Ditta individuale Avv. Christian Lavazza

Via T. Rodari 9
21052 Busto Arsizio (VA)
P.IVA 02710870128

Elenco delle misure di sicurezza consigliate

È sotto riportato un elenco non esaustivo delle misure di sicurezza consigliate. Tali misure derivano dagli ex artt. da 33 a 36 e dall'Allegato B del D.Lgs 196/2003 ad oggi modificato dal D.Lgs 101/2018. Nonostante queste misure non siano più obbligatorie per legge, costituiscono ancora una linea guida essenziale per raggiungere in maniera efficiente e veloce un livello di sicurezza minimo durante un trattamento dei dati personali. Il presente documento è esclusivamente ad uso interno dell'azienda.

Misure consigliate da adottare a livello organizzativo

Misure consigliate

Implementata	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. ► Implementata: Istruzioni per la segretezza del sistema di autenticazione e la custodia dei dispositivi personali. ► Implementata: Istruzioni sulla custodia degli strumenti elettronici durante le sessioni di trattamento. ► Implementata: Istruzioni per i supporti removibili in caso di dati sensibili o giudiziari. ► Implementata: Istruzioni scritte finalizzate al controllo ed alla custodia dei documenti cartacei.
Implementata	Descrizione scritta degli interventi effettuati da terzi. Quando ci si avvale di soggetti esterni per l'adozione pratica delle misure di sicurezza, viene richiesta la descrizione scritta dell'intervento effettuato che ne attesta la conformità a norma di legge.
Implementata	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.
Implementata	Distruzione dei supporti removibili. Nel caso di dati particolari o giudiziari, i supporti rimuovibili che contengono tali dati se non utilizzati sono distrutti o resi inutilizzabili, ovvero possono essere usati da personale non autorizzato solo dopo che i dati in essi contenuti sono resi non intelleggibili e tecnicamente in alcun modo recuperabili.
Consigliata	Individuazione estremi identificativi delle persone fisiche preposte quali amministratori di sistema dell'azienda di outsourcing esterna. Individuazione estremi identificativi delle persone fisiche preposte quali amministratori di sistema dell'azienda di outsourcing esterna.

Implementata	Verifica annuale operato Amministratori di Sistema. L'operato degli amministratori di sistema è verificato con cadenza almeno annuale da parte del Titolare al trattamento.
Implementata	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.
Consigliata	Redazione di un piano di formazione per gli addetti È previsto un piano di formazione degli addetti, per renderli edotti dei rischi che incombono sui dati, delle misure disponibili per prevedere eventi dannosi, dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure adottate. La formazione è programmata già al momento dell'ingresso in servizio, nonché in occasione di cambiamenti di mansioni, o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento dei dati personali.
Implementata	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
Consigliata	Nomina del DPO Nomina del Data Protection Officer
Implementata	Procedure Gestione Data Breach Redazione ed Implementazione Procedure strutturale ed organizzative per la gestione di eventuali Data Breach
Implementata	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
Implementata	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
Implementata	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.

Misure consigliate da adottare per ogni archivio

- **ARMADI**

Tipo di archivio:	• Archivio cartaceo.
Tipi di dati contenuti	• Dati Particolari, Dati Comuni.

Misure consigliate

Implementata	Archivio ad accesso controllato. L'accesso all'archivio è controllato dagli incaricati al trattamento o dalla sorveglianza. Dopo l'orario di chiusura possono accedere all'archivio solo le persone preventivamente autorizzate od identificate e registrate.
Implementata	Dotazione serrature archivio Se sono presenti dati particolari o giudiziari in archivi cartacei, è utilizzata una chiusura a chiave dell'archivio.
Implementata	Controllo dei documenti con dati particolari o giudiziari da parte degli addetti. Quando i documenti contenenti dati particolari o giudiziari sono affidati agli addetti del trattamento, sono controllati e custoditi dagli stessi fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate.
Implementata	Custodia in classificatori o armadi non accessibili I dati cartacei sono archiviati in modo da permettere l'accesso esclusivamente agli addetti al trattamento degli stessi e di non essere accessibili a persone non autorizzate.
Implementata	Dotazione serrature ufficio. Se sono presenti dati particolari o giudiziari in archivi cartacei, è utilizzata una chiusura a chiave dell'ufficio.
Consigliata	Separazione Fisica delle copie dei dati. Le copie cartacee dei dati personali vengono conservati in un luogo differente da quello dove vengono effettuati i trattamenti.

