

Ditta individuale Avv. Christian Lavazza

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

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 incostituito 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 removibili 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.

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.

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.

Verifica annuale operata Amministratori di Sistema.

L'operato degli amministratori di sistema è verificato con cadenza almeno annuale da parte del Titolare al trattamento.

Redazione del Registro dei Trattamenti sia in qualità di Titolare sia se necessario in qualità di Responsabile

Il Registro dei Trattamenti è 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

• Acquisti UE

Acquisti UE

| | |
|--|---|
| Dati Comuni trattati: | <ul style="list-style-type: none"> • codice fiscale ed altri numeri di identificazione personale; • nominativo, indirizzo o altri elementi di identificazione personale; • attività economiche, commerciali, finanziarie e assicurative. |
| Archivi utilizzati per il trattamento | <ul style="list-style-type: none"> • Armadi (Sede: Sede principale azienda); • Notebook (Sede: Sede principale azienda); • PC fisso (Sede: Sede principale azienda); • Server (Sede: Sede principale azienda). |

Misure Adottate

| | |
|--|---|
| Copertura Assicurativa | Stipula adeguata copertura assicurativa per eventi inerenti ai trattamenti dati relativi al GDPR |
| Installazione Allarme | Installazione Allarme |
| Installazione Porta Blindata | Installazione Porta Blindata |
| Dotazione serrature ufficio. | Se sono presenti dati particolari o giudiziari in archivi cartacei, è utilizzata una chiusura a chiave dell'ufficio. |
| Estintori | Installazione Estintori e verifica periodica degli stessi. |
| 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. |
| Dotazione serrature archivio | Se sono presenti dati particolari o giudiziari in archivi cartacei, è utilizzata una chiusura a chiave dell'archivio. |
| 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. |
| 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. |
| Separazione dei dati sulla salute dagli altri dati personali | I dati sulla salute sono separati in visualizzazione ed archiviazione dagli altri dati personali. Negli archivi cartacei basta che ad una prima occhiata non siano visibili i dati sulla salute. Gli enti sanitari hanno l'obbligo di separazione dei dati sulla salute dagli altri dati personali |
| Potenziamento Impianto Elettrico | Impianto elettrico a norma e sovrastrutturato per utilizzo |
| Installazione di un Firewall. | <p>Nel caso di trattamento di dati personali con strumenti elettronici connessi con l'esterno, anche in maniera indiretta o solo saltuariamente, è necessario installare un firewall software od hardware per evitare l'accesso abusivo ad essi.</p> <ul style="list-style-type: none"> ▶ Firewall hardware. Firewall hardware |

| | |
|--|---|
| Contratto di Manutenzione Hardware. | Un'azienda esterna cura la manutenzione e la gestione della componente Hardware del sistema informatico. |
| Antivirus. | Sono installati sugli elaboratori elettronici che contengono dati personali, programmi antivirus, aggiornati almeno semestralmente. <ul style="list-style-type: none">▶ Aggiornamento Giornaliero. |
| Credenziali di autenticazione, assegnate individualmente ad ogni addetto. | <p>Il trattamento dei dati è consentito solo dopo il superamento di una procedura di autenticazione 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.</p> <ul style="list-style-type: none">▶ Autenticazione mediante user-id e password.▶ Parola chiave di almeno 8 caratteri. Le parole chiave sono di 8 caratteri od il massimo consentito dal sistema, non devono essere riconducibili all'incaricato e vengono modificate almeno ogni 3 mesi (6 se vi sono solo dati comuni).▶ Disattivazione delle vecchie credenziali. Le credenziali di identificazione sono disattivate se non vengono usate da almeno sei mesi (salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica), oppure non appena l'incaricato perde la qualità di accedere ai dati personali.▶ Disposizioni scritte per la disponibilità dei dati. Quando l'accesso ai dati è consentito solo mediante l'uso della componente riservata della credenziale, sono impartite idonee e preventive disposizioni scritte volte ad individuare chiaramente le modalità con il quale si può assicurare la disponibilità dei dati in caso di prolungata assenza o impedimento dell'incaricato. |
| Sistema Operativo. | <p>Il Sistema operativo deve poter autenticare in maniera sicura ed univoca gli addetti al trattamento. Specificare il sistema operativo installato sul sistema.</p> <ul style="list-style-type: none">▶ Windows 10 Sistema Operativo Windows 10 |
| 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. |
| Sospensione automatica delle sessioni di lavoro. | Il sistema sospende automaticamente la sessione di lavoro in determinate circostanza (tipo dopo un tempo minimo di inattività). |
| Sospensione manuale delle sessioni di Lavoro. | Sospensione manuale delle sessioni di Lavoro. |
| Firma Elettronica. | Marcatura dei documenti e delle informazioni attraverso procedure di firma elettronica digitale. |
| Profili di autorizzazione di ambito diverso per diversi incaricati. | <p>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.</p> <ul style="list-style-type: none">▶ È utilizzato un sistema di autorizzazione. Sono definiti od utilizzati procedure e strumenti che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione.▶ I profili di autorizzazione vengono specificati prima di ogni trattamento. A ciascun incaricato viene assegnato il proprio profilo di autorizzazione prima dell'inizio del trattamento.▶ Verifica periodica del profilo di autorizzazione. Periodicamente, ed almeno annualmente, sono verificati i profili di autorizzazione. |

