Studio di Consulenza Tributaria e Societaria
Sede Legale: Milano (MI) Viale Majno 10, 20129

POLITICHE DI PROTEZIONE DATI E CODICE DI CONDOTTA

Redatto ai fini del rispetto delle norme vigenti in materia di trattamento e protezione dei dati personali (Regolamento CE 679/2016 - Artt. 24 e 25)

CODICE	EDIZIONE	DATA DI EMISSIONE
PPD-CC	01	24/05/2018

REDATTO DA	APPROVATO DAL TITOLARE DEL TRATTAMENTO
	AZIENDA LEG RAPP Direzione Generale

INDICE

1. SCOPO E CAMPO DI APPLICAZIONE 2
2. DEFINIZIONI 5
3. CONTESTO E PARTI INTERESSATE 7
4. ELENCO DEI TRATTAMENTI DEI DATI PERSONALI 8
4.1 Tipologie di dati trattati 8
4.2 Caratteristiche di aree, locali e strumenti con cui si effettuano i trattamenti 9
4.3 La mappa dei trattamenti effettuati 9
4.4 Finalità del trattamento 10
5. REGISTRO DELLE ATTIVITÀ DI TRATTAMENTO 11
6. MANSIONARIO DATA PROTECTION ED INTERVENTI FORMATIVI DEGLI INCARICATI 11
6.1 Figure individuate 12
7. VALUTAZIONE DI IMPATTO E ANALISI DEI RISCHI CHE INCOMBONO SUI DATI 16
8. MISURE ATTE A GARANTIRE L'INTEGRITÀ E LA DISPONIBILITÀ DEI DATI 22
8.1 La protezione di aree e locali 22
8.2 La custodia e l'archiviazione di atti, documenti e supporti cartacei 22
8.3 Pseudonimizzazione 23
8.4 Le misure logiche di sicurezza 23
9. CONTROLLO GENERALE SULLO STATO DELLA SICUREZZA E ATTIVITÀ DI SELF AUDIT 26
10. ANALISI DEL TITOLARE DEL TRATTAMENTO E PIANO DI MIGLIORAMENTO 27

1. SCOPO E CAMPO DI APPLICAZIONE

Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il Titolare del Trattamento, in stretta collaborazione con il Responsabile del trattamento nominato, ha definito di individuare, mettere in atto, riesaminare e aggiornare quando necessario le misure tecniche e organizzative riportate all'interno del presente documento per garantire, ed essere in grado di dimostrare, che il trattamento dei dati personali è effettuato conformemente al Regolamento CE 679/2016 (nel seguito del documento anche Regolamento o CE 679/2016).

Il presente documento redatto sotto la responsabilità della Direzione Generale di **Studio di Consulenza Tributaria e Societaria** si applica a tutta la sede e a tutte le unità operative ed è diretto a tutte le persone che lavorano in o per **Studio di Consulenza Tributaria e Societaria** e agli eventuali collaboratori esterni che in qualsiasi maniera possano avere accesso ai dati, in relazione anche alle attività di competenza di cui al successivo Cap. 3.

Obiettivi del presente documento risultano dunque:

- Illustrare le misure di sicurezza organizzative, fisiche e logiche che **STUDIO DI CONSULENZA TRIBUTARIA E SOCIETARIA (nel seguito del documento anche Titolare del Trattamento o Titolare)** attua al fine di garantire che il trattamento dei dati personali e di categorie particolari degli stessi (di cui all'Art. 9 CE 679/2016) si svolga in maniera lecita, nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali (cfr. Artt. 5, 6, 7 e 9 CE 679/2016)
- Definire sotto il profilo normativo gli obblighi che il Titolare deve adempiere in merito all'adozione delle misure minime di sicurezza
- Tutelare gli interessi dei soggetti privati e pubblici che fanno affidamento sui trattamenti svolti dal Titolare
- Evitare eventi pregiudizievoli che possano danneggiare disponibilità, riservatezza e integrità del patrimonio dei dati della struttura aziendale
- Potenziare la consapevolezza dei rischi e delle insidie che possono coinvolgere la gestione e l'utilizzo dei sistemi informativi automatizzati ed anche l'archivio cartaceo
- Definire le migliori soluzioni tecniche e/o organizzative al fine di prevenire situazioni di pericolo
- Individuare le misure di sicurezza e le procedure per ridurre al minimo:
  - la distruzione o la perdita dei dati
  - la modifica o la divulgazione non autorizzata
  - l'accesso non autorizzato ai dati trattati
  - il trattamento non consentito o non conforme dei dati stessi

Tali misure devono essere adeguate per garantire un livello di sicurezza adeguato al rischio e, ai sensi dell'Art. 3 CE 679/2016 in generale comprendono:

- la pseudonimizzazione e la cifratura dei dati personali
- la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento
- la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico
- la presenza di una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento
- l'autorizzazione al trattamento dati alle risorse interne ed esterne, ovvero formazione e costante aggiornamento delle stesse

Tutte le persone che hanno accesso ai dati, sia attraverso il sistema di computer abilitato, o tramite qualsiasi altro sistema di accesso, siano essi dipendenti della società e/o come persone esterne, sono tenuti per Legge a rispettare le disposizioni del presente documento e saranno soggetti alle conseguenze che potrebbero incorrere in caso di inadempimento.

Una copia di questo documento in formato .pdf, è disponibile a tutto il personale in una cartella che si trova al seguente indirizzo della rete informatica: **www.studiocts.net.**

La logica di approccio alla stesura e all'aggiornamento del presente documento è quella di individuare le best practice per la gestione integrale dei dati sulla base dei 3 seguenti concetti (ai sensi anche dell'Art. 25 del Regolamento CE 679/2016):

➔ **DATA PROTECTION BY DESIGN**

Intesa come modo di operare di default all'interno della nostra Organizzazione. I principi della DATA PROTECTION by Design sono applicati a tutti i tipi di informazioni personali, con particolare vigore ai dati sensibili, e si riassumo in:

- Proattività non reattività (prevenire non correggere): anticipare e prevenire gli eventi invasivi della DATA PROTECTION prima che essi accadano
- DATA PROTECTION come impostazione di default: realizzare il massimo livello di DATA PROTECTION assicurando che i dati siano automaticamente protetti in un qualunque sistema
- DATA PROTECTION incorporata nella progettazione: componente essenziale per la realizzazione del nucleo funzionale del nostro sistema di trattamento e protezione dei dati
- Massima funzionalità: conciliare tutti gli interessi legittimi e gli obiettivi comuni con modalità di valore positivo "vantaggioso per tutti"
- Sicurezza: estensione del sistema per l'intero ciclo vitale dei dati per assicurare che tutti i dati siano conservati con cura e poi distrutti in modo sicuro alla fine del processo
- Visibilità e trasparenza: informazioni ed obiettivi stabiliti, soggetti a verifica indipendente
- Rispetto per la DATA PROTECTION dell'utente: considerare prioritari gli interessi degli individui offrendo efficaci interventi di default della DATA PROTECTION, informazioni appropriate e potenziando opzioni di facile utilizzo per l'utente

➔ **DATA PROTECTION BY DEFAULT**

Intesa come messa in pratica di meccanismi per garantire che siano trattati, di default, solo i dati necessari per ciascuna finalità specifica del trattamento e che, in particolare, la quantità dei dati raccolti e la durata della loro conservazione non vadano oltre il minimo necessario per le finalità perseguite. In particolare detti meccanismi garantiscono che, di default, non siano resi accessibili dati a un numero indefinito di persone

➔ **DATA SECURITY**

Inteso come sicurezza dei dati, livello di protezione, ad esempio, da forze "distruttive" e dalle azioni indesiderate di utenti non autorizzati

Nella stesura del documento, il Titolare e il Responsabile hanno concepito i protocolli operativi e gestionali di riferimento per garantire le corrette metodologie di trattamento e protezione dei dati, apporvando in tal senso il Codice di condotta che tutto il personale (interno ed esterno) che collabora con **STUDIO DI CONSULENZA TRIBUTARIA E SOCIETARIA.** è tenuto a rispettare. In particolare, il nostro Coidce di condotta rappresenta il vero e proprio Sistema di Gestione della Protezione dei Dati (di seguito anche SGPD) che interpreta la corretta applicazione del Regolamento CE 679/2016.

