potrà utilizzare il prodotto per le finalità per cui lo ha acquistato

Inoltre il Titolare deve dichiarare che dalla data della firma del contratto non avrà nulla a pretendere rispetto all'attività di conversione svolta e prevista dal contratto e che autorizza Zucchetti a cancellare ogni dato, archivio, data base che è servito per portare a termine la fase di conversione.

Solo qualora ci fosse la necessità di mantenere gli archivi del Titolare per finalità di cautela e verifica del lavoro da noi svolto, dobbiamo inviare una comunicazione con la quale il Titolare ci autorizza a conservare gli archivi per l'ulteriore periodo, terminato il quale gli archivi dovranno essere eliminati.

Tutto l'iter autorizzativo dovrà essere inserito nel post vendita al fine di averne memoria.

Tutti i documenti contenenti dati dei Titolari stampati non possono essere riutilizzati come carta da riciclo e devono essere immediatamente distrutti.



MISURE DI SICUREZZA IMPLEMENTATE PER I SERVIZI DI ASSISTENZA HELP DESK E CONSULENZA NORMO APPLICATIVA (assistenza di II livello in capo a Sostenibile.Cloud)

ASSISTENZA ON SITE

Non prevista

ASSISTENZA TELEFONICA

Non presenta problemi da un punto di vista di trattamento di dati personali. Non sono trasmessi dati o archivi e la comunicazione rimane verbale.

ASSISTENZA TRAMITE EMAIL/TICKETS WEB

L'addetto Sostenibile.cloud non è autorizzato a farsi mandare le credenziali di accesso del cliente via e-mail né tantomeno potrà salvarle sullo strumento di ticketing.

Qualora un cliente invii le credenziali di accesso al suo ambiente senza richiesta dell'addetto Sostenibile.cloud è necessario che lo stesso risponda che non è autorizzato ad accedere ai sistemi con credenziali di altri utenti in quanto questa modalità viola le policy di sicurezza. Quindi l'addetto Sostenibile.cloud dovrà richiedere credenziali individuali oppure collegamento tramite software di teleassistenza.

ASSISTENZA ATTRAVERSO ACCESSO AI DATA BASE DEI CLIENTI

Qualora, per risolvere la segnalazione dal cliente, fosse necessario accedere alla base dati o altri files o query contenenti dati personali il Fornitore dovrà richiedere al cliente l'autorizzazione per accedere. In mancanza, gli addetti Sostenibile.Cloud non potranno operare.

ASSISTENZA ATTRAVERSO COLLEGAMENTO DA REMOTO CON SOFTWARE DI TELEASSISTENZA

Questa modalità di collegamento sugli strumenti del cliente garantisce la privacy in quanto:

- Il collegamento è sempre richiesto dal cliente
- Le credenziali di accesso sono sempre individuali
- Il cliente fa accedere gli addetti Sostenibile.cloud ad un ambiente con profilo di autorizzazione da lui scelto per far eseguire le attività di assistenza
- Il cliente può disconnettere il tecnico quando desidera

Gli addetti di Sostenibile.Cloud potranno accedere tramite software di teleassistenza o potrà visualizzare i dati mediante videoconferenza.

Le attività di cui al presente paragrafo 2 sono finalizzate ad adempiere all'obbligazione contrattuale e pertanto lecite. I documenti che il Cliente ha sottoscritto per lo svolgimento di queste attività sono il contratto e la nomina a responsabile conferendo mandato al Fornitore, nominato Responsabile, di svolgere tutte le attività necessarie all'erogazione del servizio.

3. RESPONSABILE DEL TRATTAMENTO: MISURE DI SICUREZZA IMPLEMENTATE PER I SERVIZI SAAS- PAAS

Il presente allegato contiene la descrizione delle misure tecniche e organizzative messe in atto dal Responsabile del trattamento (comprese le eventuali certificazioni pertinenti) per garantire un adeguato livello di sicurezza, tenuto conto della natura, dell'ambito di applicazione, del contesto e della finalità del



trattamento, nonché dei rischi per i diritti e le libertà delle persone fisiche. Comprese le misure tecniche e organizzative per essere in grado di fornire assistenza al Titolare e per la gestione degli eventuali sub responsabili eventualmente previsti.

