Innovando GmbH

Dorfstrasse, 29
9108 Gonten
Tel: +41717941500
P.IVA CHE396.086.464

ELENCO DELLE MISURE DI SICUREZZA ADOTTATE

Sono sotto riportate le misure di sicurezza implementate ai sensi dell'art.32 del Reg.to UE 2016/679.

Misure di sicurezza adottate a livello logico ed organizzativo

Verifica periodica dell'ambito dei trattamenti e dei profili di autorizzazione.	Periodicamente, con cadenza almeno annuale, sono aggiornati gli ambiti del trattamento consentito agli addetti ed ai responsabili della gestione o manutenzione dei sistemi elettronici.
Consegna istruzioni dettagliate agli addetti.	Ad ogni addetto sono state consegnate istruzioni dettagliate e complete riguardanti il trattamento dei dati personali, a seconda dei suoi compiti e dei dati trattati. ► Istruzioni per la segretezza del sistema di autenticazione e la custodia dei dispositivi personali. Istruzioni per assicurare la segretezza della componente riservata della credenziale (es. password) e la diligente custodia dei dispositivi in possesso ed uso esclusivo dell'incaricato. ► Istruzioni sulla custodia degli strumenti elettronici durante le sessioni di trattamento. Sono impartite istruzioni agli incaricati per non lasciare incostudito e accessibile lo strumento elettronico durante una sessione di trattamento. ► Istruzioni per i supporti removibili in caso di dati sensibili o giudiziari. In caso di dati sensibili o giudiziari, sono 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. ► Istruzioni scritte finalizzate al controllo ed alla custodia dei documenti cartacei. Gli incaricati hanno ricevuto istruzioni scritte sul comportamento da tenere per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento.
Procedure per ripristino dei dati.	Sono state 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 ai 7 giorni.
E' stato redatto e viene annualmente aggiornato il Manuale Organizzativo Privacy.	Il Manuale Organizzativo Privacy contiene i documenti relativi all'adempimento delle misure minime di sicurezza, che sono rimasti obbligatori anche dopo l'abolizione del Documento Programmatico sulla Sicurezza.
Redazione del Registro dei Trattamenti sia in qualità di Titolare sia se necessario in qualità di Responsabile	Il Registro dei Trattamenti e documento cogente e contiene la lista dei trattamenti effettuati eventuali comunicazioni degli stessi all'esterno e relative misure di sicurezza attuate.

Redazione documento Privacy by Design e By Default	Redazione Piano di Privacy by Design e By Default per documentare per tutti i trattamenti l'attuazione delle necessarie misure di sicurezza ex. Art. 32 in grado di garantire un rischio residuale basso
Procedure Gestione Data Breach	Redazione ed Implementazione Procedure strutturale ed organizzative per la gestione di eventuali Data Breach
Implementazione Procedura di Nomina a Responsabile del trattamento	Implementazione Procedura di Nomina a Responsabile del trattamento per tutte le strutture esterne che trattano dati per conto del Titolare
Implementazione procedura di verifica per i Responsabile del trattamento	Implementazione procedura di verifica affinché i trattamenti effettuati da esterni abbiano adeguate garanzie di rischio residuale basso

Misure di sicurezza adottate per trattamento

• Banche e istituti finanziari per pagamenti e incassi

Gestione dati sensibili per pagamenti e incassi tramite banche e istituti di credito

Dati Comuni trattati :	• Codice fiscale ed altri numeri di identificazione personale • Nominativo, indirizzo o altri elementi di identificazione personale • Dati relativi allo svolgimento delle attività economiche dell'interessato. • Nome e cognome
Unità di archiviazione utilizzate per il trattamento	• Banche (sede:)

• Contabilità

Trattamento dati per la gestione della contabilità

Dati Comuni trattati :	• Codice fiscale ed altri numeri di identificazione personale • Nominativo, indirizzo o altri elementi di identificazione personale • Lavoro • Nome e cognome
Unità di archiviazione utilizzate per il trattamento	• Contabilità (sede:)

• Conto terzi

Trattamento dei dati nei rapporti con terzi per le lavorazioni esterne

Dati Comuni trattati :	• Codice fiscale ed altri numeri di identificazione personale • Nominativo, indirizzo o altri elementi di identificazione personale
Unità di archiviazione utilizzate per il trattamento	• Contabilità (sede:)

• Gestione del Personale

Redazione dei cedolini per le buste paga, versamento contributi e imposte alla fonte e gestione del personale interno ed esterno. La redazione dei cedonlini per le buste paga avviene internamente.