| | |
|---|--|
| Separazione dei dati sulla salute dagli altri dati personali su sistemi elettronici | I dati sulla salute sono separati in visualizzazione ed archiviazione dagli altri dati personali. Negli archivi elettronici basta che ad nella prima schermata non siano visibili i dati sulla salute. Gli enti sanitari hanno l'obbligo di separazione dei dati sulla salute dagli altri dati personali |
| Verifica e registrazione degli accessi dell'amministratore di sistema se questo è nominato direttamente dall'Azienda | 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 | Verifica ed eventuale nomina degli amministratori di sistema se presenti |
| 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. |

• Curriculum

Curriculum

| | |
|--|---|
| Dati Comuni trattati: | <ul style="list-style-type: none"> • codice fiscale ed altri numeri di identificazione personale; • nominativo, indirizzo o altri elementi di identificazione personale; • dati relativi alla famiglia e a situazioni personali; • lavoro; • istruzione e cultura; • dati relativi al tipo di lavoro ed alla retribuzione; • voti, giudizi ed altri dati di valutazione del rendimento scolastico. |
| Dati Particolari trattati: | <ul style="list-style-type: none"> • origini razziali o etniche; • stato di salute. |
| Archivi utilizzati per il trattamento | <ul style="list-style-type: none"> • Armadi (Sede: Sede principale azienda); • Notebook (Sede: Sede principale azienda); • PC fisso (Sede: Sede principale azienda); • Server (Sede: Sede principale azienda). |

Misure Adottate

| | |
|--|--|
| Copertura Assicurativa | Stipula adeguata copertura assicurativa per eventi inerenti ai trattamenti dati relativi al GDPR |
| Installazione Allarme | Installazione Allarme |
| Installazione Porta Blindata | Installazione Porta Blindata |
| Dotazione serrature ufficio. | Se sono presenti dati particolari o giudiziari in archivi cartacei, è utilizzata una chiusura a chiave dell'ufficio. |
| Estintori | Installazione Estintori e verifica periodica degli stessi. |
| 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. |

| | |
|--|---|
| Dotazione serrature archivio | Se sono presenti dati particolari o giudiziari in archivi cartacei, è utilizzata una chiusura a chiave dell'archivio. |
| 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. |
| 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. |
| Separazione dei dati sulla salute dagli altri dati personali | I dati sulla salute sono separati in visualizzazione ed archiviazione dagli altri dati personali. Negli archivi cartacei basta che ad una prima occhiata non siano visibili i dati sulla salute. Gli enti sanitari hanno l'obbligo di separazione dei dati sulla salute dagli altri dati personali |
| Potenziamento Impianto Elettrico | Impianto elettrico a norma e sovrastrutturato per utilizzo |
| 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. <ul style="list-style-type: none"> ▶ Firewall hardware. Firewall hardware |
| Contratto di Manutenzione Hardware. | Un'azienda esterna cura la manutenzione e la gestione della componente Hardware del sistema informatico. |
| Antivirus. | Sono installati sugli elaboratori elettronici che contengono dati personali, programmi antivirus, aggiornati almeno semestralmente. <ul style="list-style-type: none"> ▶ Aggiornamento Giornaliero. |
| Credenziali di autenticazione, assegnate individualmente ad ogni addetto. | Il trattamento dei dati è consentito solo dopo il superamento di una procedura di autenticazione 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. <ul style="list-style-type: none"> ▶ Autenticazione mediante user-id e password. ▶ Parola chiave di almeno 8 caratteri. Le parole chiave sono di 8 caratteri od il massimo consentito dal sistema, non devono essere riconducibili all'incaricato e vengono modificate almeno ogni 3 mesi (6 se vi sono solo dati comuni). ▶ Disattivazione delle vecchie credenziali. Le credenziali di identificazione sono disattivate se non vengono usate da almeno sei mesi (salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica), oppure non appena l'incaricato perde la qualità di accedere ai dati personali. ▶ Disposizioni scritte per la disponibilità dei dati. Quando l'accesso ai dati è consentito solo mediante l'uso della componente riservata della credenziale, sono impartite idonee e preventive disposizioni scritte volte ad individuare chiaramente le modalità con il quale si può assicurare la disponibilità dei dati in caso di prolungata assenza o impedimento dell'incaricato. |
| Sistema Operativo. | Il Sistema operativo deve poter autenticare in maniera sicura ed univoca gli addetti al trattamento. Specificare il sistema operativo installato sul sistema. <ul style="list-style-type: none"> ▶ Windows 10 Sistema Operativo Windows 10 |