N°	Controlli																
I.	Riservatezza																
1.0	Controllo fisico degli accessi - accesso ai locali e alle strutture in cui vengono trattati i dati. Requisito: <i>è necessario evitare l'accesso (fisico) di soggetti non autorizzati agli edifici e alle strutture in cui vengono trattati i dati personali del Titolare del trattamento. Il Responsabile del trattamento deve mettere in atto sistemi di controllo degli accessi efficienti (controllo degli accessi tecnologico o mediante personale).</i>																
1.1	A tal fine vengono messe in atto le seguenti misure tecniche: <table border="1"> <tr><td>☒</td><td>Sistemi di allarme</td></tr> <tr><td>☒</td><td>Sistemi antintrusione (barriere fotoelettriche/rilevatori di movimento)</td></tr> <tr><td>☒</td><td>Sistemi automatico di controllo degli accessi</td></tr> <tr><td>☒</td><td>Barriere di accesso biometriche</td></tr> <tr><td>☒</td><td>Sistema di accesso mediante smart card/trasponder</td></tr> <tr><td>☒</td><td>Sistemi di chiusura manuali</td></tr> <tr><td>☒</td><td>Sistemi di chiusura con codice d'accesso</td></tr> <tr><td>☒</td><td>Videosorveglianza dei punti di accesso</td></tr> </table>	☒	Sistemi di allarme	☒	Sistemi antintrusione (barriere fotoelettriche/rilevatori di movimento)	☒	Sistemi automatico di controllo degli accessi	☒	Barriere di accesso biometriche	☒	Sistema di accesso mediante smart card/trasponder	☒	Sistemi di chiusura manuali	☒	Sistemi di chiusura con codice d'accesso	☒	Videosorveglianza dei punti di accesso
☒	Sistemi di allarme																
☒	Sistemi antintrusione (barriere fotoelettriche/rilevatori di movimento)																
☒	Sistemi automatico di controllo degli accessi																
☒	Barriere di accesso biometriche																
☒	Sistema di accesso mediante smart card/trasponder																
☒	Sistemi di chiusura manuali																
☒	Sistemi di chiusura con codice d'accesso																
☒	Videosorveglianza dei punti di accesso																
1.2	A tal fine vengono messe in atto le seguenti misure organizzative. <table border="1"> <tr><td>☒</td><td>Controlli del personale tramite portineria/all'accoglienza</td></tr> <tr><td>☒</td><td>Registrazione dei visitatori/libro dei visitatori</td></tr> <tr><td>☒</td><td>Accompagnamento dei visitatori</td></tr> <tr><td>☒</td><td>Registrazione delle chiavi/libro delle chiavi</td></tr> <tr><td>☒</td><td>Obbligo di indossare badge identificativo per dipendenti</td></tr> <tr><td>☒</td><td>Obbligo di indossare badge identificativo ospiti</td></tr> <tr><td>☒</td><td>Zone di sicurezza con diverse autorizzazioni di accesso</td></tr> <tr><td>☒</td><td>Supervisione del personale esterno ad es. personale per la manutenzione e di servizio ecc.</td></tr> </table>	☒	Controlli del personale tramite portineria/all'accoglienza	☒	Registrazione dei visitatori/libro dei visitatori	☒	Accompagnamento dei visitatori	☒	Registrazione delle chiavi/libro delle chiavi	☒	Obbligo di indossare badge identificativo per dipendenti	☒	Obbligo di indossare badge identificativo ospiti	☒	Zone di sicurezza con diverse autorizzazioni di accesso	☒	Supervisione del personale esterno ad es. personale per la manutenzione e di servizio ecc.
☒	Controlli del personale tramite portineria/all'accoglienza																
☒	Registrazione dei visitatori/libro dei visitatori																
☒	Accompagnamento dei visitatori																
☒	Registrazione delle chiavi/libro delle chiavi																
☒	Obbligo di indossare badge identificativo per dipendenti																
☒	Obbligo di indossare badge identificativo ospiti																
☒	Zone di sicurezza con diverse autorizzazioni di accesso																
☒	Supervisione del personale esterno ad es. personale per la manutenzione e di servizio ecc.																
2.0	Controllo logico degli accessi - L'accesso logico ai sistemi di trattamento, alle applicazioni e ai dati deve essere riservato esclusivamente ai soggetti autorizzati. Requisito: <i>è necessario evitare l'accesso non autorizzato ai sistemi IT. Devono essere messe in atto misure tecniche e organizzative per l'identificazione e l'autenticazione degli utenti.</i> <i>L'accesso ai sistemi IT del Responsabile del trattamento deve essere limitato agli utenti autorizzati mediante un processo di autenticazione sicuro. Ogni utente deve avere un ID utente univoco. La condivisione degli account non è consentita.</i> <i>L'accesso ai sistemi IT e alle applicazioni del Responsabile del trattamento deve essere accessibile tramite sistemi di autenticazione che prevede come requisito minimo l'utilizzo di credenziali composte da nome utente e password. Tale protezione deve includere ma non essere limitata a una policy per la password sicura, una disconnessione automatica dopo un determinato periodo di tempo, il blocco in seguito a diversi tentativi di accesso falliti, una procedura di ripristino della password affidabile, una modifica periodica delle password. Le password devono essere sempre conservate e trasmesse in modo sicuro, ad es. mediante crittografia e funzione hash. Il Responsabile del trattamento ha definito i requisiti, le regole e gli standard delle linee guida per le password in una politica conosciuta dagli utenti e supportata a livello tecnico. Le password devono essere assegnate a una singola persona, conservate e trasmesse in modo sicuro, essere sufficientemente lunghe e complesse, modificate su base regolare, limitate in termini di validità, bloccate e successivamente eliminate se inattive per un lungo periodo di tempo e modificate immediatamente qualora compromesse. Ove possibile, in particolare per le utenze con privilegi elevati e per i sistemi e le applicazioni che ospitano dati particolari, si predilige l'utilizzazione di sistemi di autenticazione a più fattori</i>																
2.1	A tal fine vengono messe in atto le seguenti misure tecniche: <table border="1"> <tr><td>☒</td><td>Autenticazione con username e password</td></tr> </table>	☒	Autenticazione con username e password														
☒	Autenticazione con username e password																



