

PRIVACY

Dott.ssa
Stefania Bosis

Data Protection Impact Assessment

-

Valutazione di Impatto Privacy

Informazioni sul PIA

PIA

Dott.ssa Stefania Bosis

Nome autore

Avv. Stefano Paoletti

Nome assessore

SB

Nome convalidatore

SB

Data di creazione

25/05/2018

Nome DPO

SB

Parere DPO

Vedere Piano di Azione

Ricerca del parere di persone interessate

Non è richiesto il parere di persone interessate.

Motivazione per cui il parere delle persone interessate non stato richiesto

Non è necessario

Contesto

Panoramica

Quale è il trattamento in considerazione?

La dott.ssa Stefania Bosis nata a Rho il 28 giugno 1971 con studio in Lainate (MI) Via Mazzini 46 CF. BSSSFN71H68H264F e P.Iva 05021160964 iscritto all'ordine dei dottori Commercialisti di Milano (di seguito anche lo "**Studio**" o il "**Titolare**") tratta i dati dei seguenti soggetti:

1. **Clienti** persone fisiche a cui si fornisce un servizio (di seguito il "**Servizio**") di assistenza e consulenza contabile e fiscale e elaborazione dati e buste paga;
2. **Rappresentanti** (persone fisiche) di persone giuridiche clienti dello Studio;
3. **Collaborati e Dipendenti**.
4. **Fornitori**;

I dati trattati sono:

- dati anagrafici;
- residenza abitazione;

- dati bancari in caso di pagamento della fattura del elgale a mezzo bonifico bancario;
- indirizzi email per le comunicazioni relative all'erogazione del servizio;
- eventuali dati personali relativi alle dichiarazioni dei redditi, quali scontrini spese mediche ecc.;

La base giuridica del trattamento è:

- per il Servizio di natura consulenziale: contratto d'opera professione ex art 2229 e seguenti Codice Civile;
- per i collaboratori a partita IVA rapporto d'opera professionale;
- per i dipendenti contratto di lavoro subordinato ai sensi dell'articolo 2096 e segg del codice civile e del contratto collettivo nazionale applicabile.
- per i Fornitori: contratto di vendita o di somministrazione

Quali sono le responsabilità legate al trattamento?

Io Studio archivia e tratta i dati dei clienti al fine di predisporre contabilità, bilanci, dichiarazione dei redditi, buste paga
Le responsabilità possono essere associate alla perdita dei dati per causa di furto dei server o dei dati tramite un attacco hacker o per danneggiamento a seguito di allagamento incendi od altro.

Ci sono standard applicabili al trattamento?

Vengono applicati per il trattamento gli standard di riferimento per la categoria dei Dottori Commercialisti previsti dal relativo codice di condotta

Valutazione : Accettabile

Dati, processi e risorse di supporto

Quali sono i dati trattati?

Io Studio tratta i Dati di

1. **Clienti** persone fisiche a cui si fornisce un servizio (di seguito il "**Servizio**") di assistenza e consulenza contabile e fiscale e elaborazione dati e buste paga;
2. **Rappresentanti** (persone fisiche) di persone giuridiche clienti dello Studio;
3. **Collaborati e Dipendenti**.
4. **Fornitori**;

I dati trattati sono:

- dati anagrafici;
- residenza abitazione;
- dati bancari in caso di pagamento della fattura del elgale a mezzo bonifico bancario;
- indirizzi email per le comunicazioni relative all'erogazione del servizio;
- eventuali dati personali relativi alle dichiarazioni dei redditi, quali scontrini spese mediche ecc.;
- ogni altro dato connesso alla predisposizione delle dichiarazioni dei redditi o all'assistenza richiesta oggetto del Servizio con particolare riguardo alla possibilità di trattare Dati sensibili

Com'è il ciclo di vita del trattamento dei dati?

I dati dei clienti sono raccolti seguendo il seguente processo:

- richiesta di erogazione del Servizio da parte del Cliente;
- comunicazione dati anagrafici per predisposizione del contratto di conferimento di incarico;
- sottoscrizione del contratto e registrazione dati nel gestionale telematico e cartaceo;
- raccolta documenti a fini antiriciclaggio e registrazione ed archiviazione nel registro anti-riciclaggio;
- registrazione ed archiviazione dati digitali e cartacei;
- svolgimento del Servizio richiesto;
- invio fatturazione
- archiviazione e tenuta fascicolo cartaceo e digitale per dieci anni.