| | |
|---|---|
| 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. |
| Sospensione automatica delle sessioni di lavoro. | Il sistema sospende automaticamente la sessione di lavoro in determinate circostanza (tipo dopo un tempo minimo di inattività). |
| Sospensione manuale delle sessioni di Lavoro. | Sospensione manuale delle sessioni di Lavoro. |
| Firma Elettronica. | Marcatore dei documenti e delle informazioni attraverso procedure di firma elettronica digitale. |
| Profili di autorizzazione di ambito diverso per diversi incaricati. | <p>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.</p> <ul style="list-style-type: none"> ▶ È utilizzato un sistema di autorizzazione. Sono definiti od utilizzati procedure e strumenti che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione. ▶ I profili di autorizzazione vengono specificati prima di ogni trattamento. A ciascun incaricato viene assegnato il proprio profilo di autorizzazione prima dell'inizio del trattamento. ▶ Verifica periodica del profilo di autorizzazione. Periodicamente, ed almeno annualmente, sono verificati i profili di autorizzazione. |
| Separazione dei dati sulla salute dagli altri dati personali su sistemi elettronici | I dati sulla salute sono separati in visualizzazione ed archiviazione dagli altri dati personali. Negli archivi elettronici basta che ad nella prima schermata non siano visibili i dati sulla salute. Gli enti sanitari hanno l'obbligo di separazione dei dati sulla salute dagli altri dati personali |
| Verifica e registrazione degli accessi dell'amministratore di sistema se questo è nominato direttamente dall'Azienda | 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 | Verifica ed eventuale nomina degli amministratori di sistema se presenti |
| Gruppo di continuità | Gruppo di continuità |
| Copie di Back-up. | <p>Sono impartite istruzioni organizzative e tecniche e sono predisposte attrezzature elettroniche che prevedono il salvataggio dei dati con frequenza almeno settimanale.</p> <ul style="list-style-type: none"> ▶ Back-Up giornaliero. |

• Posta elettronica

Posta elettronica

| | |
|--|--|
| Dati Comuni trattati: | <ul style="list-style-type: none"> • codice fiscale ed altri numeri di identificazione personale; • nominativo, indirizzo o altri elementi di identificazione personale. |
| Archivi utilizzati per il trattamento | <ul style="list-style-type: none"> • Armadi (Sede: Sede principale azienda); • Notebook (Sede: Sede principale azienda); • PC fisso (Sede: Sede principale azienda); • Server (Sede: Sede principale azienda). |

Misure Adottate

| | |
|--|--|
| Copertura Assicurativa | Stipula adeguata copertura assicurativa per eventi inerenti ai trattamenti dati relativi al GDPR |
| Installazione Allarme | Installazione Allarme |
| Installazione Porta Blindata | Installazione Porta Blindata |
| Dotazione serrature ufficio. | Se sono presenti dati particolari o giudiziari in archivi cartacei, è utilizzata una chiusura a chiave dell'ufficio. |
| Estintori | Installazione Estintori e verifica periodica degli stessi. |
| 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. |
| Dotazione serrature archivio | Se sono presenti dati particolari o giudiziari in archivi cartacei, è utilizzata una chiusura a chiave dell'archivio. |
| 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. |
| 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. |
| Separazione dei dati sulla salute dagli altri dati personali | I dati sulla salute sono separati in visualizzazione ed archiviazione dagli altri dati personali. Negli archivi cartacei basta che ad una prima occhiata non siano visibili i dati sulla salute. Gli enti sanitari hanno l'obbligo di separazione dei dati sulla salute dagli altri dati personali |
| Potenziamento Impianto Elettrico | Impianto elettrico a norma e sovrastrutturato per utilizzo |
| 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. <ul style="list-style-type: none"> ▶ Firewall hardware. Firewall hardware |
| Contratto di Manutenzione Hardware. | Un'azienda esterna cura la manutenzione e la gestione della componente Hardware del sistema informatico. |
| Antivirus. | Sono installati sugli elaboratori elettronici che contengono dati personali, programmi antivirus, aggiornati almeno semestralmente. <ul style="list-style-type: none"> ▶ Aggiornamento Giornaliero. |