	☒	Autenticazione a due fattori
	☒	Identity and Access Management centralizzato
	☒	Sistemi di Single Sign On
	☒	Sistemi di controllo scadenza password
	☒	Sistemi di controllo robustezza e complessità password
	☒	Sistemi di blocco account dopo numero predefinito di tentativi falliti
	☒	Sistemi di controllo dell'utilizzo contemporaneo dello stesso account sulle applicazioni
	☒	Utilizzo di VPN autenticata crittografata per accesso da remoto
	☒	Utilizzo password o pin per i dispositivi mobili
	☒	Utilizzo di salvaschermi automatici
	☒	Time-out sessione per le applicazioni
2.2	A tal fine vengono messe in atto le seguenti misure organizzative :	
	☒	Procedure di assegnazione degli account
	☒	Inventario aggiornato degli account assegnati
	☒	Inventario aggiornato degli account di servizio utilizzati dalle applicazioni
	☒	Cancellazione o disabilitazione degli account non utilizzati dopo un periodo di tempo definito
	☒	Formazione del personale sull'uso account aziendali
	☒	Regolamenti o politiche per gli account aziendali e la robustezza delle password
	☒	Procedure di azzeramento o ripristino password
3.0	Profili di autorizzazione e controllo delle autorizzazioni – Nessuna lettura, copia, modifica o rimozione non autorizzata all'interno del sistema informatico o per il trattamento di dati su supporti cartacei. Requisito: <i>Il Responsabile del trattamento deve definire specifici profili di autorizzazione per i soggetti che accedono ai dati e mettere in atto soluzioni per il controllo dei diritti di accesso e le necessarie autorizzazioni, che devono essere strettamente limitate a consentire l'attività delegata al soggetto autorizzato. Il controllo delle autorizzazioni prevede anche politiche e strumenti di monitoraggio e di registrazione degli accessi ai dati. Particolare attenzione deve essere posta all'assegnazione di privilegi elevati, che devono essere riservati ai tecnici che effettuano operazioni di amministrazione dei sistemi, delle banche dati e delle applicazioni (cd. Amministratori di sistema). Gli amministratori di sistema devono avere un account con privilegi elevati individuale per eseguire le loro attività di amministrazione diverso da quello utilizzato per le attività che non richiedono diritti particolari. I dischi e le memorie destinate allo smaltimento o riutilizzo devono essere distrutti o soggetti a cancellazione sicura</i>	
3.1	A tal fine vengono messe in atto le seguenti misure tecniche .	
	☒	Profili utente con accesso limitato alla rete ed alle applicazioni
	☒	Ruoli e autorizzazioni basati sul principio della necessità di accesso ai dati
	☒	Configurazione dei file server con aree ad accesso limitato in base alle autorizzazioni assegnate
	☒	Configurazione delle applicazioni per l'assegnazione di privilegi minimi per eseguire l'attività assegnata all'utente
	☒	Sistema di registrazione (log) delle modifiche dei privilegi assegnati
	☒	Sistema di alert delle modifiche dei privilegi assegnati
	☒	Sistema di registrazione (log) dell'accesso ai sistemi da parte degli amministratori di sistema
	☒	Sistema di registrazione (log) dell'accesso ai sistemi da parte degli utenti
	☒	Sistema di registrazione (log) dell'accesso alle applicazioni o ai database da parte degli amministratori di sistema
	☒	Sistema di registrazione (log) dell'accesso alle applicazioni da parte degli utenti
	☒	Meccanismi di cancellazione sicura dei dati (quali wiping program e formattazione a basso livello) per i dischi e le unità di memoria destinati a riutilizzo o smaltimento
3.2	A tal fine vengono messe in atto le seguenti misure organizzative .	
	☒	Creazione di profili utente con autorizzazioni in base al ruolo e a compiti assegnati (Segregation of duty, need to know e last privilege)

