Ditta individuale Avv. Christian Lavazza

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

REGISTRO DELLE ATTIVITÀ DI TRATTAMENTO

Elenco dei trattamenti

Elenco dei Trattamenti e dei Soggetti Interessati.

Elenco dei trattamenti affidati ad enti esterni

Elenco dei trattamenti affidati ad enti esterni.

Elenco delle misure di sicurezza per ogni trattamento

Descrizione generale delle misure di sicurezza tecniche ed organizzative di cui all'Art. 32, paragrafo 1 del Regolamento Europeo, finalizzate al registro dei trattamenti.

Ditta individuale Avv. Christian Lavazza

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

ELENCO DEI TRATTAMENTI E DEI SOGGETTI INTERESSATI

Viene qui riportato un elenco dettagliato contenente la descrizione dei dati personali trattati suddivisi per sedi, trattamenti, ed archivi. È inoltre disponibile l'elenco dei soggetti interessati con relativi trattamenti coinvolti, dati trattati, finalità e liceità degli stessi.

La descrizione dettagliata delle aree di competenza, dei compiti e delle istruzioni affidati ai singoli soggetti è reperibile consultando la corrispondente nomina a responsabile od ad incaricato.

Titolare del Trattamento:	Ditta individuale Avv. Christian Lavazza nella persona di Christian Lavazza.

Sedi interessate ai trattamenti dei dati personali.

- **Sede Aggiunta**

Indirizzo:	• Viale Duca d'Aosta n. 15 , 21052 Busto Arsizio (VA)
Responsabili:	• Responsabile della sicurezza: Christian Lavazza

Sono sotto riportati gli uffici od i locali della sede interessati al trattamento od alla conservazione dei dati personali.

Archivio sede aggiunta	• Archivio cartaceo sede aggiunta

- **Sede Principale Azienda**

Indirizzo:	• Via T. Rodari 9 , 21052 Busto Arsizio (VA); P. IVA: 02710870128

Sono sotto riportati gli uffici od i locali della sede interessati al trattamento od alla conservazione dei dati personali.

Ufficio principale	• Ufficio principale

Elenco Trattamenti

- ## Acquisti UE

  Acquisti UE

Elenco dei responsabili designati ai sensi del D.lgs 101/2018:	• Lisa Bonomo • Maria Cristina Cenacchi • Elena Maria Gagliardi • Christian Lavazza
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.
Interessati al trattamento:	• fornitori.
Ultimo aggiornamento valutazione di impatto:	• 12/06/2018

Archivi del trattamento

1 - Armadi (Sede: Sede principale azienda)

Descrizione archivio:	• Armadi chiusi
Tipo di archivio:	• Archivio cartaceo.
Ufficio	• Ufficio principale

2 - Notebook (Sede: Sede principale azienda)

Descrizione archivio:	• n. 4 computer portatili Studio
Tipo di archivio:	• Archivio digitale.
Ufficio	• Ufficio principale

3 - PC fisso (Sede: Sede principale azienda)

Descrizione archivio:	• N. 1 PC fisso di Studio
Tipo di archivio:	• Archivio digitale.
Ufficio	• Ufficio principale

4 - Server (Sede: Sede principale azienda)

Descrizione archivio:	• Server di Studio
Tipo di archivio:	• Archivio digitale.
Ufficio	• Ufficio principale

- ## Curriculum

  Curriculum

Elenco dei responsabili designati ai sensi del D.lgs 101/2018:	• Maria Cristina Cenacchi • Elena Maria Gagliardi • Christian Lavazza
Dati Comuni trattati:	• 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:	• origini razziali o etniche; • stato di salute.
Interessati al trattamento:	• candidati da considerare per l'instaurazione di un rapporto di lavoro.
Ultimo aggiornamento valutazione di impatto:	• 12/06/2018

Archivi del trattamento

1 - Armadi (Sede: Sede principale azienda)

Descrizione archivio:	• Armadi chiusi
Tipo di archivio:	• Archivio cartaceo.
Ufficio	• Ufficio principale

2 - Notebook (Sede: Sede principale azienda)

Descrizione archivio:	• n. 4 computer portatili Studio
Tipo di archivio:	• Archivio digitale.
Ufficio	• Ufficio principale

3 - PC fisso (Sede: Sede principale azienda)

Descrizione archivio:	• N. 1 PC fisso di Studio
Tipo di archivio:	• Archivio digitale.
Ufficio	• Ufficio principale

