Quint S.r.l.

Piazza Città di Lombardia 1
20124 Milano (MI)
P.IVA 11483430960
PEC: quint@legalmail.it
Cod. Doc. 20598.86.220666.0

REGISTRO DELLE ATTIVITÀ DI TRATTAMENTO: Servizi - Talent Assessment - Conto Terzi

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:	Quint S.r.l. nella persona di Simone Gargenti.
Responsabile della protezione dei dati (DPO) art. 37 Reg.to UE 2016/679 :	Jaera S.r.l. (Numero di protocollo Autorità: 20220002544).

Sedi interessate ai trattamenti dei dati personali.

- **Sede Principale Azienda**

Indirizzo:	• Piazza Città di Lombardia 1 , 20124 Milano (MI)

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

01_Ufficio	• 01_Ufficio

Elenco trattamenti conto terzi

- **Servizi - Talent Assessment - Conto Terzi**

  Acquisizione dati personali dei dipendenti e collaboratori inviati dal cliente e loro inserimento nelle piattaforme di analisi.

Dati Comuni trattati:	• Dati e informazioni riguardanti la carriera dell'interessato; • Report individuale comportamentale (con punteggi e informazioni qualitative); • Istruzione; • Nominativo, indirizzo email o altri elementi di identificazione personale; • Posizionamento in ranking di gruppo; • Posizione organizzativa; • Punteggi sintetici di potenziale e/o readiness; • Report individuale di personalità; • Codice identificativo; • Profilo psicometrico.
Interessati al trattamento:	• Interessati gestiti conto terzi.
Ultimo aggiornamento valutazione di impatto:	• 13/05/2022
Elenco delle evidenze ai sensi dell'art. 5 punto 2 relativamente al punto 1 comma a, b e c del Reg.to UE 2016/679:	• 07/04/2022 - Titolare - 5.1.a: Gestione per obblighi di legge e contrattuali 5.1.b: Gestione attività di vendita 5.1.c: Acquisizione dei dati strettamente necessari relativamente ai clienti e ai referenti presso le aziende clienti

Archivi del trattamento

1 - 01_MacBook Pro_Gadda (Sede: Sede principale azienda)

Tipo di archivio:	• Archivio digitale.
Ufficio	• 01_Ufficio

2 - 01_MacBook Pro_Gargenti (Sede: Sede principale azienda)

Tipo di archivio:	• Archivio digitale.
Ufficio	• 01_Ufficio

3 - Deeper Signals

Descrizione archivio:	• https://app.deepersignals.com/login
Tipo di archivio:	• Archivio in Cloud.

4 - Dropbox Business

Tipo di archivio:	• Archivio in Cloud.

5 - PICO QuintApp

Descrizione archivio:	• https://app.quint.org/login
Tipo di archivio:	• Archivio in Cloud.

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.

- **Interessati gestiti conto terzi**

Trattamenti coinvolti:	• Gestione Licenze - Conto Terzi • Servizi - Talent Acquisition - Conto Terzi • Servizi - Talent Assessment - Conto Terzi • Servizi - Consulenza Progettuale - Conto Terzi • Servizi - Organizational Network Analysis - Conto Terzi • Servizi - Deeper Signals - Conto Terzi
	• attività economiche, commerciali, finanziarie e assicurative; • codice fiscale ed altri numeri di identificazione personale; • Dati e informazioni riguardanti la carriera dell'interessato; • Dati personali comuni; • dati relativi al tipo di lavoro ed alla retribuzione; • dati relativi alla famiglia e a situazioni personali;