	☒	Procedure di autorizzazione documentate (richiesta, assegnazione, revoca delle autorizzazioni)
	☒	Riesame regolare delle autorizzazioni
	☒	Account con privilegi amministrativi individuali e utilizzati solo quando necessario
	☒	Account individuali anche per i tecnici esterni che necessitano di credenziali amministrative
	☒	Verifica delle caratteristiche soggettive di esperienza, capacità e affidabilità degli amministratori di sistema
	☒	Elenco aggiornato degli amministratori di sistema, con il dettaglio dei compiti assegnati
	☒	Verifica periodica delle attività degli amministratori di sistema
	☒	Presidio, controllo e verifica delle attività degli interventi tecnici effettuati da personale esterno
	☒	Distruzione dei supporti di memorizzazione destinati allo smaltimento
	☒	Regole e policy su utilizzo di scanner, fotocopiatrici e stampanti di rete
	☒	Utilizzo di tritadocumenti per la distruzione di documenti cartacei non più necessari
4.0	Pseudonimizzazione e cifratura – Per i dati più critici è opportuno adottare ulteriori misure di sicurezza per evitare la comprensibilità e l'usabilità dei dati anche in caso di furto o accesso non autorizzato. Requisito: <i>Nei casi in cui il trattamento riguardi dati particolari o relativi a condanne penali o reati, nonché per i dispositivi a maggiore mobilità e quindi più soggetti a furti e smarrimenti, è opportuno applicare misure tecniche e organizzative per limitare la possibilità di utilizzo dai dati da parte di soggetti non autorizzati.</i>	
4.1	A tal fine vengono messe in atto le seguenti misure tecniche .	
	☒	Sistemi di crittografia dei database
	☒	Cifratura dei dischi dei server
	☒	Cifratura dei dischi dei dispositivi
	☒	Cifratura dei dati in cloud
	☒	Cifratura dei backup
	☒	Nel caso di dati pseudonimizzati separazione dei campi identificativi su sistemi separati protetti
	☒	Abbreviazione dei record di dati per limitare le possibilità di identificazione (es. indirizzo IP)
4.2	A tal fine vengono messe in atto le seguenti misure organizzative .	
	☒	Politiche di conservazione e gestione delle chiavi di cifratura
	☒	Utilizzo di dati pseudonimizzati (codici) nelle fasi di trattamento in cui non è necessaria l'identificazione degli interessati
	☒	Rimozione degli elementi identificativi degli interessati ove non necessari (fasi di sviluppo, rendicontazione, uso o comunicazione di dati aggregati)
5.0	Protezione dei dati durante la trasmissione – È necessario garantire la sicurezza dei dati nella trasmissione tra sistemi, nel trasporto tra diverse sedi e nelle fasi di comunicazione. Requisito: <i>Nei casi di trasmissione di dati tra sistemi, di trasporto di dati tra diverse sedi e nei casi di comunicazione autorizzata a terze parti è necessario garantire la sicurezza dei canali di trasmissione. I canali di trasmissione elettronica devono essere sicuri, crittografati e garantiti. Va tutelata anche la sicurezza dei dati nel caso di trasporto e consegna di documenti cartacei.</i>	
5.1	A tal fine vengono messe in atto le seguenti misure tecniche .	
	☒	Configurazione di tunnel VPN
	☒	Trasmissione di dati, documenti o allegati con password trasmessa su altro canale
	☒	Utilizzo di https nei sistemi web based
	☒	Protocolli TLS 1.2 o successivi su web server
	☒	Crittografia delle reti WI-FI (almeno WPA2)
	☒	Utilizzo di crittografia nei server ftp (FTPS o SFTP)
	☒	Contenitori/involucri sicuri per la spedizione
	☒	Istruzioni chiare riguardo ai destinatari autorizzati
5.2	A tal fine vengono messe in atto le seguenti misure organizzative .	



	☒	Elenchi dei destinatari autorizzati
	☒	Regole e Istruzioni di trasferimento ai destinatari autorizzati
	☒	Regole per il trasporto di documenti