| | |
|---|--|
| <p>Credenziali di autenticazione, assegnate individualmente ad ogni addetto.</p> | <p>Il trattamento dei dati è consentito solo dopo il superamento di una procedura di autenticazione 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.</p> <ul style="list-style-type: none"> ▶ Autenticazione mediante user-id e password. ▶ Parola chiave di almeno 8 caratteri. Le parole chiave sono di 8 caratteri od il massimo consentito dal sistema, non devono essere riconducibili all'incaricato e vengono modificate almeno ogni 3 mesi (6 se vi sono solo dati comuni). ▶ Disattivazione delle vecchie credenziali. Le credenziali di identificazione sono disattivate se non vengono usate da almeno sei mesi (salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica), oppure non appena l'incaricato perde la qualità di accedere ai dati personali. ▶ Disposizioni scritte per la disponibilità dei dati. Quando l'accesso ai dati è consentito solo mediante l'uso della componente riservata della credenziale, sono impartite idonee e preventive disposizioni scritte volte ad individuare chiaramente le modalità con il quale si può assicurare la disponibilità dei dati in caso di prolungata assenza o impedimento dell'incaricato. |
| <p>Sistema Operativo.</p> | <p>Il Sistema operativo deve poter autenticare in maniera sicura ed univoca gli addetti al trattamento. Specificare il sistema operativo installato sul sistema.</p> <ul style="list-style-type: none"> ▶ Windows 10 Sistema Operativo Windows 10 |
| <p>Aggiornamento Software.</p> | <p>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.</p> |
| <p>Sospensione automatica delle sessioni di lavoro.</p> | <p>Il sistema sospende automaticamente la sessione di lavoro in determinate circostanza (tipo dopo un tempo minimo di inattività).</p> |
| <p>Sospensione manuale delle sessioni di Lavoro.</p> | <p>Sospensione manuale delle sessioni di Lavoro.</p> |
| <p>Firma Elettronica.</p> | <p>Marcatatura dei documenti e delle informazioni attraverso procedure di firma elettronica digitale.</p> |
| <p>Profili di autorizzazione di ambito diverso per diversi incaricati.</p> | <p>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.</p> <ul style="list-style-type: none"> ▶ È utilizzato un sistema di autorizzazione. Sono definiti od utilizzati procedure e strumenti che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione. ▶ I profili di autorizzazione vengono specificati prima di ogni trattamento. A ciascun incaricato viene assegnato il proprio profilo di autorizzazione prima dell'inizio del trattamento. ▶ Verifica periodica del profilo di autorizzazione. Periodicamente, ed almeno annualmente, sono verificati i profili di autorizzazione. |
| <p>Separazione dei dati sulla salute dagli altri dati personali su sistemi elettronici</p> | <p>I dati sulla salute sono separati in visualizzazione ed archiviazione dagli altri dati personali. Negli archivi elettronici basta che ad nella prima schermata non siano visibili i dati sulla salute. Gli enti sanitari hanno l'obbligo di separazione dei dati sulla salute dagli altri dati personali</p> |

| | |
|---|---|
| Verifica e registrazione degli accessi dell'amministratore di sistema se questo è nominato direttamente dall'Azienda | 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 | Verifica ed eventuale nomina degli amministratori di sistema se presenti |
| 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. |

• Vendite - consulenza

Vendite - consulenza

| | |
|--|--|
| Dati Comuni trattati: | <ul style="list-style-type: none"> • codice fiscale ed altri numeri di identificazione personale; • nominativo, indirizzo o altri elementi di identificazione personale; • attività economiche, commerciali, finanziarie e assicurative. |
| Archivi utilizzati per il trattamento | <ul style="list-style-type: none"> • Armadi (Sede: Sede principale azienda); • Armadio (Sede: Sede aggiunta); • Notebook (Sede: Sede principale azienda); • PC fisso (Sede: Sede principale azienda); • Server (Sede: Sede principale azienda). |