Quali sono le risorse di supporto ai dati?

I dati sono archiviati per cliente/pratica su gestionale installato con regolare licenza su PC server e PC Clients dotati di, Antivirus e Password di accesso nonché supporto file cartaceo che ripropone, in cartaceo, tutti i file contenuti sul supporto

digitale.

Lo Studio utilizza per il trattamento dei Dati applicativi gestionali per la comunicazione all'Amministrazione Finanziaria Entratel, Client di Posta Elettronica, Banche Dati di Accesso al Catasto, Conservatoria, Registro Imprese, di seguito anche gli **"Applicativi"**.

Ogni PC dello Studio è in rete con regolare licenza installata gestita da amministratore di rete. L'accesso ad ogni PC avviene mediante digitazione di password di almeno 8 caratteri.

Ulteriormente l'accesso agli Applicativi sopra indicati avviene con password.

Nello svolgimento del Servizio il Titolare e Collaboratori utilizzano device mobili personali per lo scambio di emails.

I file cartacei sono custoditi in Italia presso la sede del Titolare in armadi accessibili solo con chiave.

Tutte le pratiche dei Clienti contenute nel gestionale ripropongono la copia esatta di quanto contenuto nel file cartaceo relativo alla pratica e viceversa con la sola eccezione dei documenti in formato originale.

Tutti i dati digitali sono oggetto di doppio back-up in loco

Valutazione : Accettabile

Principi Fondamentali

Proporzionalità, necessità

Gli scopi del trattamento sono specifici, espliciti e legittimi?

Si lo Studio tratta solo i dati necessari, minimi e proporzionali allo svolgimento del Servizio erogati al cliente sulla base giuridica indicata ed in materia esplicita precisando al cliente come vengono trattati i suoi dati informandolo in occasione della sottoscrizione del conferimento di incarico.

Lo Studio tratta inoltre sulla base della normativa vigente i dati dei propri dipendenti, ecc. limitatamente ai dati anagrafici e bancari necessari per le comunicazioni ed i pagamenti.

Nell'ambito dei soggetti di cui sopra lo Studio tratta in particolare i seguenti Dati:

- dati anagrafici;
- documenti d'identità;
- residenza abitazione;
- dati bancari relativi alle domiciliazioni bancarie;
- indirizzi email per le comunicazioni relative all'erogazione del servizio;
- ogni altro dato connesso alla difesa o all'assistenza richiesta oggetto del Servizio con particolare riguardo alla possibilità di trattare Dati sensibili ipotesi contemplata dall' articolo 9 GDPR.

Valutazione : Accettabile

Quali sono le basi legali che rendono il trattamento legittimo?

La base giuridica del trattamento è:

1. per i Servizi di natura consulenziale che non hanno per oggetto una difesa in giudizio: contratto d'opera professione ex art 2229 e seguenti Codice Civile;
2. per i collaboratori a partita IVA rapporto d'opera professionale;
3. per i dipendenti contratto di lavoro subordinato ai sensi dell'articolo 2096 e segg del codice civile e del contratto collettivo nazionale applicabile.

Valutazione : Accettabile

I dati raccolti sono adeguati, rilevanti e limitati a quanto è necessario in relazione alle finalità per cui sono stati trattati (minimizzazione dei dati)?

I Dati raccolti e trattati dal Titolare sono solo ed esclusivamente quelli minimi necessari ad erogare correttamente il Servizio richiesto e non comportano mai la necessità di trattare altri dati.

Il Titolare non utilizza i Dati per scopi di profilazione, né per altri scopi di marketing o di ricerche di mercato.

I Dati sono raccolti mediante, registrazione, organizzazione, conservazione, consultazione, elaborazione, modificazione, selezione, estrazione, raffronto, utilizzo, comunicazione, cancellazione, e quando necessario o richiesto distruzione dei dati.

I Dati personali sono sottoposti a trattamento sia cartaceo che elettronico.

Valutazione : Accettabile

I dati sono accurati e mantenuti aggiornati?

Il Titolare provvede ad ogni utilizzo (ad esempio per i clienti in occasione dell'emissione ed invio della fattura) a verificare la correttezza dei dati ed a aggiornarli ove necessario.

Valutazione : Accettabile

Quale è la durata della conservazione dei dati?

Tutti i dati trattati sono accessibili solo dal Titolare ed Incaricati e non sono accessibili pubblicamente.