III.	Disponibilità e resilienza																						
1.0	Sistemi di sicurezza nelle sale server - Protezione da distruzione/perdita accidentale di dati e per la disponibilità dei servizi Requisito: <i>il Responsabile del trattamento è obbligato ad adottare le misure tecniche e organizzative per garantire la disponibilità dei dati. I dati devono essere protetti dalla distruzione o dalla perdita accidentale (ad esempio dovuta a blackout, incidenti o eventi naturali). In particolare le macchine e le sale server che le ospitano devono essere protette da influenze ambientali esterne e sabotaggi.</i>																						
1.1	A tal fine vengono messe in atto le seguenti misure tecniche . <table border="1" data-bbox="209 589 1570 1025"> <tr><td>☒</td><td>Estintori nelle sale server con estinguenti adatti</td></tr> <tr><td>☒</td><td>Aria condizionata nelle sale server</td></tr> <tr><td>☒</td><td>Dispositivi per il monitoraggio di temperatura e umidità nelle sale server</td></tr> <tr><td>☒</td><td>Sistemi di rilevamento di fiamme e fumo</td></tr> <tr><td>☒</td><td>Sistemi di controllo e alert parametri server e dispositivi di rete (uptime, temperatura, carico, errori, anomalie ecc.)</td></tr> <tr><td>☒</td><td>Sistemi di spegnimento incendi automatici</td></tr> <tr><td>☒</td><td>Alimentazione elettrica ininterrotta (UPS e gruppi di continuità)</td></tr> <tr><td>☒</td><td>infrastruttura IT duale (ridondanza)</td></tr> <tr><td>☒</td><td>Sistemi di protezione fisica per l'accesso alle sale server</td></tr> <tr><td>☒</td><td>Sistemi di accesso alle sale server con smart card / pin / trasponder / identificatori biometrici</td></tr> <tr><td>☒</td><td>Videosorveglianza delle sale server</td></tr> </table>	☒	Estintori nelle sale server con estinguenti adatti	☒	Aria condizionata nelle sale server	☒	Dispositivi per il monitoraggio di temperatura e umidità nelle sale server	☒	Sistemi di rilevamento di fiamme e fumo	☒	Sistemi di controllo e alert parametri server e dispositivi di rete (uptime, temperatura, carico, errori, anomalie ecc.)	☒	Sistemi di spegnimento incendi automatici	☒	Alimentazione elettrica ininterrotta (UPS e gruppi di continuità)	☒	infrastruttura IT duale (ridondanza)	☒	Sistemi di protezione fisica per l'accesso alle sale server	☒	Sistemi di accesso alle sale server con smart card / pin / trasponder / identificatori biometrici	☒	Videosorveglianza delle sale server
☒	Estintori nelle sale server con estinguenti adatti																						
☒	Aria condizionata nelle sale server																						
☒	Dispositivi per il monitoraggio di temperatura e umidità nelle sale server																						
☒	Sistemi di rilevamento di fiamme e fumo																						
☒	Sistemi di controllo e alert parametri server e dispositivi di rete (uptime, temperatura, carico, errori, anomalie ecc.)																						
☒	Sistemi di spegnimento incendi automatici																						
☒	Alimentazione elettrica ininterrotta (UPS e gruppi di continuità)																						
☒	infrastruttura IT duale (ridondanza)																						
☒	Sistemi di protezione fisica per l'accesso alle sale server																						
☒	Sistemi di accesso alle sale server con smart card / pin / trasponder / identificatori biometrici																						
☒	Videosorveglianza delle sale server																						
1.2	A tal fine vengono messe in atto le seguenti misure organizzative . <table border="1" data-bbox="209 1059 1570 1261"> <tr><td>☒</td><td>Notifica di allarme in caso di accesso alle stanze server</td></tr> <tr><td>☒</td><td>Notifica di allarme in caso di superamento dei parametri di temperatura/umidità/fumo</td></tr> <tr><td>☒</td><td>Divieto di accesso al personale non autorizzato al perimetro fisico dell'infrastruttura del sistema IT</td></tr> <tr><td>☒</td><td>Controllo dell'ubicazione delle sale server in relazione alle condutture idriche</td></tr> <tr><td>☒</td><td>Le sale server si trovano ai piani rialzati se in una zona soggetta a inondazioni</td></tr> </table>	☒	Notifica di allarme in caso di accesso alle stanze server	☒	Notifica di allarme in caso di superamento dei parametri di temperatura/umidità/fumo	☒	Divieto di accesso al personale non autorizzato al perimetro fisico dell'infrastruttura del sistema IT	☒	Controllo dell'ubicazione delle sale server in relazione alle condutture idriche	☒	Le sale server si trovano ai piani rialzati se in una zona soggetta a inondazioni												