4 - Server (Sede: Sede principale azienda)

Descrizione archivio:	• Server di Studio
Tipo di archivio:	• Archivio digitale.
Ufficio	• Ufficio principale

- **Posta elettronica**

  Posta elettronica

Elenco dei responsabili designati ai sensi del D.lgs 101/2018:	• Lisa Bonomo • Maria Cristina Cenacchi • Elena Maria Gagliardi • Christian Lavazza
Dati Comuni trattati:	• codice fiscale ed altri numeri di identificazione personale; • nominativo, indirizzo o altri elementi di identificazione personale.
Interessati al trattamento:	• candidati da considerare per l'instaurazione di un rapporto di lavoro; • clienti; • consulenti e liberi professionisti, anche in forma associata; • fornitori; • potenziali clienti.
Ultimo aggiornamento valutazione di impatto:	• 12/06/2018

Archivi del trattamento

1 - Armadi (Sede: Sede principale azienda)

Descrizione archivio:	• Armadi chiusi
Tipo di archivio:	• Archivio cartaceo.
Ufficio	• Ufficio principale

2 - Notebook (Sede: Sede principale azienda)

Descrizione archivio:	• n. 4 computer portatili Studio
Tipo di archivio:	• Archivio digitale.
Ufficio	• Ufficio principale

3 - PC fisso (Sede: Sede principale azienda)

Descrizione archivio:	• N. 1 PC fisso di Studio
Tipo di archivio:	• Archivio digitale.
Ufficio	• Ufficio principale

4 - Server (Sede: Sede principale azienda)

Descrizione archivio:	• Server di Studio
Tipo di archivio:	• Archivio digitale.
Ufficio	• Ufficio principale

• Vendite - consulenza

Vendite - consulenza

Elenco dei responsabili designati ai sensi del D.lgs 101/2018:	• Lisa Bonomo • Maria Cristina Cenacchi • Elena Maria Gagliardi • Christian Lavazza
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.
Interessati al trattamento:	• clienti; • consulenti e liberi professionisti, anche in forma associata.
Ultimo aggiornamento valutazione di impatto:	• 12/06/2018

Archivi del trattamento

1 - Armadi (Sede: Sede principale azienda)

Descrizione archivio:	• Armadi chiusi
Tipo di archivio:	• Archivio cartaceo.
Ufficio	• Ufficio principale

2 - Armadio (Sede: Sede aggiunta)

Descrizione archivio:	• Armadio sede aggiunta
Tipo di archivio:	• Archivio cartaceo.
Ufficio	• Archivio sede aggiunta

3 - Notebook (Sede: Sede principale azienda)

Descrizione archivio:	• n. 4 computer portatili Studio
Tipo di archivio:	• Archivio digitale.
Ufficio	• Ufficio principale

4 - PC fisso (Sede: Sede principale azienda)

Descrizione archivio:	• N. 1 PC fisso di Studio
Tipo di archivio:	• Archivio digitale.
Ufficio	• Ufficio principale

5 - Server (Sede: Sede principale azienda)

Descrizione archivio:	• Server di Studio
Tipo di archivio:	• Archivio digitale.
Ufficio	• Ufficio principale

Categorie di soggetti interessate al trattamento

Riportiamo ora in maggior dettaglio i trattamenti effettuati, distinguendo a quali soggetti interessati appartengono i dati oggetto di trattamento. Ulteriori informazioni a riguardo possono essere trovate, se previste, nelle relative informative.

• candidati da considerare per l'instaurazione di un rapporto di lavoro

Trattamenti coinvolti:	• Curriculum • Posta elettronica
Dati trattati:	• codice fiscale ed altri numeri di identificazione personale; • dati relativi al tipo di lavoro ed alla retribuzione; • dati relativi alla famiglia e a situazioni personali; • istruzione e cultura; • lavoro; • nominativo, indirizzo o altri elementi di identificazione personale; • origini razziali o etniche; • stato di salute; • voti, giudizi ed altri dati di valutazione del rendimento scolastico.
Finalità del trattamento: **[base giuridica]**	• selezione del personale per l'instaurazione di un rapporto di lavoro [richiesta di consenso].
Tipologie di trattamento dei dati:	• trattamento a mezzo di calcolatori elettronici; • trattamento manuale a mezzo di archivi cartacei.
Tempo di conservazione dei dati:	• stabilito per un arco di tempo non superiore al conseguimento delle finalità per le quali sono raccolti e trattati per l'esecuzione e l'espletamento delle finalità contrattuali.