I Dati archiviati per obbligo di legge rimarranno in capo al Titolare per i seguenti periodi:

- Clienti: decennale per legge dalla cessazione del Servizio per quanto riguarda gli aspetti fiscali e contrattuali imposti dalla legge per la conservazione al Titolare del Trattamento anche ai fini della normativa Antiriciclaggio ;
- Dipendenti e collaboratori: decennale limitatamente agli aspetti fiscali e contributivi.

Valutazione : Accettabile

Controlli per proteggere i diritti personali dei soggetti interessati

I soggetti interessati come sono informati del trattamento?

Il Titolare garantisce ed informa i clienti ed evita di raccogliere dati a loro insaputa. Lo Studio in particolare informa i Clienti//Dipendenti mediante informativa scritta inviata per posta elettronica/ordinaria.

L'informativa aggiornata è anche contenuta nel sito internet del Titolare e nel Contratto di Conferimento di Incarico per gli utenti allacciati alla centrale.

Valutazione : Non provabile

Piano d'azione / azioni correttive : Informare i Clienti con l'invio di una nuova informativa adeguata al GDPR ed inserirla nel sito internet

Come si ottiene il consenso dei soggetti interessati?

Il trattamento è strettamente connesso al Servizio richiesto e non è richiesto il preventivo consenso in quanto si rientra nell'ambito di quanto previsto dall'articolo 6 primo comma lettera b del Regolamento Europeo Privacy (GRDP).

In ogni caso lo Studio per ogni cautela raccoglie ed informa il Cliente relativamente agli adempimenti Privacy in occasioni della sottoscrizione del conferimento di incarico.

Valutazione : Accettabile

I soggetti interessati come esercitano i loro diritti di accesso alla portabilità dei dati?

Comunicandone la necessità nei termini indicati nell'informativa a loro inviata

Valutazione : Accettabile

Come i soggetti interessati esercitano i loro diritti alla rettifica e alla cancellazione?

Comunicandone la necessità al Titolare e/o al Responsabile nei termini indicati nell'informativa. Il Titolare adotta il processo di cancellazione dei dati fatte salve le norme imperative che impongono al Titolare la conservazione dei dati per le Autorità Competenti

Valutazione : Accettabile

i soggetti interessati come esercitano il loro diritto di restrizione e obiezione?

Comunicandone la necessità al Titolare nei termini indicati nell'informativa. Il Titolare adotta il processo di cancellazione dei dati fatte salve le norme imperative che impongono al Titolare la conservazione dei dati per le Autorità Competenti

Valutazione : Accettabile

Gli obblighi dei responsabili del trattamento sono chiaramente identificati e governati da un contratto?

Al momento considerate le dimensioni numeriche lo Studio non ha nominato un Responsabile

Valutazione : Accettabile

Nel caso di trasferimento di dati fuori dall'Unione Europea, i dati sono adeguatamente protetti?

I dati sono archiviati in server e computer situati in Italia nella sede di Lainate dotati di, Antivirus, Password di accesso e su supporto cartaceo in archivi accessibili solo con chiave.

Valutazione : Accettabile

Rischi

Controlli esistenti o pianificati

Accesso PC Server e Client PC

L'accesso diurno al locale dove sono contenuti i server è consentito soltanto a chi è munito di apposita chiave.

Archivi elettronici accessibili solamente attraverso credenziali di accesso assegnate al personale autorizzato.

Sono presenti delle cartelle condivise dell'organizzazione alle quali hanno accesso solo il personale incaricato.

Valutazione : Non provabile

Piano d'azione / azioni correttive :

1. Valutare l'installazione di un antifurto perimetrale

Back -Up

L'integrità dei dati viene assicurata dall'adozione di programmi antivirus, ad aggiornamento automatico.

La sicurezza del trattamento dei dati effettuato attraverso strumenti elettronici è legata all'utilizzo di apparecchiature tecnologicamente sicure. Il sistema operativo in uso sui due server è "Windows server 2018", mentre i client utilizzano "Windows 7 professional".

I dati sono memorizzati localmente su file e database sui server. I computer sono collegati in una rete locale con accesso ad internet. Sono in uso strumenti per proteggere i dati personali da rischio di intrusione: come sistema antivirus è mentre l'accesso internet è filtrato tramite firewall e content filtering proxy.