☒	Notifica di allarme in caso di accesso alle stanze server																						
☒	Notifica di allarme in caso di superamento dei parametri di temperatura/umidità/fumo																						
☒	Divieto di accesso al personale non autorizzato al perimetro fisico dell'infrastruttura del sistema IT																						
☒	Controllo dell'ubicazione delle sale server in relazione alle condutture idriche																						
☒	Le sale server si trovano ai piani rialzati se in una zona soggetta a inondazioni																						
2.0	Protezione della rete e dei dispositivi – La rete, gli host e i dispositivi collegati in rete devono disporre di misure di protezione da attacchi di malintenzionati e da software malevolo. Requisito: <i>il Responsabile del trattamento è obbligato ad adottare le misure tecniche e organizzative per garantire la disponibilità (oltre alla riservatezza e l'integrità) dei dati trattati proteggendo la rete, i dispositivi e i dati conservati, elaborati o in transito da effetti dovuti a software malevolo o attacchi di malintenzionati. I dati devono essere elaborati, trasmessi e conservati con strumenti la cui sicurezza è implementata secondo gli standard di settore</i>																						
2.1	A tal fine vengono messe in atto le seguenti misure tecniche . <table border="1" data-bbox="209 1496 1570 1854"> <tr><td>☒</td><td>Protezione tramite sistemi firewall</td></tr> <tr><td>☒</td><td>Sistemi IDS, IPS o IDPS</td></tr> <tr><td>☒</td><td>Sistemi NAC (Network Access Control)</td></tr> <tr><td>☒</td><td>Sistemi SIEM</td></tr> <tr><td>☒</td><td>DMZ per i servizi esposti</td></tr> <tr><td>☒</td><td>WAF (Web Application Firewall) per i servizi esposti</td></tr> <tr><td>☒</td><td>Software antimalware aggiornato a livello di rete</td></tr> <tr><td>☒</td><td>Software antimalware aggiornato a livello di host</td></tr> <tr><td>☒</td><td>Software antimalware aggiornato su tutti i dispositivi</td></tr> </table>	☒	Protezione tramite sistemi firewall	☒	Sistemi IDS, IPS o IDPS	☒	Sistemi NAC (Network Access Control)	☒	Sistemi SIEM	☒	DMZ per i servizi esposti	☒	WAF (Web Application Firewall) per i servizi esposti	☒	Software antimalware aggiornato a livello di rete	☒	Software antimalware aggiornato a livello di host	☒	Software antimalware aggiornato su tutti i dispositivi				
☒	Protezione tramite sistemi firewall																						
☒	Sistemi IDS, IPS o IDPS																						
☒	Sistemi NAC (Network Access Control)																						
☒	Sistemi SIEM																						
☒	DMZ per i servizi esposti																						
☒	WAF (Web Application Firewall) per i servizi esposti																						
☒	Software antimalware aggiornato a livello di rete																						
☒	Software antimalware aggiornato a livello di host																						
☒	Software antimalware aggiornato su tutti i dispositivi																						
2.2	A tal fine vengono messe in atto le seguenti misure organizzative . <table border="1" data-bbox="209 1888 1570 2045"> <tr><td>☒</td><td>Segmentazione delle reti</td></tr> <tr><td>☒</td><td>Controllo e aggiornamento periodico delle policy dei firewall</td></tr> <tr><td>☒</td><td>Analisi dei log e degli avvisi di sicurezza</td></tr> <tr><td>☒</td><td>Test di penetrazione su base regolare</td></tr> </table>	☒	Segmentazione delle reti	☒	Controllo e aggiornamento periodico delle policy dei firewall	☒	Analisi dei log e degli avvisi di sicurezza	☒	Test di penetrazione su base regolare														
☒	Segmentazione delle reti																						
☒	Controllo e aggiornamento periodico delle policy dei firewall																						
☒	Analisi dei log e degli avvisi di sicurezza																						
☒	Test di penetrazione su base regolare																						