Oltre che a essere una linua guida progettuale ed operativa, il presente documento deve essere utilizzato costantemente per il miglioramento continuo della gestione della protezione dei dati e per la limitazione del rischio sanzionatorio. A questo fine, i contenuti sono stati comunicati a tutto il personale attraverso attività di formazione programmata. Il PPD/CC è disponibile presso il Titolare e il Responsabile in originale.

Chiunque ha la possibilità di consultarlo nel caso di necessità e/o di richiederne copia conforme all'originale. Tale documento viene presentato in fase di inserimento nella struttura organizzativa dallo stesso Responsabile, o da persona incaricata, all'eventuale neoassunto. Ogni aggiornamento del presente documento viene comunicato attraverso sessioni informative e formative a tutte le risorse che collaborano con la nostra Organizzazione.

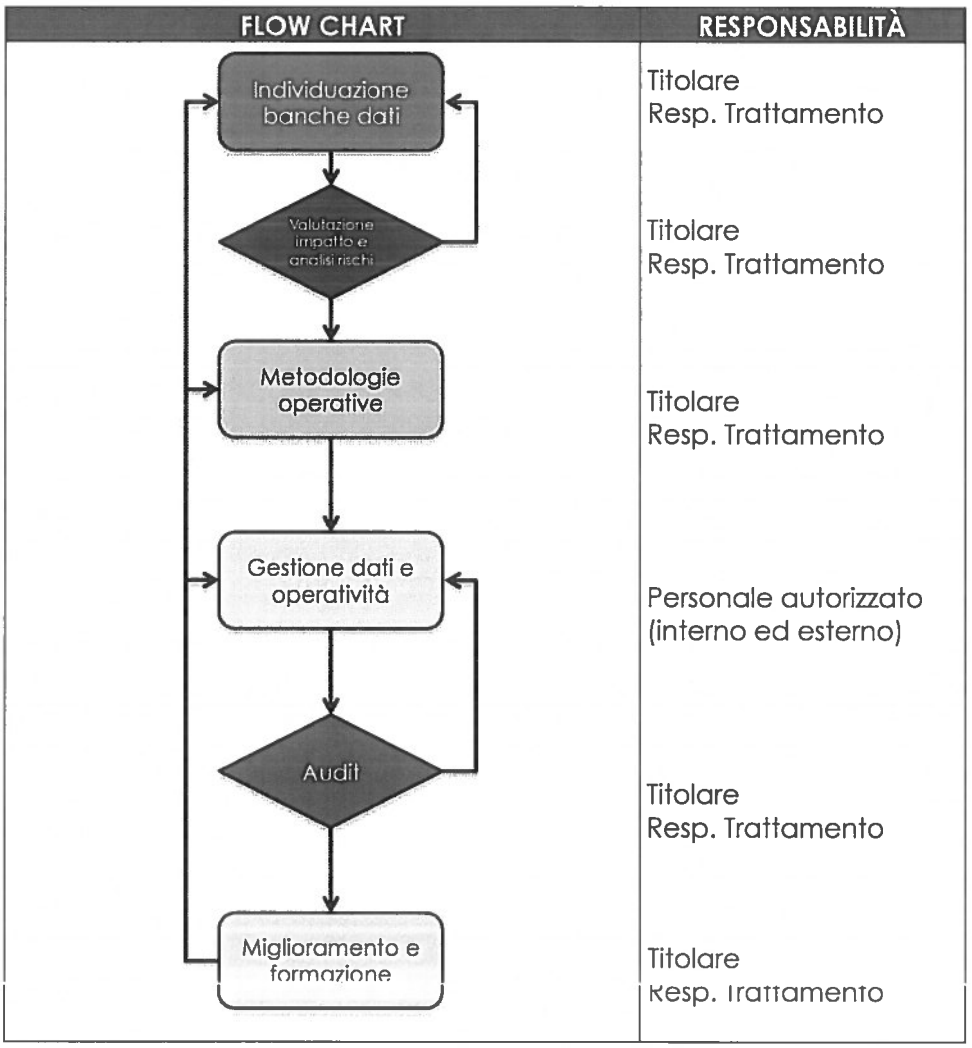
L'applicazione delle misure di sicurezza adottate è verificata giornalmente durante l'esecuzione delle attività lavorative ed in occasione delle ispezioni periodiche previste a cura dello stesso Titolare, o da persona incaricata, come specificato al successivo Cap. 8.

I principi applicabili al trattamento dei dati personali per quanto di competenza della nostra Organizzazione, ai sensi anche dell'Art. 5 CE 679/2016, sono:

- **LICEITÀ, CORRETTEZZA E TRASPARENZA:** i dati personali devono essere trattati in modo lecito, corretto e trasparente nei confronti dell'interessato
- **LIMITAZIONE DELLA FINALITÀ:** i dati personali devono essere raccolti per finalità determinate, esplicite e legittime e successivamente trattati in modo che non sia incompatibile con tali finalità
- **MINIMIZZAZIONE DEI DATI:** i dati personali devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati
- **ESATTEZZA:** i dati personali devono essere esatti e, se necessario, aggiornati. Devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati
- **LIMITAZIONE DELLA CONSERVAZIONE:** i dati personali devono essere conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati
- **INTEGRITÀ E RISERVATEZZA:** i dati personali devono essere trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali

FLUSSO LOGICO DELLE ATTIVITÀ

L'insieme delle attività svolte per la redazione del presente PPD/CC e per garantirne il continuo aggiornamento, così come richiesto dalla normativa vigente, si riassume nel seguente Flow Chart:



Il presente PPD/CC si basa sulla metodologia del PDCA (Plan - Do - Check - Act, ovvero pianificare, attuare, verificare, agire). In particolare:

- PLAN: stabilire target e sequenze di attività per fornire risultati conformi alla politica per la protezione dei dati definita dal Titolare
- DO: attuare le attività per la protezione dei dati
- CHECK: controllare le attività per la protezione dei dati rispetto alla politica, ai target e ai requisiti cogenti
- ACT: messa in azione del progresso continuo del SGPD

Il dettaglio delle fasi è riportato nei Capitoli successivi.

2. DEFINIZIONI

Archivio: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico.

Antivirus: software che individua i virus presenti sui files del computer che si preoccupa di segnalare ed eliminare tali infezioni dal computer stesso.

Autenticazione informatica: l'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità dell'utente.

Audit: processo sistematico, indipendente e documentato per ottenere le evidenze dell'audit (registrazioni, dichiarazioni di fatti o altre informazioni) e valutarle con obiettività, al fine di stabilire in quale misura i criteri dell'audit (insieme di politiche, procedure o requisiti come riferimento) sono stati soddisfatti (fonte: ISO 19011:2012).

Auditor: persona che conduce un audit (fonte: ISO 19011:2012).

Autorità di controllo: l'autorità pubblica indipendente istituita da uno Stato membro.

Autorità di controllo interessata: un'autorità di controllo interessata dal trattamento di dati personali in quanto:

- il titolare del trattamento o il responsabile del trattamento è stabilito sul territorio dello Stato membro di tale autorità di controllo
- gli interessati che risiedono nello Stato membro dell'autorità di controllo sono o sono probabilmente
- influenzati in modo sostanziale dal trattamento; oppure
- un reclamo è stato proposto a tale autorità di controllo

Blocco: la conservazione di dati personali con sospensione temporanea di ogni altra operazione del trattamento.

Banca dati (database): qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti.