Giornalmente viene effettuata procedura di Back-up dei file e dello stato del sistema operativo dei server su hard disk esterno locato

Valutazione : Non provabile

Piano d'azione / azioni correttive :

1. Valutare l'installazione di un antifurto perimetrale

Controllo degli accessi

Con Password (implementare)

Valutazione : Non provabile

Piano d'azione / azioni correttive :

1. Valutare l'installazione di un antifurto perimetrale

Lotta contro il malware

I server e tutti i PC sono dotati di Antivirus e Firewall

Valutazione : Non provabile

Piano d'azione / azioni correttive :

1. Valutare l'installazione di un antifurto perimetrale

Manutenzione

Non Esiste un Contratto di Manutenzione con Amministratore di Rete

Valutazione : Non provabile

Piano d'azione / azioni correttive :

1. Valutare l'installazione di un antifurto perimetrale

Archiviazione

I dati sono archiviati per cliente/pratica su gestionale installato con regolare licenza su PC server e PC Clients dotati di, Antivirus e Password di accesso nonchè supporto file cartaceo che ripropone, in cartaceo, tutti i file contenuti sul supporto digitale.

Lo Studio utilizza per il trattamento dei Dati applicativi gestionali per la comunicazione all'Amministrazione Finanziaria Entratel, Client di Posta Elettronica, Banche Dati di Accesso al Catasto, Conservatoria, Registro Imprese, di seguito anche gli "**Applicativi**".

Ogni PC dello Studio è in rete con regolare licenza installata gestita da amministratore di rete. L'accesso ad ogni PC avviene mediante digitazione di password di almeno 8 caratteri.

Ulteriormente l'accesso agli Applicativi sopra indicati avviene con password.

Nello svolgimento del Servizio il Titolare e Collaboratori utilizzano device mobili personali per lo scambio di emails.

I file cartacei sono custoditi in Italia presso la sede del Titolare in armadi accessibili solo con chiave.

Tutte le pratiche dei Clienti contenute nel gestionale ripropongono la copia esatta di quanto contenuto nel file cartaceo relativo alla pratica e viceversa con la sola eccezione dei documenti in formato originale.

Tutti i dati digitali sono oggetto di doppio back-up in loco

Valutazione : Non provabile

Piano d'azione / azioni correttive :

1. Valutare l'installazione di un antifurto perimetrale

Sicurezza dei documenti cartacei

I Dati cartacei sono archiviati in uffici accessibili solo da personale munito di chiavi di accesso

Valutazione : Non provabile

Piano d'azione / azioni correttive :

1. Valutare l'installazione di un antifurto perimetrale

Accesso illegittimo ai dati

Quale potrebbe essere l'impatto sui soggetti interessati se il rischio si dovesse realizzare?

medio, alto

Quali sono le principali minacce che potrebbero concretizzare il rischio?

bassa protezione del firewall e delle password di accesso ai client, furto

Quali sono le fonti di rischio?

furto, un utente malintenzionato che si rivolge a una delle società incaricata del trattamento utilizzando la sua conoscenza delle società che potrebbero consentire di attaccare la propria immagine

Quali dei controlli identificati contribuiscono a gestire il rischio?

Back -Up, Accesso PC Server e Client PC, Controllo degli accessi, Lotta contro il malware, Manutenzione

Come stimeresti la gravità del rischio, specialmente riguardo i potenziali impatti e i controlli pianificati?

Importante, Considerate le misure adottate dal Titolare il rischio si giudica limitato si suggerisce di tenere monitorato con l'amministratore di rete il servizio di back-up e di valutare l'installazione di un antifurto perimetrale in ufficio

Come stimeresti la probabilità del rischio, specialmente riguardo le minacce, fonti di rischio e i controlli pianificati?

Importante, Considerate le misure adottate dal Titolare il rischio si giudica limitato si suggerisce di tenere monitorato con l'amministratore di rete il servizio di back-up e di valutare l'installazione di un antifurto perimetrale in ufficio

Valutazione : Accettabile

Modifiche indesiderate dei dati

Quali impatti ci sarebbero sui soggetti interessati se il rischio si dovesse concretizzare?

medio

Quali sono le principali minacce che possono portare al rischio?

erroneo inserimento, cancellazione errata

Quali sono le fonti di rischio?

Fonte Umana Interna, Fonte Umana Esterna, interruzione di corrente, danno

Quali dei controlli identificati contribuiscono a gestire il rischio?

Accesso PC Server e Client PC, Back -Up, Lotta contro il malware

Come stimeresti la gravità del rischio, in particolare riguardo l'impatto potenziale e i controlli pianificati?