Dati trattati:	• dati sul comportamento; • informazioni concernenti i provvedimenti giudiziari; • istruzione e cultura; • lavoro; • Log File di Navigazione Internet; • nominativo, indirizzo o altri elementi di identificazione personale; • Punteggi di sintesi e ranking; • Report individuale comportamentale (con punteggi e informazioni qualitative); • stato di salute; • Username; • voti, giudizi ed altri dati di valutazione del rendimento scolastico.
Tipologie di trattamento dei dati:	• a mezzo calcolatori elettronici con utilizzo di sistemi software gestiti da Terzi; • a mezzo calcolatori elettronici con utilizzo di sistemi software gestiti o programmati direttamente; • affidamento a terzi di operazioni di elaborazione; • creazione di profili professionali o relativi a candidati; • raccolta di dati tramite test psicoattitudinali.; • trattamento manuale a mezzo di archivi cartacei; • trattamento mediante mezzi elettronici.
Tempo di conservazione dei dati:	• 5 - 10 anni ai sensi dell'art. 2948 codice civile che prevede la prescrizione di 5 anni per i pagamenti periodici; art. 2220 codice civile che prevede la conservazione per 10 anni delle scritture contabili; art. 22 del D.P.R. 29 Settembre 1973, n.600.; • 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; • Nel rispetto dei termini prescritti dalla legge per la tipologia di attività e comunque fino alla revoca del consenso o fino all'esercizio del diritto di opposizione ai sensi del Provv. generale del 15/05/13; art. 21 Reg. UE 2016/679.
I dati potranno essere comunicati a: **[base giuridica]**	• banche e istituti di credito [adempimento contrattuale]; • consulenti e liberi professionisti, anche in forma associata [adempimento contrattuale]; • 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]; • subfornitori [adempimento contrattuale].
I dati potranno essere trasferiti in: **[base giuridica]**	• paesi UE [obbligo di legge o contrattuale].

Quint S.r.l.

Piazza Città di Lombardia 1
20124 Milano (MI)
P.IVA 11483430960
PEC: quint@legalmail.it
Cod. Doc. 20598.86.220666.0

ELENCO DEI RESPONSABILI ESTERNI

Apple Inc.

One Apple Park Way, CA 95014, Cupertino, USA
Telefono: 1 408 996 1010

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

Acquisti - Fornitori

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

Amministrazione

Dati Comuni:	• 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 • attività economiche, commerciali, finanziarie e assicurative • istruzione e cultura • voti, giudizi ed altri dati di valutazione del rendimento scolastico • dati relativi al tipo di lavoro ed alla retribuzione
Dati Particolari:	• adesione a sindacati • stato di salute
Dati relativi a condanne penali e reati:	• informazioni concernenti i provvedimenti giudiziari

Marketing - Business Development

Dati Comuni:	• codice fiscale ed altri numeri di identificazione personale • nominativo, indirizzo o altri elementi di identificazione personale • lavoro • istruzione e cultura • dati sul comportamento • Dati e informazioni riguardanti la carriera dell'interessato • Punteggi di sintesi e ranking • Report individuale comportamentale (con punteggi e informazioni qualitative)

Servizi - Talent Acquisition

Dati Comuni:	• Dati e informazioni riguardanti la carriera dell'interessato • Report individuale comportamentale (con punteggi e informazioni qualitative) • Istruzione • Nominativo, indirizzo email o altri elementi di identificazione personale • Posizionamento in ranking di gruppo • Posizione organizzativa • Punteggi sintetici di potenziale e/o readiness • Report individuale di personalità • Codice identificativo

Servizi - Talent Acquisition - Conto Terzi

Dati Comuni:	• Dati e informazioni riguardanti la carriera dell'interessato • Report individuale comportamentale (con punteggi e informazioni qualitative) • Istruzione • Nominativo, indirizzo email o altri elementi di identificazione personale • Posizionamento in ranking di gruppo • Posizione organizzativa • Punteggi sintetici di potenziale e/o readiness • Report individuale di personalità • Codice identificativo

Servizi - Talent Assessment

Dati Comuni:	• Dati e informazioni riguardanti la carriera dell'interessato • Report individuale comportamentale (con punteggi e informazioni qualitative) • Istruzione • Nominativo, indirizzo email o altri elementi di identificazione personale • Posizionamento in ranking di gruppo • Posizione organizzativa • Punteggi sintetici di potenziale e/o readiness • Report individuale di personalità • Codice identificativo • Profilo psicometrico

Servizi - Talent Assessment - Conto Terzi

Dati Comuni:	• Dati e informazioni riguardanti la carriera dell'interessato • Report individuale comportamentale (con punteggi e informazioni qualitative) • Istruzione • Nominativo, indirizzo email o altri elementi di identificazione personale • Posizionamento in ranking di gruppo • Posizione organizzativa • Punteggi sintetici di potenziale e/o readiness • Report individuale di personalità • Codice identificativo • Profilo psicometrico

Servizi - Consulenza Progettuale - Conto Terzi

Dati Comuni:	• Dati e informazioni riguardanti la carriera dell'interessato • Istruzione • Nominativo, indirizzo email o altri elementi di identificazione personale • Posizione organizzativa • Report individuale di personalità • Codice identificativo • Profilo psicometrico

Vendite

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:

Sistema di backup

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

01_MacBook Pro_Gargenti, 01_iPhone_Gargenti

Criterio adottato per garantire il rispetto delle misure di sicurezza:

L'adozione di apposite clausole contrattuali, nelle quali l'affidatario è disciplinato ai sensi dell'art. 28.2, 28.3 e 28.4.