	☒	Regolamento / Disciplinare/ Policy sull'utilizzo della rete e degli strumenti informatici da parte degli utenti
	☒	Formazione degli utenti in merito ad attacchi di phishing e social engineering
3.0	Controllo delle disponibilità e controllo della recuperabilità – Salvataggio periodico dei dati e procedure per recuperare i dati il prima possibile. Requisito: <i>I dati devono essere conservati i più copie su reti/sistemi/sedi separate. Il Responsabile del trattamento deve mettere in atto una politica di backup e di ripristino che garantisce il recupero del sistema e dei dati.</i>	
3.1	A tal fine vengono messe in atto le seguenti misure tecniche .	
	☒	Sistemi di backup automatizzato
	☒	Sistemi di backup in cloud
	☒	Sistemi di disaster recovery con infrastrutture proprie
	☒	Sistemi di disaster recovery con piattaforme DRaaS in cloud
3.2	A tal fine vengono messe in atto le seguenti misure organizzative .	
	☒	Piani di backup e di recovery del software, delle configurazioni e dei dati
	☒	Procedure di continuità operativa
	☒	Procedure di ripristino dei dati
	☒	Test di ripristino periodici
	☒	Esercitazioni di simulazione di crisi/emergenza su base regolare con prove di ripristino
4.0	Gestione e Controllo delle Risorse informatiche e del software: <i>Il Responsabile del trattamento deve garantire la sicurezza dell'ambiente di trattamento e degli strumenti utilizzati.</i> Requisito: <i>È necessaria una gestione globale e attiva (inventariare, abilitare, tracciare, aggiornare) tutti gli strumenti utilizzati per il trattamento dei dati, compresi gli strumenti non direttamente attivi nel trattamento ma connessi alle reti o ai sistemi utilizzati per la conservazione, il transito o l'elaborazione dei dati. Questi comprendono i sistemi di rete, i sistemi di protezione, i sistemi server di elaborazione e archiviazione, i sistemi di comunicazione e trasmissione dei dati, i dispositivi dell'utente autorizzato, mobili e portatili inclusi, dispositivi di rete, i dispositivi IoT connessi all'infrastruttura fisicamente, virtualmente, in remoto e quelli in ambienti cloud, per conoscere con precisione la totalità delle risorse che devono essere monitorate e protette.</i> <i>Parimenti è necessario gestire attivamente (inventariare, tracciare e aggiornare) tutto il software (sistemi operativi e applicazioni) sulla rete in modo che solo il software autorizzato possa essere installato ed eseguito, adottando politiche o misure per impedire l'installazione o l'esecuzione di software non autorizzato</i>	
4.1	A tal fine vengono messe in atto le seguenti misure tecniche .	
	☒	Strumenti di rilevamento attivo delle risorse connesse alla/e rete/i
	☒	Strumenti di rilevamento passivo delle risorse connesse alla/e rete/i
	☒	Strumenti di inventario dei dispositivi ad alimentazione manuale
	☒	Strumenti automatici di rilevamento dei software utilizzati a livello di rete
	☒	Strumenti di inventario dei software installati ad alimentazione manuale
	☒	Sistemi di aggiornamento automatico del software
	☒	Vulnerability assessment periodici
4.2	A tal fine vengono messe in atto le seguenti misure organizzative .	
	☒	Inventario accurato, dettagliato e aggiornato di tutte le risorse aziendali con la possibilità di archiviazione o elaborazione dati
	☒	Procedure per la gestione delle risorse non autorizzate (rimozione, blocco, quarantena)
	☒	Inventario accurato, dettagliato e aggiornato di tutti software utilizzati a livello aziendale
	☒	Registrazione e monitoraggio di tutte le modifiche alle configurazioni di risorse, apparati e sistemi IT
	☒	Procedure per l'aggiornamento e l'applicazione delle correzioni di sicurezza nei software
	☒	Verifica periodica bollettini di sicurezza per le vulnerabilità rilevate