Dati Comuni trattati :	• Codice fiscale ed altri numeri di identificazione personale • Nominativo, indirizzo o altri elementi di identificazione personale • Lavoro
Unità di archiviazione utilizzate per il trattamento	• Synology RAID4 (sede: Sede principale azienda)

• Gestione finanziaria e controllo fiscale

Trattamento dei dati per la gestione finanziaria e il controllo fiscale

Dati Comuni trattati :	• Codice fiscale ed altri numeri di identificazione personale • Nominativo, indirizzo o altri elementi di identificazione personale • Attività economiche, commerciali, finanziarie e assicurative • Dati relativi al tipo di lavoro ed alla retribuzione • Nome e cognome

• Marketing

La gestione marketing dell'azienda avviene internamente

Dati Comuni trattati :	• Codice fiscale ed altri numeri di identificazione personale • Nominativo, indirizzo o altri elementi di identificazione personale • Attività economiche, commerciali, finanziarie e assicurative
Unità di archiviazione utilizzate per il trattamento	• Synology RAID4 (sede: Sede principale azienda)

• Pagina social Facebook

Gestione trattamento dati provenienti da pagina social facebook

Dati Comuni trattati :	• Nominativo, indirizzo o altri elementi di identificazione personale • Attività economiche, commerciali, finanziarie e assicurative • cookie essenziali (strictly necessary) • cookie di tipo statistico (performance cookie) • cookie di tipo funzionale alla navigazione (functionality cookie) • cookie di tipo pubblicitario (advertising cookie)
Unità di archiviazione utilizzate per il trattamento	• Synology RAID4 (sede: Sede principale azienda)

• Pagina social Google +

Gestione trattamento dati provenienti da pagina social Google +

Dati Comuni trattati :	• Nominativo, indirizzo o altri elementi di identificazione personale • Dati relativi allo svolgimento delle attività economiche dell'interessato. • cookie essenziali (strictly necessary) • cookie di tipo statistico (performance cookie) • cookie di tipo funzionale alla navigazione (functionality cookie) • cookie di tipo pubblicitario (advertising cookie)
Unità di archiviazione utilizzate per il trattamento	• Synology RAID4 (sede: Sede principale azienda)

• Pagina social Instagram

Gestione trattamento dati provenienti da pagina social Instagram

Dati Comuni trattati :	• Nominativo, indirizzo o altri elementi di identificazione personale • Attività economiche, commerciali, finanziarie e assicurative • cookie essenziali (strictly necessary) • cookie di tipo statistico (performance cookie) • cookie di tipo funzionale alla navigazione (functionality cookie) • cookie di tipo pubblicitario (advertising cookie)
Unità di archiviazione utilizzate per il trattamento	• Synology RAID4 (sede: Sede principale azienda)

• Pagina social LinkedIn

Gestione trattamento dati provenienti da pagina social LinkedIn

Dati Comuni trattati :	• Nominativo, indirizzo o altri elementi di identificazione personale • Attività economiche, commerciali, finanziarie e assicurative • cookie essenziali (strictly necessary) • cookie di tipo statistico (performance cookie) • cookie di tipo funzionale alla navigazione (functionality cookie) • cookie di tipo pubblicitario (advertising cookie)
Unità di archiviazione utilizzate per il trattamento	• Synology RAID4 (sede: Sede principale azienda)

• Pagina social Twitter

Gestione trattamento dati provenienti da pagina social Twitter

Dati Comuni trattati :	• Nominativo, indirizzo o altri elementi di identificazione personale • Dati relativi allo svolgimento delle attività economiche dell'interessato. • cookie essenziali (strictly necessary) • cookie di tipo statistico (performance cookie) • cookie di tipo funzionale alla navigazione (functionality cookie) • cookie di tipo pubblicitario (advertising cookie)
Unità di archiviazione utilizzate per il trattamento	• Synology RAID4 (sede: Sede principale azienda)

• Pagina social Youtube

Gestione trattamento dati provenienti da pagina social Youtube

Dati Comuni trattati :	• Nominativo, indirizzo o altri elementi di identificazione personale • Attività economiche, commerciali, finanziarie e assicurative • cookie essenziali (strictly necessary) • cookie di tipo statistico (performance cookie) • cookie di tipo funzionale alla navigazione (functionality cookie) • cookie di tipo pubblicitario (advertising cookie)
Unità di archiviazione utilizzate per il trattamento	• Synology RAID4 (sede: Sede principale azienda)

• Posta elettronica

Trattamento dei dati per la gestione della posta elettronica

Dati Comuni trattati :	• Codice fiscale ed altri numeri di identificazione personale • Nominativo, indirizzo o altri elementi di identificazione personale
Unità di archiviazione utilizzate per il trattamento	• Synology RAID4 (sede: Sede principale azienda)