Importante, Considerate le misure adottate dal Titolare il rischio si giudica limitato

Come stimeresti la probabilità del rischio, specialmente riguardo minacce, fonti di rischio e controlli pianificati?

Importante, Considerate le misure adottate dal Titolare la probabilità che il rischio accada si giudica limitato

Valutazione : Accettabile

Scomparsa di dati

Quale potrebbe essere l'impatto sui soggetti interessati se il rischio dovesse realizzarsi?

medio, alto

Quali sono le minacce che potrebbero portare al rischio?

furto, danneggiamento, cancellazione errata, interruzione elettrica

Quali sono le fonti di rischio?

assenza di back-up, errore umano, furto, mancanza di password, autorizzazione errata

Quali dei controlli identificati contribuisce a gestire il rischio?

Back -Up, Controllo degli accessi, Accesso PC Server e Client PC, Lotta contro il malware, Manutenzione

Come stimeresti la gravità del rischio, specialmente riguardo il potenziale impatto e i controlli pianificati?

Importante, Considerate le misure adottate dal Titolare il rischio si giudica limitato si suggerisce di tenere monitorato con l'amministratore di rete il servizio di back-up e di valutare l'installazione di un antifurto perimetrale in ufficio

Come stimeresti la probabilità del rischio, specialmente rispetto le minacce, fonti di rischio e i controlli pianificati?

Importante, Considerate le misure adottate dal Titolare il rischio si giudica limitato si suggerisce di tenere monitorato con l'amministratore di rete il servizio di back-up e di valutare l'installazione di un antifurto perimetrale in ufficio

Valutazione : Accettabile

Piano d'azione

Principi fondamentali

Informazioni per i soggetti interessati

Informare i Clienti con l'invio di una nuova informativa adeguata al GDPR ed inserirla nel sito internet

Data prevista di implementazione

Controlli esistenti o pianificati

Accesso PC Server e Client PC

1. impostare procedura di modifica password di Default Policy ogni 6 mesi;
2. Impostare procedura di salvataggio delle password di accesso di ogni utente non su carta custodita in studio senza chiave su file protetti e crittografati sui device mobili personali e accessibili con rilievo dell'impronta digitale.
3. valutare di installare nello Studio antifurto perimetrale.

Data prevista di implementazione

Back -Up

1. verificare la Procedura di back-up;
2. implementare la Policy di Back-Up con servizio remoto incrementale.

Data prevista di implementazione

Controllo degli accessi

1. Valutare procedure di doppia autenticazione;
2. implementare policy di modifica password

Data prevista di implementazione

Lotta contro il malware

1. Installare o attivare Firewall sul server

Data prevista di implementazione

Manutenzione

1. Valutare la sottoscrizione di un contratto di amministrazione di rete

Data prevista di implementazione

Archiviazione

1. verificare la Procedura di back-up;
2. implementare la Policy di Back-Up con servizio remoto incrementale.
3. procedere con modifica della password automatica ogni sei mesi.
4. valutare doppia autenticazione.

Data prevista di implementazione

Sicurezza dei documenti cartacei

1. Valutare l'installazione di un antifurto perimetrale

Data prevista di implementazione

Rischi

Nessun piano d'azione registrato.

Potential impacts

medio

alto

Threat

bassa protezione del firewa...

furto

erroneo inserimento

cancellazione errata

danneggiamento

interruzione elettrica

Sources

furto

un utente malintenzionato ch...

Fonte Umana Interna

Fonte Umana Esterna

interruzione di corrente

danno

assenza di back-up

errore umano

mancanza di password

autorizzazione errata

Measures

Back -Up

Accesso PC Server e Client...