- **ARMADIO**

Tipo di archivio:	• Archivio cartaceo.
Tipi di dati contenuti	• Dati Comuni.

Misure consigliate

- **NOTEBOOK**

Tipo di archivio:	• Archivio digitale su rete pubblica.
Tipi di dati contenuti	• Dati Particolari, Dati Comuni.

Misure consigliate

Implementata	Sistema Operativo. Il Sistema operativo deve poter autenticare in maniera sicura ed univoca gli addetti al trattamento. Specificare il sistema operativo installato sul sistema. ► Implementata: Windows 10
Consigliata	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.
Implementata	Antivirus. Sono installati sugli elaboratori elettronici che contengono dati personali, programmi antivirus, aggiornati almeno semestralmente. ► Implementata: Aggiornamento Giornaliero.
Consigliata	Pseudonimizzazione. Pseudonimizzazione e cifratura dei dati personali
Implementata	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. ► Implementata: Parola chiave di almeno 8 caratteri. ► Implementata: Disattivazione delle vecchie credenziali. ► Implementata: Disposizioni scritte per la disponibilità dei dati. ► Implementata: Autenticazione mediante user-id e password.
Implementata	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.
Implementata	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. ► Implementata: È utilizzato un sistema di autorizzazione. ► Implementata: I profili di autorizzazione vengono specificati prima di ogni trattamento. ► Implementata: Verifica periodica del profilo di autorizzazione.
Implementata	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. ► Implementata: Firewall hardware.
Consigliata	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

• PC FISSO

Tipo di archivio:	• Archivio digitale su rete pubblica.

Tipi di dati contenuti	• Dati Particolari, Dati Comuni.

Misure consigliate

Implementata	Sistema Operativo. Il Sistema operativo deve poter autenticare in maniera sicura ed univoca gli addetti al trattamento. Specificare il sistema operativo installato sul sistema. ► Implementata: Windows 10
Consigliata	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.
Implementata	Antivirus. Sono installati sugli elaboratori elettronici che contengono dati personali, programmi antivirus, aggiornati almeno semestralmente. ► Implementata: Aggiornamento Giornaliero.
Consigliata	Pseudonimizzazione. Pseudonimizzazione e cifratura dei dati personali
Implementata	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. ► Implementata: Parola chiave di almeno 8 caratteri. ► Implementata: Disattivazione delle vecchie credenziali. ► Implementata: Disposizioni scritte per la disponibilità dei dati. ► Implementata: Autenticazione mediante user-id e password.
Implementata	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.
Implementata	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. ► Implementata: È utilizzato un sistema di autorizzazione. ► Implementata: I profili di autorizzazione vengono specificati prima di ogni trattamento. ► Implementata: Verifica periodica del profilo di autorizzazione.
Implementata	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. ► Implementata: Firewall hardware.
Consigliata	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

SERVER

Tipo di archivio:	• Archivio digitale su rete pubblica.
Tipi di dati contenuti	• Dati Particolari, Dati Comuni.

Misure consigliate

Implementata	Sistema Operativo. Il Sistema operativo deve poter autenticare in maniera sicura ed univoca gli addetti al trattamento. Specificare il sistema operativo installato sul sistema. ► Implementata: Windows 10
Implementata	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. ► Implementata: Back-Up giornaliero.
Implementata	Antivirus. Sono installati sugli elaboratori elettronici che contengono dati personali, programmi antivirus, aggiornati almeno semestralmente. ► Implementata: Aggiornamento Giornaliero.
Consigliata	Pseudonimizzazione. Pseudonimizzazione e cifratura dei dati personali
Implementata	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. ► Implementata: Parola chiave di almeno 8 caratteri. ► Implementata: Disattivazione delle vecchie credenziali. ► Implementata: Disposizioni scritte per la disponibilità dei dati. ► Implementata: Autenticazione mediante user-id e password.
Implementata	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.
Implementata	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. ► Implementata: È utilizzato un sistema di autorizzazione. ► Implementata: I profili di autorizzazione vengono specificati prima di ogni trattamento. ► Implementata: Verifica periodica del profilo di autorizzazione.
Implementata	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. ► Implementata: Firewall hardware.

Consigliata	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