• clienti

Trattamenti coinvolti:	• Posta elettronica • Vendite - consulenza
Dati trattati:	• codice fiscale ed altri numeri di identificazione personale; • nominativo, indirizzo o altri elementi di identificazione personale.
Finalità del trattamento: **[base giuridica]**	• adempimenti obbligatori per legge in campo fiscale e contabile [obbligo di legge o contrattuale]; • gestione del contenzioso [obbligo di legge o contrattuale]; • gestione della clientela [obbligo di legge o contrattuale]; • programmazione delle attività [obbligo di legge o contrattuale]; • storico fatturazione clienti [obbligo di legge o contrattuale].
Tipologie di trattamento dei dati:	• affidamento a terzi di operazioni di elaborazione; • creazione di profili relativi a clienti, fornitori o consumatori; • trattamento a mezzo di calcolatori elettronici; • trattamento manuale a mezzo di archivi cartacei.
Tempo di conservazione dei dati:	• stabilito per un arco di tempo non superiore al conseguimento delle finalità per le quali sono raccolti e trattati per l'esecuzione e l'espletamento delle finalità contrattuali; • stabilito per un arco di tempo non superiore all'espletamento dei servizi erogati; • stabilito per un arco di tempo non superiore al conseguimento delle finalità per le quali sono raccolti e trattati e nel rispetto dei tempi obbligatori prescritti dalla legge.

I dati potranno essere comunicati a: **[base giuridica]**	• associazioni di enti locali [richiesta di consenso]; • associazioni e fondazioni [richiesta di consenso]; • banche e istituti di credito [obbligo di legge o contrattuale]; • comunicazione di legge relativa alla normativa antiriciclaggio (legge 5 luglio 1991, n. 197 e successive modificazioni; D.Lgs. 20 febbraio 2004, n. 56; Legge 25 gennaio 2006, n. 29; D.D. M.M. 3 febbraio 2006, n.n. 141, 142 e 143; Provvedimento UIC (Ufficio Italiano Cambi) 24 febbraio 2006) [obbligo di legge o contrattuale]; • consulenti e liberi professionisti, anche in forma associata [obbligo di legge o contrattuale]; • datori di lavoro [richiesta di consenso]; • enti locali [richiesta di consenso]; • nell'ambito di soggetti pubblici e/o privati per i quali la comunicazione dei dati è obbligatoria o necessaria in adempimento ad obblighi di legge o sia comunque funzionale all'amministrazione del rapporto [obbligo di legge o contrattuale]; • enti pubblici economici [obbligo di legge o contrattuale]; • enti pubblici non economici [obbligo di legge o contrattuale]; • familiari dell'interessato [richiesta di consenso]; • forze armate [obbligo di legge o contrattuale]; • forze di polizia [obbligo di legge o contrattuale]; • ordini e collegi professionali [richiesta di consenso]; • organizzazioni di volontariato [richiesta di consenso].

• consulenti e liberi professionisti, anche in forma associata

Trattamenti coinvolti:	• Posta elettronica • Vendite - consulenza
Dati trattati:	• codice fiscale ed altri numeri di identificazione personale; • nominativo, indirizzo o altri elementi di identificazione personale.
Finalità del trattamento: **[base giuridica]**	• adempimento degli obblighi di legge relativi alla normativa antiriciclaggio (legge 5 luglio 1991, n. 197 e successive modificazioni; D.Lgs. 20 febbraio 2004, n. 56; Legge 25 gennaio 2006, n. 29; D.D. M.M. 3 febbraio 2006, n.n. 141, 142 e 143; Provvedimento UIC (Ufficio Italiano Cambi) 24 febbraio 2006) [obbligo di legge o contrattuale]; • adempimenti obbligatori per legge in campo fiscale e contabile [obbligo di legge o contrattuale]; • attività di consulenza [obbligo di legge o contrattuale]; • gestione della clientela [obbligo di legge o contrattuale]; • programmazione delle attività [obbligo di legge o contrattuale]; • storico fatturazione clienti [obbligo di legge o contrattuale].
Tipologie di trattamento dei dati:	• trattamento a mezzo di calcolatori elettronici; • trattamento manuale a mezzo di archivi cartacei.
Tempo di conservazione dei dati:	• stabilito per un arco di tempo non superiore al conseguimento delle finalità per le quali sono raccolti e trattati per l'esecuzione e l'espletamento delle finalità contrattuali; • stabilito per un arco di tempo non superiore all'espletamento dei servizi erogati; • stabilito per un arco di tempo non superiore al conseguimento delle finalità per le quali sono raccolti e trattati e nel rispetto dei tempi obbligatori prescritti dalla legge.