Comunicazione: il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del Titolare nel territorio dello Stato o dal Responsabile, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

Comunicazione elettronica: ogni informazione scambiata o trasmessa tra un numero finito di soggetti tramite un servizio di comunicazione elettronica accessibile al pubblico.

Consenso dell'interessato: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento.

Dati biometrici: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici (dati sensibili).

Dati genetici: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione (dati sensibili).

Dato personale: qualsiasi informazione riguardante una persona fisica identificata o identificabile ("interessato"). Si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.

Dati relativi alla salute: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute (dati sensibili).

Dato sensibile (Art. 9 - Categorie particolari di dati personali): qualsiasi informazione riguardante una persona fisica identificata o identificabile ("interessato") idonea a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale ed eventuali altri Diritti fondamentali garantiti dalla costituzione Europea.

Destinatario: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi.

Diffusione: il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

Documento cogente di riferimento: Regolamento CE 679/2016 del Parlamento Europeo e del Consiglio del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati) - Gazzetta ufficiale dell'Unione europea - 4 maggio 2016

Hardware: sono i componenti fisici, meccanici e elettronici che compongono una macchina calcolatrice (per esempio scheda madre, hard disk, processore, cd-rom ecc).

Interessato: la persona fisica cui si riferiscono i dati personali.

Limitazione di trattamento: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro.

Persone autorizzate: le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dai responsabili.

Profilazione: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica.

Pseudonimizzazione: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile.

Rappresentante: la persona fisica o giuridica stabilita nell'Unione che, designata dal titolare del trattamento o dal responsabile del trattamento per iscritto, li rappresenta per quanto riguarda gli obblighi rispettivi a norma del documento cogente di riferimento.

Responsabile della protezione dei dati - Data Protection Officer (DPO): la persona fisica designata dal titolare del trattamento e dal responsabile del trattamento incaricata di informare e fornire consulenza al titolare ed al responsabile, nonché ai dipendenti dell'entità, sorvegliare l'osservanza della normativa cogente e del codice di condotta in ambito protezione dati personali, fornire pareri sulla valutazione d'impatto, cooperare e fungere da punto di contatto con l'autorità di controllo per tutte le questioni inerenti la protezione dati personali.

Responsabile del trattamento: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento.

Reti di comunicazione elettronica: i sistemi di trasmissione, le apparecchiature di commutazione o di instradamento e altre risorse che consentono di trasmettere segnali via cavo, via radio, a mezzo di fibre ottiche o con altri mezzi elettromagnetici, incluse le reti satellitari, le reti terrestri mobili e fisse a commutazione di circuito e a commutazione di pacchetto, compreso internet, le reti utilizzate per la diffusione circolare dei programmi sonori e televisivi, i sistemi per il trasporto della corrente elettrica, nella misura in cui sono utilizzati per trasmettere i segnali, le reti televisive via cavo, indipendentemente dal tipo di informazione trasportato.

Rischio: effetto dell'incertezza che può avere effetti positivi o negativi.

Strumenti elettronici: gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento.

Sistema anti-intrusione: l'insieme di tecnologie informatiche e non atte ad evitare l'ingresso non autorizzato dall'esterno ai locali e ai dati di proprietà della nostra Organizzazione.

Software: sono tutti i sistemi operativi e/o programmi che permettono ad una macchina di funzionare (per esempio Windows, Office, ecc.).

Terzo: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile.

Titolare del trattamento: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri.

Trattamento: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.

User ID: Codice identificativo personale, ovvero chiave di accesso ad un sistema informatico.

Utente: qualsiasi persona fisica che utilizza un servizio di comunicazione elettronica accessibile al pubblico, per motivi privati o commerciali, senza esservi necessariamente abbonata.

Violazione dei dati personali: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

Virus: software che infetta i files del computer inserendo copie di se stesso in tali files.

3. CONTESTO

Lo Studio CTS è caratterizzato da una lunga e consolidata esperienza in diritto tributario e dalla specializzazione principalmente nei settori immobiliare, di servizi, bancario ed assicurativo.

E' composto da dottori commercialisti e revisori contabili che formano una struttura attiva e dinamica, in grado di erogare servizi professionali che hanno come obiettivo principale quello di adattarsi alle esigenze del cliente, fornendo "soluzioni su misura" ed un servizio idoneo e di qualità, volto a soddisfare le molteplici esigenze derivanti dalla crescente complessità del mondo dei rapporti giuridici ed economici.

La struttura è composta come riportato nell'Organigramma allegato al presente documento ***(Allegato 1. Organigramma)***

Per quanto riguarda ruoli e responsabilità, così anche come richiesto dal CE 679/2016, si rimanda al successivo Cap. 4.

FATTORI

I fattori, interni ed esterni, che influenzano i processi relativi al trattamento dei dati sono:

FATTORE	INTERNO / ESTERNO	DESCRIZIONE
INFRASTRUTTURE E AMBIENTE DI LAVORO	Interno	Insieme delle attrezzature informatiche e non utili al trattamento e alla protezione dei dati.
ORGANIZZAZIONE	Interno	Insieme delle attività atte a garantire il rispetto delle mansioni definite e degli obiettivi definiti dal Titolare e dal Responsabile e rivolti al personale.
ASPETTI LEGALI	Interno / Esterno	Insieme delle attività che possono determinare prescrizioni particolari in ambito di trattamento dati, derivanti da tutte quelle organizzazioni che emanano Leggi, Norme e/o Regolamenti in ambito che devono essere rispettati dalla nostra Organizzazione.

MERCATO DI RIFERIMENTO	Esterno	Territorio geografico in cui opera la nostra organizzazione, con riferimento al trattamento dati, ovvero trasferimento dati verso Paesi Terzi ed extra CE

PARTI INTERESSATE

Le parti interessate interne che hanno rilevanza sul nostro SGPD sono:

INTERNE	DESCRIZIONE
SOCI/AZIONISTI	Inteso come la proprietà
DIPENDENTI	Inteso come tutte le risorse umane che concorrono alla realizzazione del servizio offerto e che devono rispettare le prescrizioni del DPMS e quelle previste dalla normativa vigente in ambito di trattamento dati.

ESTERNE	DESCRIZIONE
FORNITORI	Che devono garantire alla nostra Azienda il rispetto dei requisiti contrattuali previsti in termini di conformità dei servizi offerti e soprattutto in termini di conformità del trattamento dei dati. I fornitori coinvolti nel nostro DPMS sono agenti, consulenti e collaboratori in genere.
CLIENTI/PROSPECT	Ai quali dobbiamo garantire sicurezza di trattamento dei dati, soddisfazione e buona resa dei servizi.

In generale, le esigenze e le aspettative delle parti interessate in ambito di trattamento dati rispecchiano le prescrizoni del Regolamento CE 679/2016 al quale il presente documento si rivolge e si adegua.

Dall'analisi del contesto sopra riportata, correlata ai fattori influenzanti interni ed esterni e alle esigenze ed aspettative delle parti interessate, risulta evidente che le misure di sicurezza tecniche e organizzative sono adottate in riferimento ai dati del personale, dei Clienti, dei Fornitori e degli Interessati.

Per quanto concerne la sicurezza dei dati trattati, oltre a predisporre il presente documento, la nostra Organizzazione ha previsto una serie di misure atte a garantire misure di prevenzione dettagliate nell'Allegato 2 al presente documento ***(Allegato 2 - ELENCO DELLE SEDI IN CUI VENGONO TRATTATI I DATI RELATIVE MISURE DI SICUREZZA FISICA)***

4. ELENCO DEI TRATTAMENTI DEI DATI PERSONALI

Al fine di elaborare l'elenco dei trattamenti dei dati, posti in essere dal Titolare, si procede come segue:

- si individuano i tipi di dati trattati, in base alla loro natura (personali, sensibili, biometrici, genetici, relativi alla salute - vedi definizioni al precedente Cap. 2) ed alla categoria di soggetti cui essi si riferiscono (dipendenti/collaboratori, clienti e fornitori)
- si descrivono le aree, i locali e gli strumenti con i quali si effettuano i trattamenti
- si elabora la mappa dei trattamenti effettuati, che si ottiene incrociando le coordinate dei due punti precedenti

4.1 Tipologie di dati trattati

I dati trattati dal Titolare alla data odierna sono identificati nell'Allegato 3 al presente documenti (***Allegato 3. ELENCO DEGLI ARCHIVI DEI DATI OGGETTO DEL TRATTAMENTO***).