Misure Adottate

| | |
|--|---|
| Copertura Assicurativa | Stipula adeguata copertura assicurativa per eventi inerenti ai trattamenti dati relativi al GDPR |
| Installazione Allarme | Installazione Allarme |
| Installazione Porta Blindata | Installazione Porta Blindata |
| Dotazione serrature ufficio. | Se sono presenti dati particolari o giudiziari in archivi cartacei, è utilizzata una chiusura a chiave dell'ufficio. |
| Estintori | Installazione Estintori e verifica periodica degli stessi. |
| 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. |
| Dotazione serrature archivio | Se sono presenti dati particolari o giudiziari in archivi cartacei, è utilizzata una chiusura a chiave dell'archivio. |
| 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. |
| 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. |

| | |
|--|---|
| Separazione dei dati sulla salute dagli altri dati personali | I dati sulla salute sono separati in visualizzazione ed archiviazione dagli altri dati personali. Negli archivi cartacei basta che ad una prima occhiata non siano visibili i dati sulla salute. Gli enti sanitari hanno l'obbligo di separazione dei dati sulla salute dagli altri dati personali |
| Copia dei documenti cartacei. | I documenti cartacei vengono copiati per garantire un ripristino dei dati in caso di perdita o danneggiamento, incendio, etc... |
| Distuggi Documenti | Apparecchio elettrico per distruggere i documenti cartacei in forma illeggibile |
| 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. |
| Potenziamento Impianto Elettrico | Impianto elettrico a norma e sovrastrutturato per utilizzo |
| 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. <ul style="list-style-type: none"> ▶ Firewall hardware. Firewall hardware |
| Contratto di Manutenzione Hardware. | Un'azienda esterna cura la manutenzione e la gestione della componente Hardware del sistema informatico. |
| Antivirus. | Sono installati sugli elaboratori elettronici che contengono dati personali, programmi antivirus, aggiornati almeno semestralmente. <ul style="list-style-type: none"> ▶ Aggiornamento Giornaliero. |
| Credenziali di autenticazione, assegnate individualmente ad ogni addetto. | Il trattamento dei dati è consentito solo dopo il superamento di una procedura di autenticazione 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. <ul style="list-style-type: none"> ▶ Autenticazione mediante user-id e password. ▶ Parola chiave di almeno 8 caratteri. Le parole chiave sono di 8 caratteri od il massimo consentito dal sistema, non devono essere riconducibili all'incaricato e vengono modificate almeno ogni 3 mesi (6 se vi sono solo dati comuni). ▶ Disattivazione delle vecchie credenziali. Le credenziali di identificazione sono disattivate se non vengono usate da almeno sei mesi (salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica), oppure non appena l'incaricato perde la qualità di accedere ai dati personali. ▶ Disposizioni scritte per la disponibilità dei dati. Quando l'accesso ai dati è consentito solo mediante l'uso della componente riservata della credenziale, sono impartite idonee e preventive disposizioni scritte volte ad individuare chiaramente le modalità con il quale si può assicurare la disponibilità dei dati in caso di prolungata assenza o impedimento dell'incaricato. |
| Sistema Operativo. | Il Sistema operativo deve poter autenticare in maniera sicura ed univoca gli addetti al trattamento. Specificare il sistema operativo installato sul sistema. <ul style="list-style-type: none"> ▶ Windows 10 Sistema Operativo Windows 10 |
| 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. |

| | |
|---|---|
| Sospensione automatica delle sessioni di lavoro. | Il sistema sospende automaticamente la sessione di lavoro in determinate circostanza (tipo dopo un tempo minimo di inattività). |
| Sospensione manuale delle sessioni di Lavoro. | Sospensione manuale delle sessioni di Lavoro. |
| Firma Elettronica. | Marcatura dei documenti e delle informazioni attraverso procedure di firma elettronica digitale. |
| Profili di autorizzazione di ambito diverso per diversi incaricati. | <p>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.</p> <ul style="list-style-type: none"> ▶ È utilizzato un sistema di autorizzazione. Sono definiti od utilizzati procedure e strumenti che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione. ▶ I profili di autorizzazione vengono specificati prima di ogni trattamento. A ciascun incaricato viene assegnato il proprio profilo di autorizzazione prima dell'inizio del trattamento. ▶ Verifica periodica del profilo di autorizzazione. Periodicamente, ed almeno annualmente, sono verificati i profili di autorizzazione. |
| Separazione dei dati sulla salute dagli altri dati personali su sistemi elettronici | I dati sulla salute sono separati in visualizzazione ed archiviazione dagli altri dati personali. Negli archivi elettronici basta che ad nella prima schermata non siano visibili i dati sulla salute. Gli enti sanitari hanno l'obbligo di separazione dei dati sulla salute dagli altri dati personali |
| Verifica e registrazione degli accessi dell'amministratore di sistema se questo è nominato direttamente dall'Azienda | 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 | Verifica ed eventuale nomina degli amministratori di sistema se presenti |
| Gruppo di continuità | Gruppo di continuità |
| Copie di Back-up. | <p>Sono impartite istruzioni organizzative e tecniche e sono predisposte attrezzature elettroniche che prevedono il salvataggio dei dati con frequenza almeno settimanale.</p> <ul style="list-style-type: none"> ▶ Back-Up giornaliero. |