Controllo degli accessi

Lotta contro il malware

Manutenzione

Accesso illegittimo ai dati

Severity : **Importante**

Likelihood : **Importante**

Modifiche indesiderate dei dati

Severity : **Importante**

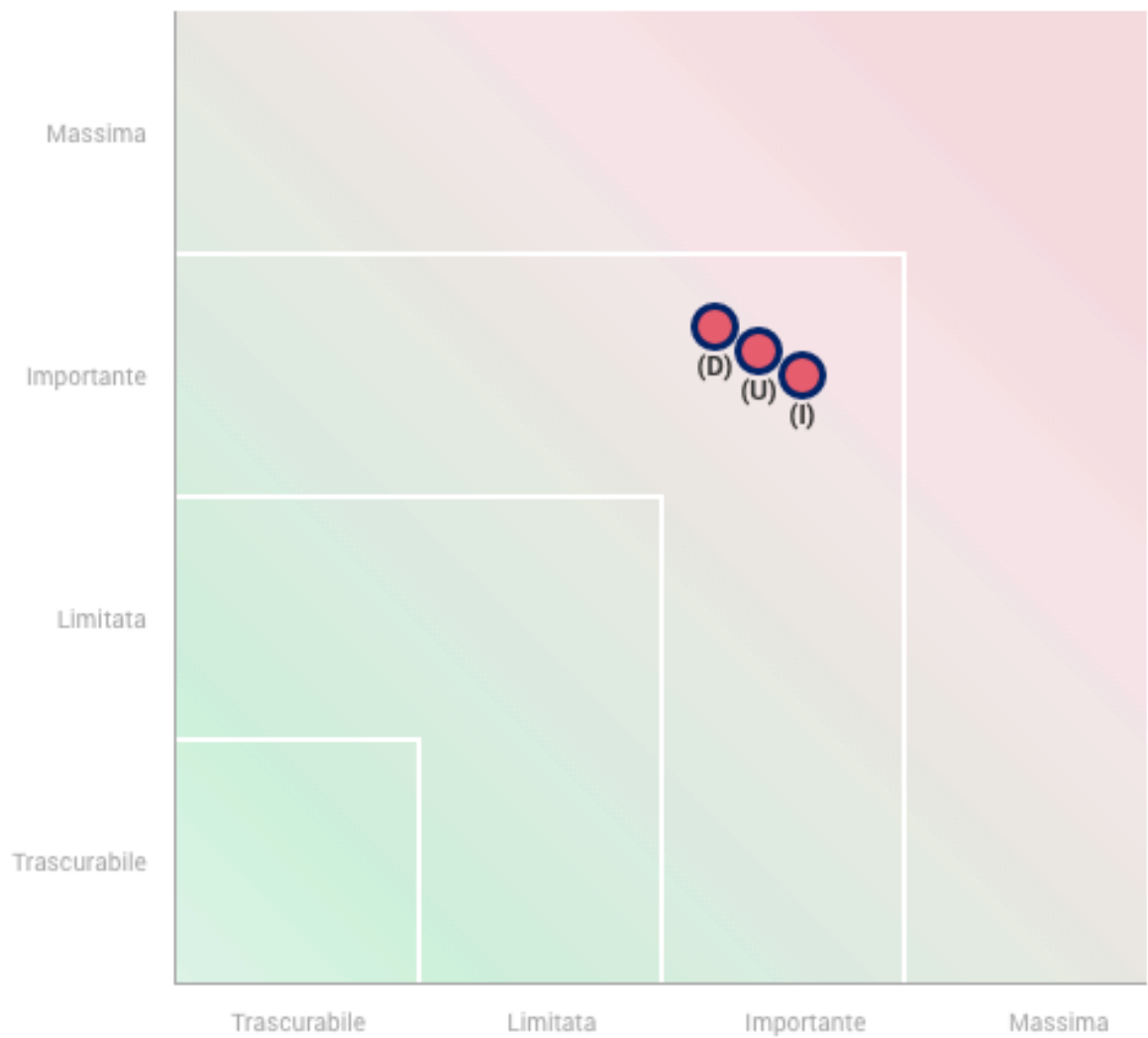
Likelihood : **Importante**

Scomparsa di dati

Severity : **Importante**

Likelihood : **Importante**

Serietà del rischio



- **Misure pianificate o esistenti**
- **Misure correttive implementate**
- **Accesso ai dati illegittimo**
- **Modifiche dei dati non volute**
- **Dati scomparsi**

Panoramica




Principi fondamentali

Finalità	
Basi legali	
Dati adeguati	
Accuratezza dei dati	
Durata dell'archiviazione	
Informazioni per i soggetti interessati	
Ottenere il consenso	
Informazioni per i soggetti interessati	
Diritto di rettifica e cancellazione	
Diritto di restrizione e obiezione	
Subappalto	
Trasferimenti	

Controlli pianificati o esistenti

	Accesso PC Server e Client PC
	Back-Up
	Controllo degli accessi
	Lotta contro il malware
	Manutenzione
	Archiviazione
	Sicurezza dei documenti cartacei

Rischi

	Accesso illegittimo ai dati
	Modifiche dei dati non volute
	Dati scomparsi

Controlli Migliorabili

Controlli Accettabili