• fornitori

Trattamenti coinvolti:	• Acquisti UE • Posta elettronica
Dati trattati:	• attività economiche, commerciali, finanziarie e assicurative; • codice fiscale ed altri numeri di identificazione personale; • nominativo, indirizzo o altri elementi di identificazione personale.
Finalità del trattamento: **[base giuridica]**	• adempimenti obbligatori per legge in campo fiscale e contabile [obbligo di legge o contrattuale]; • gestione dei fornitori [obbligo di legge o contrattuale]; • di obblighi previsti dalle leggi vigenti [obbligo di legge o contrattuale]; • programmazione delle attività [obbligo di legge o contrattuale]; • storico ordini forniture [obbligo di legge o contrattuale].
Tipologie di trattamento dei dati:	• affidamento a terzi di operazioni di elaborazione; • trattamento a mezzo di calcolatori elettronici; • trattamento manuale a mezzo di archivi cartacei.
Tempo di conservazione dei dati:	• stabilito per un arco di tempo non superiore al conseguimento delle finalità per le quali sono raccolti e trattati per l'esecuzione e l'espletamento delle finalità contrattuali; • stabilito per un arco di tempo non superiore all'espletamento dei servizi erogati; • stabilito per un arco di tempo non superiore al conseguimento delle finalità per le quali sono raccolti e trattati e nel rispetto dei tempi obbligatori prescritti dalla legge.
I dati potranno essere comunicati a: **[base giuridica]**	• banche e istituti di credito [obbligo di legge o contrattuale]; • consulenti e liberi professionisti, anche in forma associata [obbligo di legge o contrattuale]; • spedizionieri, Trasportatori, Padroncini, Poste, Aziende per la Logistica [obbligo di legge o contrattuale].

- **potenziali clienti**

Trattamenti coinvolti:	• Posta elettronica
Dati trattati:	• codice fiscale ed altri numeri di identificazione personale; • nominativo, indirizzo o altri elementi di identificazione personale.
Finalità del trattamento: **[base giuridica]**	• gestione della clientela [obbligo di legge o contrattuale].
Tipologie di trattamento dei dati:	• trattamento a mezzo di calcolatori elettronici; • trattamento manuale a mezzo di archivi cartacei.
Tempo di conservazione dei dati:	• stabilito per un arco di tempo non superiore all'espletamento dei servizi erogati; • stabilito per un arco di tempo non superiore al conseguimento delle finalità per le quali sono raccolti e trattati e nel rispetto dei tempi obbligatori prescritti dalla legge.

Ditta individuale Avv. Christian Lavazza

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

ELENCO DEI RESPONSABILI ESTERNI

Da. Sa. Consulting srls

Da. Sa. Consulting srls
Piazza CArlo Noé n. 1
21052 Busto Arsizio (VA)
P. IVA 03610720124

I dati affidati all'esterno fanno riferimento ai seguenti trattamenti:

Acquisti UE

Dati Comuni:	• codice fiscale ed altri numeri di identificazione personale • nominativo, indirizzo o altri elementi di identificazione personale • attività economiche, commerciali, finanziarie e assicurative

Vendite - consulenza

Dati Comuni:	• codice fiscale ed altri numeri di identificazione personale • nominativo, indirizzo o altri elementi di identificazione personale • attività economiche, commerciali, finanziarie e assicurative

Finalità del Trattamento:

Elaborazione contabilità e dichiarazione dei redditi

Criterio adottato per garantire il rispetto delle misure di sicurezza:

La nomina dell'affidatario a Responsabile del trattamento.

Banca Cariparma

Banca Cariparma
Agenzia 344
Busto Arsizio, Piazza Manzoni n.17

I dati affidati all'esterno fanno riferimento ai seguenti trattamenti:

Acquisti UE

Dati Comuni:	• codice fiscale ed altri numeri di identificazione personale • nominativo, indirizzo o altri elementi di identificazione personale • attività economiche, commerciali, finanziarie e assicurative

Vendite - consulenza

Dati Comuni:	• codice fiscale ed altri numeri di identificazione personale • nominativo, indirizzo o altri elementi di identificazione personale • attività economiche, commerciali, finanziarie e assicurative

Finalità del Trattamento:

Pagamenti da cliente e verso fornitori

Criterio adottato per garantire il rispetto delle misure di sicurezza:

La nomina dell'affidatario a Responsabile del trattamento.