Misure di sicurezza adottate per archivio

• ARMADI

| | |
|------------------------|--|
| Trattamenti | <ul style="list-style-type: none"> • Vendite - consulenza • Posta elettronica • Curriculum • Acquisti UE |
| Tipo di archivio: | <ul style="list-style-type: none"> • Archivio cartaceo. |
| Tipi di dati contenuti | <ul style="list-style-type: none"> • Dati Particolari, Dati Comuni. |

Misure Adottate

| | |
|---|---|
| Copertura Assicurativa | Stipula adeguata copertura assicurativa per eventi inerenti ai trattamenti dati relativi al GDPR |
| Installazione Allarme | Installazione Allarme |
| Installazione Porta Blindata | Installazione Porta Blindata |
| Dotazione serrature ufficio. | Se sono presenti dati particolari o giudiziari in archivi cartacei, è utilizzata una chiusura a chiave dell'ufficio. |
| Estintori | Installazione Estintori e verifica periodica degli stessi. |
| 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. |
| Dotazione serrature archivio | Se sono presenti dati particolari o giudiziari in archivi cartacei, è utilizzata una chiusura a chiave dell'archivio. |
| 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. |
| 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. |
| Separazione dei dati sulla salute dagli altri dati personali | I dati sulla salute sono separati in visualizzazione ed archiviazione dagli altri dati personali. Negli archivi cartacei basta che ad una prima occhiata non siano visibili i dati sulla salute. Gli enti sanitari hanno l'obbligo di separazione dei dati sulla salute dagli altri dati personali |

• ARMADIO

| | |
|------------------------|--|
| Trattamenti | <ul style="list-style-type: none"> • Vendite - consulenza |
| Tipo di archivio: | <ul style="list-style-type: none"> • Archivio cartaceo. |
| Tipi di dati contenuti | <ul style="list-style-type: none"> • Dati Comuni. |

Misure Adottate

| | |
|--|---|
| Copertura Assicurativa | Stipula adeguata copertura assicurativa per eventi inerenti ai trattamenti dati relativi al GDPR |
| Installazione Porta Blindata | Installazione Porta Blindata |
| Dotazione serrature ufficio. | Se sono presenti dati particolari o giudiziari in archivi cartacei, è utilizzata una chiusura a chiave dell'ufficio. |
| Estintori | Installazione Estintori e verifica periodica degli stessi. |
| 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. |
| Dotazione serrature archivio | Se sono presenti dati particolari o giudiziari in archivi cartacei, è utilizzata una chiusura a chiave dell'archivio. |
| Copia dei documenti cartacei. | I documenti cartacei vengono copiati per garantire un ripristino dei dati in caso di perdita o danneggiamento, incendio, etc... |
| 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. |
| Distruggi Documenti | Apparecchio elettrico per distruggere i documenti cartacei in forma illeggibile |
| Separazione dei dati sulla salute dagli altri dati personali | I dati sulla salute sono separati in visualizzazione ed archiviazione dagli altri dati personali. Negli archivi cartacei basta che ad una prima occhiata non siano visibili i dati sulla salute. Gli enti sanitari hanno l'obbligo di separazione dei dati sulla salute dagli altri dati personali |
| 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. |

• NOTEBOOK

| | |
|-------------------------------|--|
| Trattamenti | <ul style="list-style-type: none"> • Vendite - consulenza • Posta elettronica • Curriculum • Acquisti UE |
| Tipo di archivio: | <ul style="list-style-type: none"> • Archivio digitale su rete pubblica. |
| Tipi di dati contenuti | <ul style="list-style-type: none"> • Dati Particolari, Dati Comuni. |