Per quanto riguarda l'analisi per singolo archivio, si faccia riferimento a quanto riportato nell'Allegato 3 e nei successivi capitoli.

4.2 Caratteristiche di aree, locali e strumenti con cui si effettuano i trattamenti

Per quanto riguarda la descrizione dei locali all'interno dei quali avviene il trattamento dei dati, si faccia riferimento al precedente Cap. 3, all'Allegato 2 al presente documento ***(Allegato 2 - ELENCO DELLE SEDI IN CUI VENGONO TRATTATI I DATI RELATIVE MISURE DI SICUREZZA FISICA)*** ed al Documento Valutazione Rischi disponibile presso il RSPP.

Il trattamento dei dati avviene utilizzando i seguenti strumenti:

A - SCHEDARI ED ALTRI SUPPORTI CARTACEI

I supporti cartacei, ivi inclusi quelli contenenti dati sensibili, vengono ordinatamente raccolti in schedari, ovvero nella pratica cui si riferiscono, per essere archiviati sotto chiusura a chiave, una volta terminato il ciclo di attività di riferimento. Si veda ***Allegato 3. ELENCO DEGLI ARCHIVI DEI DATI OGGETTO DEL TRATTAMENTO***.

B - ELABORATORI IN RETE

La verifica dell'efficacia e della validità nel tempo delle misure di sicurezza adottate è punto fondamentale di tutto il processo per la sicurezza del Sistema Informativo. Infatti, in un contesto tecnologico in rapidissima evoluzione, è necessario avere le massime garanzie circa l'adeguatezza delle misure di sicurezza adottate nei confronti del sempre più vasto, articolato ed aggiornato panorama delle minacce possibili.

La tipologia della rete è descritta nel documento ***Allegato 4. INFRASTRUTTURE CONTENENTI DATI E RELATIVE MISURE DI SICUREZZA LOGICO-INFORMATICHE*** al presente documento. I dati trattati con tali strumenti elettronici sono gli stessi indicati nell'' ***Allegato 3. ELENCO DEGLI ARCHIVI DEI DATI OGGETTO DEL TRATTAMENTO***. Le misure tecniche ed organizzative per il loro utilizzo sono definite al successivo Cap. 7.

C - ELABORATORI NON IN RETE

Per elaboratori non in rete si intendono quelli non accessibili da altri elaboratori, terminali o, più in generale, da altri strumenti elettronici. Il sistema informativo della nostra Organizzazione

X **NON PREVEDE** □ **PREVEDE**

alla data di redazione del presente PPD/CC la presenza di elaboratori non in rete. Ad ogni modo, nel caso in cui venisse inserito anche solo un elaboratore non in rete, verranno applicate, per tale elaboratore, le misure di sicurezza richieste dalla nomina di Responsabile esterno debitamente emessa dal Titolare del Trattamento.

4.3 La mappa dei trattamenti effettuati

Incrociando le coordinate di cui ai due paragrafi precedenti ed ai relativi allegati citati, si ottiene la mappa dei trattamenti di dati personali effettuati dal Titolare. In relazione al diverso grado di rischio, è opportuno distinguere i trattamenti che vengono posti in essere nelle distinte aree in cui sono dislocati gli strumenti, nei casi in cui la circostanza sia significativa.

Nell'Allegato 3 al presente documento, è stato predisposto un apposito campo (figura 1 a lato) per identificare le modalità di trattamento effettuate, apponendo il simbolo X nella casella di incrocio idicando quindi che determinati tipi di dati sono trattati con determinati strumenti

TIPO DI TRATTAMENTO	ACCESSO CONTROLLATO	ACCESSO NON CONTROLATO
Schedari ed altri supporti cartacei		
Elaboratori di Rete		
Elaboratori non in rete		
Server		

Figura 1 - Mappatura dei trattamenti (Allegato 3)

Da una prima lettura della mappa, si possono apprezzare gli accorgimenti adottati per ridurre i rischi. Infatti, i dati sensibili relativi Dipendenti/Collaboratori (3 e 1) vengono trattati esclusivamente in aree ad accesso controllato, con strumenti cartacei ed elettronici, ivi localizzati e gestiti tramite accessi controllati.

Per tutti i Clienti ed i Fornitori presenti nell'anagrafica è stata effettuata l'informativa per il trattamento dei dati, come richiesto dall'Art. 13 CE 679/2016. Tale informativa viene preventivamente fornita anche ai nuovi Clienti e/o Fornitori che col tempo vengono inseriti in anagrafica.

4.4 Finalità del trattamento

Le finalità del trattamento sono descritte nella tabella di cui all' ***Allegato 3. ELENCO DEGLI ARCHIVI DEI DATI OGGETTO DEL TRATTAMENTO***.

5. REGISTRO DELLE ATTIVITÀ DI TRATTAMENTO

Stante le dimensioni dell'azienda (<250 dipendenti) non è obbligatoria la tenuta dei registri relativi al Titolare e al Responsabile come richiesto dall'Art. 30 CE 679/2016. Il Titolare e il Responsabile hanno predisposto e tengono aggiornati gli allegati al presente documento secondo quanto previsto dal Reg. CE 679/2016.

6. MANSIONARIO DATA PROTECTION ED INTERVENTI FORMATIVI DEGLI INCARICATI

Per il trattamento dei dati personali, il Titolare ha nominato un Responsabile del trattamento e ha definito, per singola Funzione/Processo, una serie di incarichi di ordine organizzativo e direttivo e ha individuato gli incaricati, intesi come persone autorizzate, con compiti esecutivi. Tali figure sono state istruite con opportune procedure operative ed incontri formativi in maniera tale renderle edotte sulle metodologie di trattamento e protezione dei dati.

Essi si impegnano a garantire che tutte le misure di sicurezza riguardanti i dati siano applicate all'interno della nostra Organizzazione ed eventualmente al di fuori, qualora siano cedute a terzi quali Responsabili del Trattamento, tutte o parte delle attività di trattamento, e ad informare il Titolare nella eventualità che si siano rilevati dei rischi. Il trattamento dei dati viene effettuato solo da soggetti che hanno ricevuto un formale incarico, mediante designazione per iscritto da parte del Titolare, con il quale si individua puntualmente l'ambito del trattamento consentito e le mansioni dello stesso incaricato. Oltre alle istruzioni generali, su come devono essere trattati i dati, agli incaricati vengono fornite esplicite istruzioni in merito ai seguenti punti, aventi specifica attinenza con la sicurezza:

- procedure da seguire per la classificazione dei dati, al fine di distinguere quelli sensibili, per garantire la sicurezza dei quali occorrono maggiori cautele, rispetto a quanto è previsto per i dati di natura personale
- modalità di reperimento dei documenti contenenti dati e modalità da osservare per la custodia degli stessi e la loro archiviazione, al termine dello svolgimento del lavoro per il quale è stato necessario utilizzare i documenti
- modalità per elaborare e custodire le password necessarie per accedere agli elaboratori elettronici ed ai dati in essi contenuti
- prescrizione di non lasciare incustoditi e accessibili gli strumenti elettronici mentre è in corso una sessione di lavoro
- procedure e modalità di utilizzo degli strumenti e dei programmi atti a proteggere i sistemi informativi
- procedure per il salvataggio dei dati
- modalità di custodia ed utilizzo dei computer portatili e dei supporti rimovibili contenenti dati
- dovere di aggiornarsi, utilizzando il materiale e gli strumenti forniti dal Titolare e dal Responsabile, sulle misure di sicurezza e sulle procedure generali per il trattamento dei dati

Le lettere ed i contratti di nomina vengono raccolte in base all'organizzazione interna: in tale modo il Titolare dispone di un quadro chiaro di chi fa cosa (*Mansionario DATA PROTECTION*) nell'ambito del trattamento dei dati.