Dropbox, Inc.

1800 Owens St, CA 94158, San Francisco, USA

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

Acquisti - Fornitori

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

Amministrazione

Dati Comuni:	• 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 • attività economiche, commerciali, finanziarie e assicurative • istruzione e cultura • voti, giudizi ed altri dati di valutazione del rendimento scolastico • dati relativi al tipo di lavoro ed alla retribuzione
Dati Particolari:	• adesione a sindacati • stato di salute
Dati relativi a condanne penali e reati:	• informazioni concernenti i provvedimenti giudiziari

Marketing - Business Development

Dati Comuni:	• codice fiscale ed altri numeri di identificazione personale • nominativo, indirizzo o altri elementi di identificazione personale • lavoro • istruzione e cultura • dati sul comportamento • Dati e informazioni riguardanti la carriera dell'interessato • Punteggi di sintesi e ranking • Report individuale comportamentale (con punteggi e informazioni qualitative)

Servizi - Talent Acquisition

Dati Comuni:	• Dati e informazioni riguardanti la carriera dell'interessato • Report individuale comportamentale (con punteggi e informazioni qualitative) • Istruzione • Nominativo, indirizzo email o altri elementi di identificazione personale • Posizionamento in ranking di gruppo • Posizione organizzativa • Punteggi sintetici di potenziale e/o readiness • Report individuale di personalità • Codice identificativo

Servizi - Talent Acquisition - Conto Terzi

Dati Comuni:	• Dati e informazioni riguardanti la carriera dell'interessato • Report individuale comportamentale (con punteggi e informazioni qualitative) • Istruzione • Nominativo, indirizzo email o altri elementi di identificazione personale • Posizionamento in ranking di gruppo • Posizione organizzativa • Punteggi sintetici di potenziale e/o readiness • Report individuale di personalità • Codice identificativo

Servizi - Talent Assessment

Dati Comuni:	• Dati e informazioni riguardanti la carriera dell'interessato • Report individuale comportamentale (con punteggi e informazioni qualitative) • Istruzione • Nominativo, indirizzo email o altri elementi di identificazione personale • Posizionamento in ranking di gruppo • Posizione organizzativa • Punteggi sintetici di potenziale e/o readiness • Report individuale di personalità • Codice identificativo • Profilo psicometrico

Servizi - Talent Assessment - Conto Terzi

Dati Comuni:	• Dati e informazioni riguardanti la carriera dell'interessato • Report individuale comportamentale (con punteggi e informazioni qualitative) • Istruzione • Nominativo, indirizzo email o altri elementi di identificazione personale • Posizionamento in ranking di gruppo • Posizione organizzativa • Punteggi sintetici di potenziale e/o readiness • Report individuale di personalità • Codice identificativo • Profilo psicometrico

Servizi - Consulenza Progettuale - Conto Terzi

Dati Comuni:	• Dati e informazioni riguardanti la carriera dell'interessato • Istruzione • Nominativo, indirizzo email o altri elementi di identificazione personale • Posizione organizzativa • Report individuale di personalità • Codice identificativo • Profilo psicometrico

Vendite

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:

Dropbox

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

Dropbox Business

Criterio adottato per garantire il rispetto delle misure di sicurezza:

L'adozione di apposite clausole contrattuali, nelle quali l'affidatario è disciplinato ai sensi dell'art. 28.2, 28.3 e 28.4.

Adeguatezza:

Adeguatezza rilevata il da: PrivacyLab

Quint S.r.l.