• Sito Internet

Trattamento dei dati relativi alla gestione del sito internet

Dati Comuni trattati :	• cookie essenziali (strictly necessary) • cookie di tipo statistico (performance cookie) • cookie di tipo funzionale alla navigazione (functionality cookie) • cookie di tipo pubblicitario (advertising cookie)
Unità di archiviazione utilizzate per il trattamento	• Synology RAID4 (sede: Sede principale azienda)

• Vendite

Trattamento dei dati dei rapporti commenrciali con i clienti o potenziali clienti

Dati Comuni trattati :	• Codice fiscale ed altri numeri di identificazione personale • Nominativo, indirizzo o altri elementi di identificazione personale • Attività economiche, commerciali, finanziarie e assicurative
Unità di archiviazione utilizzate per il trattamento	• Synology RAID4 (sede: Sede principale azienda)

Misure di sicurezza adottate per archivio

• BANCHE

Trattamenti:	• Banche e istituti finanziari per pagamenti e incassi
Tipo di archivio	• Archivio in Cloud
Tipi di dati contenuti	• Dati comuni

Misure Adottate

Credenziali di autentificazione, assegnate individualmente ad ogni addetto.	Il trattamento dei dati è consentito solo dopo il superamento di una procedura di autentificazione univocamente associata all'addetto e relativa ad uno specifico trattamento o ad un insieme di trattamenti. Inoltre il codice di identificazione, quando utilizzato, non viene mai assegnato ad altri addetti, nemmeno in tempi diversi. ► Autenticazione mediante dispositivo di autenticazione ad uso esclusivo dell'incaricato. ► Parola chiave di almeno 8 caratteri. ► Disattivazione delle vecchie credenziali. ► Disposizioni scritte per la disponibilità dei dati.
Cifratura dei dati memorizzati.	I dati salvati su sistemi di archiviazione digitale vengono cifrati attraverso sistemi di protezione in ssl, PGP, o altri sistemi di cifratura proprietari
Cifratura dei dati trasmessi.	Quando vengono trasmessi da un sistema digitale ad un altro i dati prima della trasmissione vengono cifrati co sistemi di protezione come SSL, PGP, ZIP con password o altri Sistemi proprietari. Gli enti sanitari e gli operatori in ambito sanitario hanno l'obbligo di trasmettere i dati sensibili sulla salute utilizzando sistemi di cifratura
Sono stati adottati adeguati criteri tra cui l'eventuale nomina a Responsabile per garantire che la struttura esterna presso cui l'unità di archiviazione risiede abbia adeguate contromisure che garantiscano un rischio residuale basso.	Nel caso di archivio gestito in modalità ISP, è necessario che il gestore dell'archivio attui adeguate misure di sicurezza in modo da garantire rischi residuali bassi sui trattamenti. Vedere la sezione sul Registro dei Trattamenti per ulteriori informazione nel caso di dati affidati all'esterno.
Verifica e registrazione degli accessi dell'amministratore di sistema se questo è nominato direttamente dall'Azienda	
Verifica ed eventuale nomina degli amministratori di sistema se presenti	

• CONTABILITÀ

Trattamenti:	• Conto terzi • Contabilità
Tipo di archivio	• Archivio in Cloud
Tipi di dati contenuti	• Dati comuni

Misure Adottate

Cifratura dei dati memorizzati.	I dati salvati su sistemi di archiviazione digitale vengono cifrati attraverso sistemi di protezione in ssl, PGP, o altri sistemi di cifratura proprietari
Cifratura dei dati trasmessi.	Quando vengono trasmessi da un sistema digitale ad un altro i dati prima della trasmissione vengono cifrati co sistemi di protezione come SSL, PGP, ZIP con password o altri Sistemi proprietari. Gli enti sanitari e gli operatori in ambito sanitario hanno l'obbligo di trasmettere i dati sensibili sulla salute utilizzando sistemi di cifratura
Sono stati adottati adeguati criteri tra cui l'eventuale nomina a Responsabile per garantire che la struttura esterna presso cui l'unità di archiviazione risiede abbia adeguate contromisure che garantiscano un rischio residuale basso.	Nel caso di archivio gestito in modalità ISP, è necessario che il gestore dell'archivio attui adeguate misure di sicurezza in modo da garantire rischi residuali bassi sui trattamenti. Vedere la sezione sul Registro dei Trattamenti per ulteriori informazione nel caso di dati affidati all'esterno.
Verifica e registrazione degli accessi dell'amministratore di sistema se questo è nominato direttamente dall'Azienda	