Periodicamente si procede ad aggiornare, se necessario, la definizione dei dati cui le persone sono autorizzate ad accedere e dei trattamenti che sono autorizzate a porre in essere, al fine di verificare la sussistenza delle condizioni che giustificano tali autorizzazioni. La stessa operazione viene compiuta per le autorizzazioni rilasciate ai soggetti incaricati della gestione o manutenzione degli strumenti elettronici e a eventuali Responsabili in outsourcing.

Tutto ciò permette al Titolare di garantire:

- la massima conoscenza e controllo dei processi e degli incaricati del trattamento
- la sussistenza in seno ai Responsabili dei necessari poteri per l'implementazione e verifica delle misure di sicurezza adottate
- la necessaria competenza, esperienza ed affidabilità che deve sussistere nei Responsabili

6.1 Figure individuate

In particolare sono state individuate le seguenti figure:

FIGURA	DESCRIZIONE	NOMINE E DOCUMENTI
Titolare del trattamento	Definito dal Reg. CE 679 all'Art. 4 punto 7 come la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;	Il titolare del trattamento dei dati è **STUDIO DI CONSULENZA TRIBUTARIA E SOCIETARIA,** rappresentata dal suo Legale Rappresentante chè è tenuto ad osservare tutto quanto previsto dal Regolamento in materia di Protezione dei Dati con particolare riferimento all'Art. 24 del regolamento CE 679/2016
Responsabili del trattamento	Definito dal Reg. CE 679 all'Art. 4 punto 8 come la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento. Il Responsabile del Trattamento è tenuto ad osservare tutto quanto previsto dal Regolamento in materia di Protezione dei Dati con particolare riferimento all'Art. 28 del regolamento CE 679/2016 I reponsabili possono essere Interni o Esterni alla società	Il Responsabile del trattamento per **STUDIO DI CONSULENZA TRIBUTARIA E SOCIETARIA** è stato nominato mediante lettera di nomina comprensiva delle relative responsabilità per il trattamento dei dati. Tale nomina, controfirmata per accettazione, è conservata presso il Titolare del Trattamento.
Responsabile della Protezione dei Dati (Data Protection Officer - DPO)	La figura del DPO è obbligatoria solo in determinati casi come disciplinato dall'ART. 37 del Regolamento CE 679/2016. I compiti e le responsabilità del DPO sono esplicitate agli art. 38 e 39 del GDPR.	Nel caso specifico di **STUDIO DI CONSULENZA TRIBUTARIA E SOCIETARIA** non è necessaria la nomina di un DPO (Art. 37 CE 679/16).
Persone autorizzate (interne ed esterne)	Le persone autorizzate, o oincaricati, al trattamento dei dati sono tutte quelle figure, interne o esterne, che hanno accesso ai dati oggetto del trattamento e che, seppur a diversi livelli, possono effettuare operazioni di trattamento dei dati.	Ogni persona autorizzata al trattamento ha ricevuto una lettera riportante compiti e responsabilità. Tali lettere sono state controfirmate per accettazione e sono conservate presso il Titolare del Trattamento.

FIGURA	DESCRIZIONE	NOMINE E DOCUMENTI
Incaricati della gestione e della manutenzione degli strumenti elettronic	L'incaricato della gestione e della manutenzione degli strumenti elettronici è la persona fisica che sovrintende alle risorse del sistema operativo di un elaboratore o di un sistema di Banche di dati. E' compito degli Incaricati della gestione e della manutenzione degli strumenti elettronici: ➢ Attivare per tutti i trattamenti effettuati con strumenti elettronici le Credenziali di autenticazione assegnate agli Incaricati del trattamento. ➢ definire l'attivazione di idonei strumenti per la protezione contro il rischio di intrusione e dell'azione di programmi informatici aventi per scopo o per effetto il danneggiamento di un sistema informatico o telematico, dei dati o dei programmi in esso contenuti o ad esso pertinenti, ovvero l'interruzione, totale o parziale, o l'alterazione del suo funzionamento. Questi strumenti debbono essere aggiornati con cadenza almeno semestrale. ➢ aggiornare periodicamente (almeno una volta l'anno) i programmi per elaboratore per prevenire la vulnerabilità degli strumenti elettronici e correggerne difetti. In caso di trattamento di dati sensibili o giudiziari l'aggiornamento è almeno semestrale. ➢ proteggere, mediante l'utilizzo di idonei strumenti elettronici, i dati sensibili o giudiziari contro l'accesso da parte di chiunque abusivamente si introduce nel sistema informatico o telematico (art. 615-ter del Codice Penale). ➢ Informare il Responsabile della sicurezza dei dati personali nella eventualità che si siano rilevati dei rischi relativamente alle misure di sicurezza riguardanti i dati personali. Qualora il Responsabile della sicurezza dei dati personali ritenga di non nominare alcun Incaricato della gestione e della manutenzione degli strumenti elettronici, ne assumerà tutte le responsabilità e funzioni.	Il Titolare del Trattamento o il Responsabile del Trattamento, nomina uno o più soggetti Incaricati della gestione e della manutenzione degli strumenti elettronici La nomina di uno o più Incaricati della gestione e della manutenzione degli strumenti elettronici deve essere effettuata con una lettera di incarico e deve essere controfirmata per accettazione e copia della lettera di nomina accettata deve essere conservata a cura del Responsabile in luogo sicuro. La nomina dell'Incaricato della gestione e della manutenzione degli strumenti elettronici, benchè possa essere revocata in qualsiasi momento dal Titolare o dal Responsabile, è a tempo indeterminato, e decade per revoca o dimissioni dello stesso.
Incaricato della custodia delle copie delle credenziali	E' compito degli Incaricati della custodia delle copie delle credenziali: ➢ Autorizzare l'assegnazione e la gestione delle Credenziali di autenticazione per l'accesso ai dati personali degli Incaricati del trattamento, su richiesta del Responsabile dello specifico trattamento, avvalendosi del supporto tecnico dell'incaricato della gestione e della manutenzione degli strumenti elettronici. ➢ Istruire gli incaricati del trattamento sull'uso delle componenti riservata delle credenziali di autenticazione, e sulle caratteristiche che debbono avere, e sulle modalità per la loro modifica in autonomia. ➢ Assicurare che il Codice per l'identificazione, laddove sia stato già utilizzato, non sia assegnato ad altri Incaricati del trattamento, neppure in tempi diversi, ➢ Revocare le Credenziali di autenticazione per l'accesso ai dati degli Incaricati del trattamento nel caso di mancato utilizzo per oltre 6 (sei) mesi, ➢ Revocare tutte le Credenziali di autenticazione non utilizzate in caso di perdita della qualità che consentiva all'Incaricato del trattamento l'accesso ai dati personali. ➢ Impartire istruzioni agli Incaricati del trattamento per non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento.	Il Titolare del trattamento (o il responsabile) nomina uno o più soggetti Incaricati della custodia delle copie delle credenziali. La nomina di uno o più Incaricati della custodia delle copie delle credenziali deve essere effettuata con una lettera di incarico, deve essere controfirmata per accettazione e copia della lettera di nomina accettata deve essere conservata a cura del Responsabile della sicurezza dei dati personali in luogo sicuro. La nomina di uno o più Incaricati della custodia delle copie delle credenziali, benchè possa essere revocata dal Responsabile in qualsiasi momento, è a tempo indeterminato, e decade per revoca o dimissioni dello stesso.