Misure Adottate

| | |
|---|---|
| Potenziamento Impianto Elettrico | Impianto elettrico a norma e sovrastrutturato per utilizzo |
| Installazione di un Firewall. | <p>Nel caso di trattamento di dati personali con strumenti elettronici connessi con l'esterno, anche in maniera indiretta o solo saltuariamente, è necessario installare un firewall software od hardware per evitare l'accesso abusivo ad essi.</p> <ul style="list-style-type: none"> ▶ Firewall hardware. |

| | |
|--|--|
| Contratto di Manutenzione Hardware. | Un'azienda esterna cura la manutenzione e la gestione della componente Hardware del sistema informatico. |
| Copertura Assicurativa | Stipula adeguata copertura assicurativa per eventi inerenti ai trattamenti dati relativi al GDPR |
| Installazione Allarme | Installazione Allarme |
| Installazione Porta Blindata | Installazione Porta Blindata |
| Dotazione serrature ufficio. | Se sono presenti dati particolari o giudiziari in archivi cartacei, è utilizzata una chiusura a chiave dell'ufficio. |
| Estintori | Installazione Estintori e verifica periodica degli stessi. |
| Antivirus. | Sono installati sugli elaboratori elettronici che contengono dati personali, programmi antivirus, aggiornati almeno semestralmente. <ul style="list-style-type: none"> ▶ Aggiornamento Giornaliero. |
| Credenziali di autenticazione, assegnate individualmente ad ogni addetto. | Il trattamento dei dati è consentito solo dopo il superamento di una procedura di autenticazione 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. <ul style="list-style-type: none"> ▶ 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. <ul style="list-style-type: none"> ▶ Windows 10 |
| 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. |
| Sospensione automatica delle sessioni di lavoro. | Il sistema sospende automaticamente la sessione di lavoro in determinate circostanza (tipo dopo un tempo minimo di inattività). |
| Sospensione manuale delle sessioni di Lavoro. | Sospensione manuale delle sessioni di Lavoro. |
| Firma Elettronica. | Marcatatura dei documenti e delle informazioni attraverso procedure di firma elettronica digitale. |
| 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. <ul style="list-style-type: none"> ▶ È utilizzato un sistema di autorizzazione. ▶ I profili di autorizzazione vengono specificati prima di ogni trattamento. ▶ Verifica periodica del profilo di autorizzazione. |
| Separazione dei dati sulla salute dagli altri dati personali su sistemi elettronici | I dati sulla salute sono separati in visualizzazione ed archiviazione dagli altri dati personali. Negli archivi elettronici basta che ad nella prima schermata non siano visibili i dati sulla salute. Gli enti sanitari hanno l'obbligo di separazione dei dati sulla salute dagli altri dati personali |

Verifica e registrazione degli accessi dell'amministratore di sistema se questo è nominato direttamente dall'Azienda

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

Verifica ed eventuale nomina degli amministratori di sistema se presenti

• **PC FISSO**

| | |
|-------------------------------|--|
| Trattamenti | <ul style="list-style-type: none"> • Vendite - consulenza • Posta elettronica • Curriculum • Acquisti UE |
| Tipo di archivio: | <ul style="list-style-type: none"> • Archivio digitale su rete pubblica. |
| Tipi di dati contenuti | <ul style="list-style-type: none"> • Dati Particolari, Dati Comuni. |