Piazza Città di Lombardia 1
20124 Milano (MI)
P.IVA 11483430960
PEC: quint@legalmail.it
Cod. Doc. 20598.86.220666.0

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

Redazione di un piano di formazione per gli addetti	È previsto un piano di formazione degli addetti, per renderli edotti dei rischi che incombono sui dati, delle misure disponibili per prevedere eventi dannosi, dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure adottate. La formazione è programmata già al momento dell'ingresso in servizio, nonché in occasione di cambiamenti di mansioni, o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento dei dati personali.
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.
È stato redatto e viene annualmente aggiornato il Manuale Organizzativo Privacy.	Il Manuale Organizzativo Privacy contiene i documenti e le procedure organizzative ed operative da effettuarsi da parte degli operatori durante un trattamento di dati personali.
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.
Individuazione estremi identificativi delle persone fisiche preposte quali amministratori di sistema dell'azienda di outsourcing esterna.	Individuazione estremi identificativi delle persone fisiche preposte quali amministratori di sistema dell'azienda di outsourcing esterna.
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
Nomina del DPO	Nomina del Data Protection Officer
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
Verifica delle valutazioni preventive ai sensi dell'art. 5 paragrafo 1 del GDPR.	Ogni Titolare ai sensi dell'articolo 5 paragrafo 2 deve essere in grado di dare evidenza della valutazione effettuata prima e durante il trattamento dei dati. Il Titolare del trattamento deve essere in grado di dimostrare la conformità delle attività dello stesso compresa l'efficacia delle misure di sicurezza ai sensi dell'articolo 32 e della Privacy by Design e by Default ai sensi dell'articolo 25 del GDPR.

Misure di sicurezza adottate per trattamento

- **Servizi - Talent Assessment - Conto Terzi**

Acquisizione dati personali dei dipendenti e collaboratori inviati dal cliente e loro inserimento nelle piattaforme di analisi.

Dati Comuni trattati:	• Dati e informazioni riguardanti la carriera dell'interessato; • Report individuale comportamentale (con punteggi e informazioni qualitative); • Istruzione; • Nominativo, indirizzo email o altri elementi di identificazione personale; • Posizionamento in ranking di gruppo; • Posizione organizzativa; • Punteggi sintetici di potenziale e/o readiness; • Report individuale di personalità; • Codice identificativo; • Profilo psicometrico.
Archivi utilizzati per il trattamento	• Deeper Signals ; • PICO QuintApp ; • 01_MacBook Pro_Gadda (Sede: Sede principale azienda); • 01_MacBook Pro_Gargenti (Sede: Sede principale azienda); • Dropbox Business .

Misure Adottate

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. ► Back-Up in Cloud. Back-Up Su Sitemi in CLOUD
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. ► Autenticazione mediante caratteristica biometrica dell'incaricato.
Cifratura dei dati memorizzati.	I dati salvati su sistemi di archiviazione digitale vengono cifrati attraverso sistemi di protezione in ssl, PGP, o altri sistemi di cifratura proprietari

Cifratura dei dati trasmessi.	Quando vengono trasmessi da un sistema digitale ad un altro i dati prima della trasmissione vengono cifrati co sistemi di protezione come SSL, PGP, ZIP con password o altri Sistemi proprietari. Gli enti sanitari e gli operatori in ambito sanitario hanno l'obbligo di trasmettere i dati sensibili sulla salute utilizzando sistemi di cifratura ► Cifratura con protocollo SSL.
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.
Trattamento dei dati con protocolli criptati.	Trattamento dei dati con protocolli criptati ad es. SSL o criptazione dei dati tramite PGP
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.
Sono stati adottati adeguati criteri tra cui l'eventuale nomina a Responsabile per garantire che la struttura esterna presso cui l'unità di archiviazione risiede abbia adeguate contromisure che garantiscano un rischio residuale basso.	Nel caso di archivio gestito in modalità ISP, è necessario che il gestore dell'archivio attui adeguate misure di sicurezza in modo da garantire rischi residuali bassi sui trattamenti. Vedere la sezione sul Registro dei Trattamenti per ulteriori informazioni nel caso di dati affidati all'esterno.
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
Pseudonimizzazione.	Pseudonimizzazione e cifratura dei 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.
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 software. Firewall Software
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. ► Aggiornamento Giornaliero.
Sistema Operativo.	Il Sistema operativo deve poter autenticare in maniera sicura ed univoca gli addetti al trattamento. Specificare il sistema operativo installato sul sistema. ► Mac OS X
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.
Installazione Software testato e certificato.	Installazione Software testato e certificato.