FIGURA	DESCRIZIONE	NOMINE E DOCUMENTI
		Qualora il Responsabile ritenga di non nominare alcun Incaricato, ne assumerà tutte le responsabilità e funzioni.
Incaricato delle copie di sicurezza delle banche dati	L'Incaricato delle copie di sicurezza delle banche dati è la persona fisica o la persona giuridica che ha il compito di sovrintendere alla esecuzione periodica delle copie di sicurezza delle Banche di dati personali gestite. Al fine di garantire l'integrità dei dati contro i rischi di distruzione o perdita, il Responsabile stabilisce, con il supporto tecnico dell'Incaricato della gestione e della manutenzione degli strumenti elettronici la periodicità con cui debbono essere effettuate le copie di sicurezza delle Banche di dati trattate. I criteri debbono essere concordati con l'Incaricato della gestione e della manutenzione degli strumenti elettronici in relazione al tipo di rischio potenziale e in base al livello di tecnologia utilizzata. La frequenza con cui debbono essere effettuate le copie dei dati personali non deve superare in nessun caso i 7 (sette) giorni. In particolare per ogni Banca di dati debbono essere definite le seguenti specifiche: ➢ Il "Tipo di supporto" da utilizzare per le "Copie di Back-Up". ➢ Il numero di "Copie di Back-Up" effettuate ogni volta. ➢ Se i supporti utilizzati per le "Copie di Back-Up" sono riutilizzati e in questo caso con quale periodicità. ➢ Se per effettuare le "Copie di Back-Up" si utilizzano procedure automatizzate e programmate. ➢ Le modalità di controllo delle "Copie di Back-Up". ➢ La durata massima stimata di conservazione delle informazioni senza che ci siano perdite o cancellazione di dati. ➢ L'Incaricato del trattamento a cui è stato assegnato il compito di effettuare le "Copie di Back-Up". ➢ Le istruzioni e i comandi necessari per effettuare le "Copie di Back-Up". E' compito degli Incaricati delle copie di sicurezza delle banche dati: ➢ Prendere tutti i provvedimenti necessari ad evitare la perdita o la distruzione dei dati e provvedere al ricovero periodico degli stessi con copie di sicurezza secondo i criteri stabiliti dal Responsabile della sicurezza dei dati personali. ➢ Assicurarsi della qualità delle copie di sicurezza dei dati e della loro conservazione in luogo adatto e sicuro. ➢ Assicurarsi della conservazione delle copie di sicurezza in luogo adatto e sicuro e ad accesso controllato. ➢ Di provvedere a conservare con la massima cura e custodia i dispositivi utilizzati per le copie di sicurezza, impedendo l'accesso agli stessi dispositivi da parte di personale non autorizzato.	Il Responsabile, in relazione all'attività svolta, può individuare, nominare e incaricare per iscritto, se lo ritiene opportuno, uno o più Incaricati delle copie di sicurezza delle banche dati a cui è conferito il compito di effettuare periodicamente le copie di sicurezza delle Banche di dati gestite specificando gli elaboratori o le banche dati che è chiamato a sovrintendere. Il Responsabile deve informare ciascun Incaricato delle copie di sicurezza delle banche dati delle responsabilità che gli sono affidate in conformità a quanto disposto dalle normative in vigore. La nomina di uno o più Incaricati delle copie di sicurezza delle banche dati deve essere effettuata con una lettera di incarico e deve essere controfirmata. Copia della lettera di nomina accettata deve essere conservata a cura del Responsabile della sicurezza dei dati personali in luogo sicuro. Qualora il Responsabile ritenga di non nominare alcun Incaricato della custodia delle copie delle credenziali, ne assumerà tutte le responsabilità e funzioni.

FIGURA	DESCRIZIONE	NOMINE E DOCUMENTI
	➢ Di segnalare tempestivamente all'Incaricato della gestione e della manutenzione degli strumenti elettronici, ogni eventuale problema dovesse verificarsi nella normale attività di copia delle banche dati.	
Incaricato della custodia delle aree e dei locali	Gli Incaricati della custodia delle aree e dei locali debbono: ➢ Consentire l'accesso alle aree e ai locali di cui debbono assicurare il controllo solo agli Incaricati del trattamento autorizzati. ➢ Identificare e registrare le persone ammesse, a qualunque titolo, dopo l'orario di chiusura. ➢ Informare tempestivamente il Responsabile della sicurezza dei dati personali nel caso in cui si siano riscontrate situazioni anomale. ➢ Controllare la chiusura dei locali al termine dell'orario.	Il Responsabile deve informare ciascun Incaricato della custodia delle aree e dei locali delle responsabilità che gli sono affidate in conformità a quanto disposto dalle normative in vigore. La nomina di uno o più Incaricati della custodia delle aree e dei locali deve essere effettuata con una lettera di incarico e deve essere controfirmata. Copia della lettera di nomina accettata deve essere conservata a cura del Responsabile della sicurezza dei dati personali in luogo sicuro. La nomina dell'Incaricato della custodia delle aree e dei locali può essere revocata in qualsiasi momento dal Responsabile della sicurezza dei dati personali che gli ha affidato l'incarico, senza preavviso, ed eventualmente può essere affidata ad altro soggetto. Qualora il Responsabile della sicurezza dei dati personali ritenga di non nominare alcun Incaricato della custodia delle aree e dei locali, ne assumerà tutte le responsabilità e funzioni.

Alla data di redazione del presente documento, la struttura organizzativa della nostra Società, in relazione anche alla gestione e al trattamento dei dati risulta quella riportata nell'***Allegato 1 ORGANIGRAMMA***. Il Titolare ed i Responsabili del Trattamento sia interni che esterni sono riepilogati nell'***Allegato 3 ELENCO DEGLI ARCHIVI DEI DATI OGGETTO DEL TRATTAMENTO***.

A tutte le persone autorizzate al trattamento dei dati per conto del Titolare sono impartite istruzioni scritte finalizzate al controllo, alla gestione ed alla custodia, per l'intero svolgimento delle operazioni di trattamento, dei dati personali e sensibili. Inoltre, agli eventuali soggetti incaricati alla gestione e manutenzione del sistema informativo, siano essi interni o esterni all'organizzazione del Titolare, viene prescritto di non effettuare alcun trattamento sui dati contenuti negli strumenti elettronici, fatta unicamente eccezione per i trattamenti di carattere temporaneo strettamente necessari per effettuare la gestione o manutenzione del sistema.

Per tutti i collaboratori sono previsti interventi formativi, finalizzati ad approfondire i seguenti aspetti:

- profili della disciplina sulla protezione dei dati che appaiono più rilevanti per l'attività svolta e delle conseguenti responsabilità che ne derivano
- rischi che incombono sui dati
- misure organizzative e tecniche disponibili per prevenire eventi dannosi
- modalità per aggiornarsi sulle misure di sicurezza adottate dal Titolare

Tali interventi formativi sono programmati in modo tale, da avere luogo al verificarsi di una delle seguenti circostanze:

- all'inizio della collaborazione
- in occasione di cambiamenti, che implichino modifiche rilevanti rispetto al trattamento dei dati
- in occasione della introduzione di nuovi significativi strumenti, che implichino modifiche rilevanti nel trattamento dei dati
- in occasione di aggiornamenti legislativi

Gli interventi formativi possono avvenire sia all'interno, a cura del Titolare o di altri soggetti esperti nella materia, che all'esterno, presso soggetti specializzati e preventivamente valutati. Per il 2017/2018 è stato individuato un piano di addestramento esplicitato nell'***Allegato 5 PIANO DI FORMAZIONE E ADDESTRAMENTO***.

7. VALUTAZIONE DI IMPATTO E ANALISI DEI RISCHI CHE INCOMBONO SUI DATI

Questa sezione rappresenta il nucleo fondamentale del documento, in quanto sulla base di questa valutazione la nostra Organizzazione ha individuato le specifiche azioni da intraprendere.