Misure Adottate

| | |
|--|---|
| Potenziamento Impianto Elettrico | Impianto elettrico a norma e sovrastrutturato per utilizzo |
| Installazione di un Firewall. | <p>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.</p> <ul style="list-style-type: none"> ▶ Firewall hardware. |
| Contratto di Manutenzione Hardware. | Un'azienda esterna cura la manutenzione e la gestione della componente Hardware del sistema informatico. |
| Copertura Assicurativa | Stipula adeguata copertura assicurativa per eventi inerenti ai trattamenti dati relativi al GDPR |
| Installazione Allarme | Installazione Allarme |
| Installazione Porta Blindata | Installazione Porta Blindata |
| Dotazione serrature ufficio. | Se sono presenti dati particolari o giudiziari in archivi cartacei, è utilizzata una chiusura a chiave dell'ufficio. |
| Estintori | Installazione Estintori e verifica periodica degli stessi. |
| Antivirus. | <p>Sono installati sugli elaboratori elettronici che contengono dati personali, programmi antivirus, aggiornati almeno semestralmente.</p> <ul style="list-style-type: none"> ▶ Aggiornamento Giornaliero. |
| Credenziali di autenticazione, assegnate individualmente ad ogni addetto. | <p>Il trattamento dei dati è consentito solo dopo il superamento di una procedura di autenticazione 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.</p> <ul style="list-style-type: none"> ▶ 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. <ul style="list-style-type: none"> ▶ Windows 10 |
| 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. |
| Sospensione automatica delle sessioni di lavoro. | Il sistema sospende automaticamente la sessione di lavoro in determinate circostanza (tipo dopo un tempo minimo di inattività). |
| Sospensione manuale delle sessioni di Lavoro. | Sospensione manuale delle sessioni di Lavoro. |
| Firma Elettronica. | Marcatatura dei documenti e delle informazioni attraverso procedure di firma elettronica digitale. |
| 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. <ul style="list-style-type: none"> ▶ È utilizzato un sistema di autorizzazione. ▶ I profili di autorizzazione vengono specificati prima di ogni trattamento. ▶ Verifica periodica del profilo di autorizzazione. |
| Separazione dei dati sulla salute dagli altri dati personali su sistemi elettronici | I dati sulla salute sono separati in visualizzazione ed archiviazione dagli altri dati personali. Negli archivi elettronici basta che ad nella prima schermata non siano visibili i dati sulla salute. Gli enti sanitari hanno l'obbligo di separazione dei dati sulla salute dagli altri dati personali |
| Verifica e registrazione degli accessi dell'amministratore di sistema se questo è nominato direttamente dall'Azienda | 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 | Verifica ed eventuale nomina degli amministratori di sistema se presenti |

• **SERVER**

| | |
|-------------------------------|--|
| Trattamenti | <ul style="list-style-type: none"> • Vendite - consulenza • Posta elettronica • Curriculum • Acquisti UE |
| Tipo di archivio: | <ul style="list-style-type: none"> • Archivio digitale su rete pubblica. |
| Tipi di dati contenuti | <ul style="list-style-type: none"> • Dati Particolari, Dati Comuni. |

Misure Adottate

| | |
|---|---|
| Potenziamento Impianto Elettrico | Impianto elettrico a norma e sovrastrutturato per utilizzo |
| 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. <ul style="list-style-type: none"> ▶ Firewall hardware. |

| | |
|--|--|
| Contratto di Manutenzione Hardware. | Un'azienda esterna cura la manutenzione e la gestione della componente Hardware del sistema informatico. |
| Copertura Assicurativa | Stipula adeguata copertura assicurativa per eventi inerenti ai trattamenti dati relativi al GDPR |
| Installazione Allarme | Installazione Allarme |
| Installazione Porta Blindata | Installazione Porta Blindata |
| Dotazione serrature ufficio. | Se sono presenti dati particolari o giudiziari in archivi cartacei, è utilizzata una chiusura a chiave dell'ufficio. |
| Estintori | Installazione Estintori e verifica periodica degli stessi. |
| 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. <ul style="list-style-type: none"> ▶ Back-Up giornaliero. |
| Antivirus. | Sono installati sugli elaboratori elettronici che contengono dati personali, programmi antivirus, aggiornati almeno semestralmente. <ul style="list-style-type: none"> ▶ Aggiornamento Giornaliero. |
| Credenziali di autenticazione, assegnate individualmente ad ogni addetto. | Il trattamento dei dati è consentito solo dopo il superamento di una procedura di autenticazione 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. <ul style="list-style-type: none"> ▶ 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. <ul style="list-style-type: none"> ▶ Windows 10 |
| 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. |
| Sospensione automatica delle sessioni di lavoro. | Il sistema sospende automaticamente la sessione di lavoro in determinate circostanza (tipo dopo un tempo minimo di inattività). |
| Sospensione manuale delle sessioni di Lavoro. | Sospensione manuale delle sessioni di Lavoro. |
| Firma Elettronica. | Marca dei documenti e delle informazioni attraverso procedure di firma elettronica digitale. |

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.

- ▶ È utilizzato un sistema di autorizzazione.
- ▶ I profili di autorizzazione vengono specificati prima di ogni trattamento.
- ▶ Verifica periodica del profilo di autorizzazione.

Separazione dei dati sulla salute dagli altri dati personali su sistemi elettronici

I dati sulla salute sono separati in visualizzazione ed archiviazione dagli altri dati personali. Negli archivi elettronici basta che ad nella prima schermata non siano visibili i dati sulla salute. Gli enti sanitari hanno l'obbligo di separazione dei dati sulla salute dagli altri dati personali

Verifica e registrazione degli accessi dell'amministratore di sistema se questo è nominato direttamente dall'Azienda

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

Verifica ed eventuale nomina degli amministratori di sistema se presenti