Banca BPM

Banca BPM
Busto Arsizio, Via Fratelli d'Italia 4

I dati affidati all'esterno fanno riferimento ai seguenti trattamenti:

Acquisti UE

Dati Comuni:	• codice fiscale ed altri numeri di identificazione personale • nominativo, indirizzo o altri elementi di identificazione personale • attività economiche, commerciali, finanziarie e assicurative

Vendite - consulenza

Dati Comuni:	• codice fiscale ed altri numeri di identificazione personale • nominativo, indirizzo o altri elementi di identificazione personale • attività economiche, commerciali, finanziarie e assicurative

Finalità del Trattamento:

pagamenti da clienti e verso fornitori

Criterio adottato per garantire il rispetto delle misure di sicurezza:

La nomina dell'affidatario a Responsabile del trattamento.

EMMEA Service srl di Marchetti Alessandro

EMMEA Service srl di Marchetti Alessandro
Via F. Corridoni n. 10
21052 Busto Arsizio (VA)
P. IVA 07658820969
C.F. MRCLSN70L16B300S

I dati affidati all'esterno fanno riferimento ai seguenti trattamenti:

Posta elettronica

Dati Comuni:	• codice fiscale ed altri numeri di identificazione personale • nominativo, indirizzo o altri elementi di identificazione personale

Finalità del Trattamento:

Assistenza e consulenza in materia informatica, anche in relazioni alle componenti hardware e software dello Studio; assistenza tecnica on site e da remoto.

L'affidatario è responsabile alla gestione ordinaria dei seguenti archivi:

Notebook, PC fisso, Server

Criterio adottato per garantire il rispetto delle misure di sicurezza:

La nomina dell'affidatario a Responsabile del trattamento.

Banca CREDEM

Piazza Garibaldi
21052 Busto Arsizio (VA)

I dati affidati all'esterno fanno riferimento ai seguenti trattamenti:

Posta elettronica

Dati Comuni:	• codice fiscale ed altri numeri di identificazione personale • nominativo, indirizzo o altri elementi di identificazione personale

Finalità del Trattamento:

Pagamenti

Criterio adottato per garantire il rispetto delle misure di sicurezza:

La nomina dell'affidatario a Responsabile del trattamento.

D.ssa Sara Labate

D.ssa Sara Labate - Ordine dei Commercialisti di Busto Arsizio
P. za CArlo Noé n. 1
21052 Busto Arsizio (VA)
P. IVA 03448600126
C.F. LBTSRA88D45B300B

I dati affidati all'esterno fanno riferimento ai seguenti trattamenti:

Acquisti UE

Dati Comuni:	• codice fiscale ed altri numeri di identificazione personale • nominativo, indirizzo o altri elementi di identificazione personale • attività economiche, commerciali, finanziarie e assicurative

Vendite - consulenza

Dati Comuni:	• codice fiscale ed altri numeri di identificazione personale • nominativo, indirizzo o altri elementi di identificazione personale • attività economiche, commerciali, finanziarie e assicurative

Finalità del Trattamento:

Contabilità; consulenza in materia fiscale e societaria.

Criterio adottato per garantire il rispetto delle misure di sicurezza:

La nomina dell'affidatario a Responsabile del trattamento.

Ditta individuale Avv. Christian Lavazza

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

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.
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 operato 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 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

- **Acquisti UE**

Acquisti UE

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.
Archivi utilizzati per il trattamento	• 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. ▸ 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. ► 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. 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. ► 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.	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. 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:	• 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:	• origini razziali o etniche; • stato di salute.
Archivi utilizzati per il trattamento	• 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. ► 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. ► 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. 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. ► 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.	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. 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.

• Posta elettronica

Posta elettronica

Dati Comuni trattati:	• codice fiscale ed altri numeri di identificazione personale; • nominativo, indirizzo o altri elementi di identificazione personale.
Archivi utilizzati per il trattamento	• 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. ► 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. ► 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. 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. ► 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.	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. 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.

• Vendite - consulenza

Vendite - consulenza

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.
Archivi utilizzati per il trattamento	• 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...
Distruggi 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. ► 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. ► 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. 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. ► 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.	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. 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.