IV.	Politiche e procedure per la gestione della tutela dei dati personali, per l'esame periodico del sistema di trattamento, la valutazione e la verifica su base regolare																						
1.0	Politiche di protezione dei dati personali Requisito: <i>Il Responsabile del trattamento deve implementare un proprio sistema di tutela dei dati personali.</i> <i>Gli elementi includono:</i> <i>Una struttura organizzativa vigente per la protezione dei dati con responsabilità definite (incl. la nomina di un responsabile della protezione dei dati, qualora richiesto a livello legale)</i> <i>Conformità a tutti i requisiti legali per la protezione dei dati personali</i> <i>Sistema di gestione dei contratti vigente per la conservazione di tutti gli accordi relativi alla protezione dei dati (es. accordi per il trattamento dei dati, accordi con sub-responsabili del trattamento ecc.)</i> <i>Formazione sulla tutela dei dati personali per i dipendenti del Responsabile del trattamento che trattano i dati personali del Titolare del trattamento</i> <i>Accordi sulla riservatezza dei dati personali per i dipendenti del Responsabile del trattamento che trattano i dati personali del Titolare del trattamento</i> <i>Una procedura che garantisce i diritti dei soggetti interessati (in cooperazione con il Titolare del trattamento)</i> <i>L'adozione di certificazioni sulla sicurezza dei dati e l'adesione a codici di condotta possono essere validi strumenti di controllo delle politiche di protezione</i> A tal fine vengono messe in atto le seguenti misure organizzative. <table border="1"> <tr><td>☒</td><td>Registro del trattamento in qualità di responsabile</td></tr> <tr><td>☒</td><td>Analisi dei rischi che incombono sugli interessati in relazione ai trattamenti effettuati</td></tr> <tr><td>☒</td><td>Nomina di un responsabile della protezione dei dati (se richiesto a livello legale)</td></tr> <tr><td>☒</td><td>Adozione di un sistema di gestione o di un Modello Organizzativo per la tutela dei dati personali</td></tr> <tr><td>☒</td><td>Adesione a codici di condotta in relazione al trattamento di dati personali</td></tr> <tr><td>☒</td><td>Contratti con i fornitori che svolgono parte dei trattamenti affidati (sub-responsabili) che prevedono meccanismi di tutela dei dati personali e relativi accordi di riservatezza</td></tr> <tr><td>☒</td><td>Piano di formazione del personale in relazione alla tutela dei dati personali</td></tr> <tr><td>☒</td><td>Autorizzazione formale al personale incaricato del trattamento dei dati personali affidati</td></tr> <tr><td>☒</td><td>Adozione di un accordo di riservatezza per il personale a cui è affidato il trattamento</td></tr> <tr><td>☒</td><td>Procedura per la risposta alle richieste di esercizio dei diritti degli interessati</td></tr> <tr><td>☒</td><td>Registrazione delle richieste di esercizio dei diritti degli interessati</td></tr> </table>	☒	Registro del trattamento in qualità di responsabile	☒	Analisi dei rischi che incombono sugli interessati in relazione ai trattamenti effettuati	☒	Nomina di un responsabile della protezione dei dati (se richiesto a livello legale)	☒	Adozione di un sistema di gestione o di un Modello Organizzativo per la tutela dei dati personali	☒	Adesione a codici di condotta in relazione al trattamento di dati personali	☒	Contratti con i fornitori che svolgono parte dei trattamenti affidati (sub-responsabili) che prevedono meccanismi di tutela dei dati personali e relativi accordi di riservatezza	☒	Piano di formazione del personale in relazione alla tutela dei dati personali	☒	Autorizzazione formale al personale incaricato del trattamento dei dati personali affidati	☒	Adozione di un accordo di riservatezza per il personale a cui è affidato il trattamento	☒	Procedura per la risposta alle richieste di esercizio dei diritti degli interessati	☒	Registrazione delle richieste di esercizio dei diritti degli interessati
☒	Registro del trattamento in qualità di responsabile																						
☒	Analisi dei rischi che incombono sugli interessati in relazione ai trattamenti effettuati																						
☒	Nomina di un responsabile della protezione dei dati (se richiesto a livello legale)																						
☒	Adozione di un sistema di gestione o di un Modello Organizzativo per la tutela dei dati personali																						
☒	Adesione a codici di condotta in relazione al trattamento di dati personali																						
☒	Contratti con i fornitori che svolgono parte dei trattamenti affidati (sub-responsabili) che prevedono meccanismi di tutela dei dati personali e relativi accordi di riservatezza																						
☒	Piano di formazione del personale in relazione alla tutela dei dati personali																						
☒	Autorizzazione formale al personale incaricato del trattamento dei dati personali affidati																						
☒	Adozione di un accordo di riservatezza per il personale a cui è affidato il trattamento																						
☒	Procedura per la risposta alle richieste di esercizio dei diritti degli interessati																						
☒	Registrazione delle richieste di esercizio dei diritti degli interessati																						
2.0	Gestione delle risposte agli incidenti che possono comportare violazioni dei dati personali / data breach Requisito: <i>Il Responsabile del trattamento deve implementare un proprio sistema di gestione degli incidenti e delle violazioni dei dati personali (cd. Data breach).</i> <i>Gli elementi includono:</i> <i>Un processo per segnalare violazioni della protezione dei dati personali (in particolare in cooperazione con il Titolare del trattamento)</i> <i>Una procedura per la gestione degli incidenti che possono comportare violazioni dei dati personali</i>																						
2.1	A tal fine vengono messe in atto le seguenti misure organizzative. <table border="1"> <tr><td>☒</td><td>Procedura per la risposta ad incidenti di sicurezza</td></tr> <tr><td>☒</td><td>Procedura per la gestione e la notifica delle violazioni dei dati (data breach)</td></tr> <tr><td>☒</td><td>Adozione di un registro dei data breach</td></tr> <tr><td>☒</td><td>Assegnazione dei ruoli di valutazione degli incidenti di sicurezza</td></tr> <tr><td>☒</td><td>Procedure o meccanismi di risposta agli incidenti di sicurezza, comprensivi dell'assegnazione di compiti e ruoli</td></tr> <tr><td>☒</td><td>Regole o procedure di segnalazione delle anomalie o degli incidenti di sicurezza da parte degli utenti</td></tr> </table>	☒	Procedura per la risposta ad incidenti di sicurezza	☒	Procedura per la gestione e la notifica delle violazioni dei dati (data breach)	☒	Adozione di un registro dei data breach	☒	Assegnazione dei ruoli di valutazione degli incidenti di sicurezza	☒	Procedure o meccanismi di risposta agli incidenti di sicurezza, comprensivi dell'assegnazione di compiti e ruoli	☒	Regole o procedure di segnalazione delle anomalie o degli incidenti di sicurezza da parte degli utenti										
☒	Procedura per la risposta ad incidenti di sicurezza																						
☒	Procedura per la gestione e la notifica delle violazioni dei dati (data breach)																						
☒	Adozione di un registro dei data breach																						
☒	Assegnazione dei ruoli di valutazione degli incidenti di sicurezza																						
☒	Procedure o meccanismi di risposta agli incidenti di sicurezza, comprensivi dell'assegnazione di compiti e ruoli																						
☒	Regole o procedure di segnalazione delle anomalie o degli incidenti di sicurezza da parte degli utenti																						



2.0	Protezione dei dati by design e by default Requisito: <i>il Responsabile del trattamento è obbligato a mettere in atto misure tecniche e organizzative nelle fasi iniziali della progettazione delle operazioni del trattamento, in modo da rispettare i principi della privacy e della protezione dei dati fin dall'inizio. Inoltre, il Responsabile del trattamento deve garantire che i dati personali vengano trattati con il massimo livello di protezione, in modo che i dati personali non siano accessibili a un numero indefinito di persone by default.</i>
2.1	A tal fine vengono messe in atto le seguenti misure organizzative .
	☒ Procedura di privacy by design e by default
3.0	Procedure di controllo Requisito: <i>il Responsabile deve mettere in atto politiche e procedure per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.</i>
3.1	A tal fine vengono messe in atto le seguenti misure organizzative .
	☒ Revisione periodica del sistema di trattamento dati e delle misure di sicurezza implementate
	☒ Audit interni periodici documentati
	☒ Audit del Responsabile della Protezione dei Dati (DPO) periodici documentati
	☒ Audit di seconda parte documentati
	☒ Audit di terza parte (es. come parte di procedure di certificazione o revisione di certificazioni)