• SYNOLOGY RAID4

Trattamenti:	• Vendite • Sito Internet • Posta elettronica • Pagina social Youtube • Pagina social Twitter • Pagina social LinkedIn • Pagina social Instagram • Pagina social Google + • Pagina social Facebook • Marketing • Gestione del Personale
Tipo di archivio	• Archivio digitale
Tipi di dati contenuti	• Dati comuni

Misure Adottate

Linea Dati Ridondante	Linea Dati Ridondante
Aumento Banda Trasmissione Dati	Aumento Banda Trasmissione Dati
Potenziamento Impianto Elettrico	Impianto elettrico a norma e sovrastrutturato per utilizzo
Gruppo Elettrogeno	Gruppo Elettrogeno
Installazione di un Firewall.	Nel caso di trattamento di dati personali con strumenti elettronici connessi con l'esterno, anche in maniere indiretta o solo saltuariamente, è necessario installare un firewall software od hardware per evitare l'accesso abusivo ad essi. ► Firewall hardware. ► Firewall software.
Installazione Impianto Antiincendio	Installazione Impianto Antiincendio

Installazione Allarme	Installazione Allarme
Installazione Porta Blindata	Installazione Porta Blindata
Estintori	Installazione Estintori e verifica periodica degli stessi.
Impianto di Drenaggio.	Installazione Impianto di Drenaggio
Accesso Controllato al locale.	Installazione Accesso Controllato con Badge Magnetici o altri sistemi di verifica digitali
Gruppo di continuità	Gruppo di continuità
Copie di Back-up.	Sono impartite istruzioni organizzative e tecniche e sono predisposte attrezzature elettroniche che prevedono il salvataggio dei dati con frequenza almeno settimanale. ► Back-Up giornaliero.
Antivirus.	Sono installati sugli elaboratori elettronici che contengono dati personali, programmi antivirus, aggiornati almeno semestralmente. ► Aggiornamento Giornaliero.
Credenziali di autentificazione, assegnate individualmente ad ogni addetto.	Il trattamento dei dati è consentito solo dopo il superamento di una procedura di autentificazione univocamente associata all'addetto e relativa ad uno specifico trattamento o ad un insieme di trattamenti. Inoltre il codice di identificazione, quando utilizzato, non viene mai assegnato ad altri addetti, nemmeno in tempi diversi. ► Autenticazione mediante user-id e password. ► Parola chiave di almeno 8 caratteri. ► Disattivazione delle vecchie credenziali. ► Disposizioni scritte per la disponibilità dei dati.
Sistema Operativo.	Il Sistema operativo deve poter autenticare in maniera sicura ed univoca gli addetti al trattamento. Specificare il sistema operativo installato sul sistema. ► Linux.
Aggiornamento Software.	Gli aggiornamenti periodici dei programmi, volti a prevenire la vulnerabilità o a correggere difetti, sono effettuati tenendo conto di avere installato almeno la versione precedente all'ultima disponibile.
Cifratura dei dati memorizzati.	I dati salvati su sistemi di archiviazione digitale vengono cifrati attraverso sistemi di protezione in ssl, PGP, o altri sistemi di cifratura proprietari
Cifratura dei dati trasmessi.	Quando vengono trasmessi da un sistema digitale ad un altro i dati prima della trasmissione vengono cifrati co sistemi di protezione come SSL, PGP, ZIP con password o altri Sistemi proprietari. Gli enti sanitari e gli operatori in ambito sanitario hanno l'obbligo di trasmettere i dati sensibili sulla salute utilizzando sistemi di cifratura
Monitoraggio Accessi.	Monitoraggio Accessi.
Sospensione automatica delle sessioni di lavoro.	Il sistema sospende automaticamente la sessione di lavoro in determinate circostanza (tipo dopo un tempo minimo di inattività).
Installazione Software testato e certificato.	Installazione Software testato e certificato.

sistema RAID.	E' presente un sistema di RAID (Redundant array of inexpensive disks), che permettono la disponibilità e l'integrità dei dati anche in caso di rottura di un singolo Hard-Disk
Sistema di Mirroring.	Presenza nel sistema di dischi ridondanti in mirroring (dati duplicati)
Profili di autorizzazione di ambito diverso per diversi incaricati.	Nel caso in cui gli incaricati possano accedere solo a certi tipi di dato, od effettuare solo alcuni trattamenti, i profili di autorizzazione devono essere diversificati per ciascun incaricato. ► E' utilizzato un sistema di autorizzazione. ► I profili di autorizzazione vengono specificati prima di ogni trattamento. ► Verifica periodica del profilo di autorizzazione.
Verifica e registrazione degli accessi dell'amministratore di sistema se questo è nominato direttamente dall'Azienda	
Separazione Fisica dellInformazioni di copia	Separazione Fisica delle copie delle informazioni in un luogo differente da quello dove vengono trattati i dati