La Valutazione di impatto (cosiddetta PIA - Protection Impact Analysis), ai sensi dell'Art. 35 CE 679/2016 è parte integrante del presente documento e i suoi requisiti sono riconducibili ai seguenti Capitoli:

- Descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento: Cap. 4
- Valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità: Cap. 4 e Cap. 6 (Analisi rischi)
- Valutazione dei rischi per i diritti e le libertà degli interessati: Cap. 6 (Analisi rischi)
- Misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al Regolamento CE 679/2016, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione: Cap. 5, Cap. 7 e Cap. 8
- Identificazione del Responsabile del trattamento: Cap. 6

La valutazione dei rischi è effettuata su tutti i processi interni utilizzando il seguente metodo:

RISCHIO = PROBABILITÀ X DANNO

Dalla valutazione dei rischi deriva il carattere di urgenza o di priorità con cui intervenire sul singolo rischio. La probabilità dell'accadimento viene definita mediante la scala seguente:

VALORE	LIVELLO PROBABILITÀ	DEFINIZIONI/CRITERI
1	IMPROBABILE	Il danno può essere provocato solo indirettamente Non sono noti episodi già verificatisi
2	POCO PROBABILE	Il danno può essere provocato solo in circostanze sfortunate Sono noti solo rarissimi episodi già verificatisi Il verificarsi del danno susciterebbe grande sorpresa e incredulità
3	PROBABILE	L'inadempienza rilevata può provocare un danno anche se in modo non automatico e diretto È noto qualche episodio già verificato Il verificarsi del danno susciterebbe sorpresa
4	MOLTO PROBABILE	Esiste correlazione diretta tra inadempienza rilevata e verificarsi del danno Si sono già verificati danni per la stessa inadempienza Il verificarsi del danno non susciterebbe alcuna sorpresa

Per la determinazione del livello di gravità danno si è utilizzata la seguente scala:

VALORE	DANNO	DEFINIZIONI/CRITERI
1	LIEVE	Nessuno o minimi costi per il superamento del danno Completamento solo parziale di registrazioni e/o registrazioni effettuate a posteriori oltre il momento stabilito Nessun/Lieve danno all'immagine aziendale Nessuna/Lieve sanzione
2	MEDIO	Costi per il superamento del danno Azioni contrarie al metodo aziendale e/o alle procedure non deliberatamente attuate Mancata registrazione dei controlli Medio danno all'immagine aziendale Sanzione di carattere medio
3	GRAVE	Elevati costi per il superamento del danno Azioni volutamente contrarie al metodo aziendale e/o alle procedure Non effettuazione di controlli Mancata richiesta di autorizzazioni necessarie Danni all'immagine aziendale Sanzioni di carattere grave
4	GRAVISSIMO	Perdita di un cliente Ingenti costi per il superamento del danno Azioni di sabotaggio al metodo aziendale e/o alle procedure Danni ingenti all'immagine aziendale Reiterata mancanza di effettuazione di controlli Sanzioni gravissime Azioni contro la legge o norme o regolamenti Azioni contro la deontologia professionale

Il prodotto Calcolato (**Rischio = Probabilità x Danno**) definisce il grado di rischio ovvero la "criticità dell'anomalia" e permette di stabilire una gerarchia dei rischi così Classificata:

GRADO DI RISCHIO	VALUTAZIONE RISCHIO	AZIONE CORRISPONDENTE
<2	NON SIGNIFICATIVO	Nessuna azione
2 - 4	BASSO	Le eventuali azioni da programmare sono solo per migliorare una situazione di partenza di per sé non pericolosa significativamente (subito dopo quelle a priorità media se possibile entro l'anno)
5 - 8	MEDIO	Introduzione azioni correttive o migliorative da programmare entro un mese
9 - 16	ALTO	Introduzione azioni correttive da programmare entro una settimana

FATTORI DI RISCHIO

Sono stati individuati i seguenti fattori che possono portare a rischi sul trattamento dei dati:

- Personale: inteso come mancanza di adeguata competenza e/o mancanza di personale
- Infrastrutture: inteso come malfunzionamento macchine e attrezzature e/o mancanza di macchine e attrezzature e/o obsolescenza macchine e attrezzature
- Metodologia: inetso come metodo non efficiente e/o non definito
- Materiali: inteso come mancanza di adeguate assicurazioni da parte del fornitore e/o materiale o servizio non conforme o difettoso
- Controlli: inteso come controlli non effettuati e/o non previsti e/o non registrati
- Contesto: inteso come insieme dei fattori aziendali influenzanti i vari processi (si veda precedente Punto 3)

Al fine di mettere in atto le misure necessarie a garantire la sicurezza dei dati come patrimonio della nostra Azienda e dei nostri Clienti, anche per rischi non legati specificatamente al trattamento dei dati stessi, si è proceduto a:

- l'individuazione di tutti i beni da proteggere:
  - ☑ risorse hardware
  - ☑ risorse software
  - ☑ dati
  - ☑ risorse professionali
  - ☑ documenti cartacei
  - ☑ supporti di memorizzazione
- l'individuazione, caso per caso, dei rischi:
  - ☑ uso non autorizzato di hardware
  - ☑ uso non autorizzato di software
  - ☑ perdita o riutilizzo di supporti cartacei e magnetici
  - ☑ rilevazione illegittima di informazioni
  - ☑ alterazione non autorizzata di informazioni
  - ☑ perdita di informazioni
  - ☑ uso non autorizzato di informazioni
  - ☑ penetrazione nelle reti di comunicazione
  - ☑ guasti tecnici delle attrezzature
  - ☑ minacce fisiche (intrusioni, incendio, ecc.)

La stima del rischio complessivo, che grava su un determinato trattamento di dati, è il risultato della combinazione di due tipi di rischi:

- quelli insiti nella tipologia dei dati trattati, che dipendono dalla loro appetibilità per soggetti estranei all'organizzazione, nonché dalla loro pericolosità per la riservatezza dei soggetti cui essi si riferiscono
- quelli legati alle caratteristiche degli strumenti utilizzati per procedere al trattamento dei dati

Si stima, inoltre, il grado di rischio, che dipende dalla tipologia dei dati trattati, combinando il fattore della loro appetibilità per terzi, con quello che esprime la loro pericolosità per la protezione dei dati del soggetto cui i dati si riferiscono:

Nella valutazione dei rischi per come sopra dettagliata, sono state individuate le seguenti ***MINACCE***:

COD	MINACCIA	EFFETTO	DATI
01	Accesso non autorizzato al sistema informatico da parte di personale interno.	Integrità e Riservatezza Sistemi Informativi e Gestionali	Art. 4 Artt. 9-10
02	Accesso non autorizzato al sistema informatico proveniente dall'esterno	Integrità e Riservatezza Sistemi Informativi	Art. 4 Artt. 9-10
03	Possibilità di visionare dagli schermi degli operatori le informazioni fornite dai sistemi gestionali, oppure possibilità di intercettare informazioni tra i terminali	Riservatezza delle postazioni locali di accesso ai gestionali	Art. 4 Artt. 9-10
04	Furto di informazioni presenti nei sistemi gestionali e nelle cartelle su server.	Disponibilità, Integrità e Riservatezza delle banche dati informatiche e dei sistemi gestionali	Art. 4 Artt. 9-10
05	Errato utilizzo dei software con pericolo di perdita delle informazioni contenute nei sistemi gestionali	Integrità dei dati contenuti nei sistemi informatici	Art. 4 Artt. 9-10
06	Guasto di componenti hardware idonei ad interrompere la disponibilità delle informazioni	Efficienza delle infrastrutture informatiche deputate al trattamento	Art. 4 Artt. 9-10
07	Azioni da Virus o Malware sui sistemi di gestione e sui client	Riservatezza, Integrità e Disponibilità delle banche dati informatiche	Art. 4 Artt. 9-10
08	Possibilità di conoscenza delle informazioni da parte dei tecnici esterni incaricati della manutenzione delle attrezzature informatiche	Riservatezza delle banche dati informatiche	Art. 4 Artt. 9-10
09	Perdita di dati dovuta ad errori logici, procedurali o fisici relativi all' infrastruttura informatica	Integrità, Disponibilità dei dati informatici	Art. 4
10	Smarrimento della documentazione cartacea durante le operazioni di trattamento – dati comuni	Disponibilità degli archivi cartacei	Art. 4
11	Smarrimento Documentazione cartacea durante le operazioni di trattamento – dati relativi allo stato di salute	Disponibilità degli archivi cartacei	Artt. 9-10
12	Possibilità di Incendio	Integrità dei documenti	Art. 4 Artt. 9-10
13	Situazioni che permettono la visione del contenuto dei documenti cartacei da parte di personale non autorizzato interno od esterno	Riservatezza dei documenti cartacei	Art. 4 Artt. 9-10
14	Accesso non autorizzato dovuto a mancanza di definizione dei ruoli aziendali e di legge	Riservatezza dei dati cartacei	Art. 4 Artt. 9-10
15	Furto di documentazione cartacea e dispositivi fisici di archiviazione dei dati informatici.	Riservatezza, Integrità e Disponibilità	Art. 4 Artt. 9-10
16	Errori degli operatori durante le operazioni di trattamento	Integrità e Disponibilità dei dati	Art. 4 Artt. 9-10
17	Impossibilità di accesso alle banche dati	Disponibilità dei dati	Art. 4 Artt. 9-10

Nella valutazione dei rischi per come sopra dettagliata, sono state individuate le seguenti ***MISURE*** applicabili:

COD	MISURA	DESCRIZIONE	TIPO
01	Controllo autorizzazione d'accesso ai sistemi gestionali	I sistemi gestionali dispongono di una user-id e password di accesso che identifica l'operatore e ne associa un profilo di autorizzazione. La scadenza delle password avviene ogni 90 o 180 giorni in funzione della natura sensibile o comune dei dati trattati. L'utente è in grado di definire autonomamente una nuova password. All'interno della gestione della password esiste una funzione di controllo sulla lunghezza minima.	Logica
02	FireWall	I dispositivi Firewall sono presenti per proteggere la rete aziendale dall'esterno.	Logica
03	Antivirus	I Server e tutti i client dispongono di programma antivirus (.....). Le definizioni dei virus sono aggiornate con cadenza giornaliera.	Logica
04	Autorizzazione accesso dominio	I client possono accedere al server di dominio solo attraverso una procedura di autenticazione informatica. La validità delle password rilasciate dal server è pari a 90 o 180 giorni in funzione della natura dei dati trattati.	
05	Password di accesso al client	L'accesso al client destinato al trattamento è protetto da Nome utente e password.	Logica
06	Salva schermo (screensaver) protetto da password	I client dispongono di salva schermo che in caso di mancato utilizzo del computer oscurano il video e proteggono il terminale con password di sblocco	Logica
07	Controllo aggiornamenti software	Con cadenza semestrale, il responsabile della sicurezza verifica gli aggiornamenti dei programmi utilizzati per il trattamento.	Logica
08	Isolamento da rete informatica	In alcuni casi si prevede di isolare il client dalla rete, diminuendo, in questo modo il rischio di esposizione del computer ad attacchi dall'esterno o dall'interno della rete aziendale.	Fisica
09	Backup su dispositivo magnetico	Il sistema di backup esegue una copia giornaliera di tutti i dati presenti su server.	Fisica
10	Armadio con chiusura per copie Backup	Le copie sono custodite in luoghi protetti da serratura e separati dal locale server.	Fisica
11	Istruzioni operative generiche per gli incaricati del trattamento	Agli incaricati vengono date disposizioni, per iscritto per l'accesso ai soli dati, la cui conoscenza sia strettamente necessaria per adempiere ai compiti loro assegnati: in caso di dubbio, è stato loro prescritto di rivolgersi ad un superiore, o ad un responsabile del trattamento, o direttamente al titolare. Gli incaricati devono custodire in modo appropriato gli atti, i documenti ed i supporti contenenti dati personali, loro affidati per lo svolgimento delle mansioni lavorative. Per quanto concerne l'archiviazione, sono state adibite apposite aree nelle quali conservare ordinatamente documenti, atti e supporti, in modo distinto per le diverse funzioni aziendali.	Organizzativa
12	Controllo accessi	Nelle sedi aziendali è presente una persona specificamente incaricata preposta al controllo delle persone che accedono agli uffici.	Organizzativa
13	Sistema di allarme	E' presente un sistema di allarme	Fisica
14	Corsi di formazione	Sono previsti corsi di formazione per il personale coinvolto nel processi di trattamento	Organizzativa
15	Custodia delle credenziali di accesso	Il Titolare del trattamento nomina un incaricato che detiene copia delle credenziali di accesso al sistema informatico. Le credenziali vengono mantenute in busta chiusa in armadio con serratura	Organizzativa
16	Estintori	Nelle sedi del trattamento sono presenti estintori secondo i parametri stabiliti dal D. Lgs. 81/08	Fisica

A seguito di questa analisi del rischio è scaturito, inoltre, un Piano di Miglioramento di cui si veda il riferimento al Cap. 9 del presente PPD/CC. In generale, sono state individuate le seguenti priorità di intervento, in base al rischio individuato:

- Priorità MASSIMA (RISCHIO ALTO): intervenire entro 7 giorni
- Priorità MEDIA (RISCHIO MEDIO): intervenire entro 30 giorni
- Priorità BASSA (RISCHIO BASSO): intervenire entro 365 giorni
- Priorità >BASSA (RISCHIO NON SIGNIFICATIVO): nessuna azione

Per un maggiore dettaglio operativo si veda di seguito.

MINACCIA	FATTORE DI RISCHIO e RELATIVA ESPOSIZIONE (PxD=R)			MISURA	FATTORE DI RISCHIO e RELATIVA ESPOSIZIONE (PxD=R) Post Misura			MIGLIORAMENTO NECESSARIO? (vedi Piano di Miglioramento Cap. 9)		PIORITÀ (vedi pagina precedente e Piano di Miglioramento Cap. 9)
	P	D	R		P	D	R	SI	NO	
01	1	3	3	1/4/5/6/8/11	1	1	1			
02	2	3	6	1/2/3/4/7/8	2	1	2			
03	1	2	2	1/5/6/11	1	2	2			
04	2	4	8	1/2/3/5/6/7/9/11/12	1	2	2			
05	2	4	8	9/11/14	1	2	2			
06	1	2	2	3/7/9	1	1	1			
07	2	4	8	3/7/8	1	2	2			
08	1	2	2	1/2/4/6/12	1	2	2			
09	2	2	4	9/14	1	2	2			
10	2	2	4	11	1	2	2			
11	2	2	4	11	1	2	2			
12	1	4	4	16	1	2	2			
13	1	3	3	11/12	1	2	2			
14	1	3	3	11/14	1	2	2			
15	1	3	3	10/11/12/13	1	2	2			
16	2	2	4	14	1	2	2			
17	1	3	3	7/16	1	2	2			

Tale valutazione viene aggiornata almeno una volta all'anno da parte del Titolare e del Responsabile.

8. MISURE ATTE A GARANTIRE L'INTEGRITÀ E LA DISPONIBILITÀ DEI DATI

Nel presente paragrafo vengono descritte le misure atte a garantire:

- la protezione delle aree e dei locali, nei quali si svolge il trattamento dei dati
- la corretta archiviazione e custodia di atti, documenti e supporti contenenti dei dati
- la sicurezza logica, nell'ambito dell'utilizzo degli strumenti elettronici

Si procede alla descrizione:

- delle misure che risultano già adottate dal Titolare, nel momento in cui viene redatto il presente documento
- delle ulteriori misure, finalizzate ad incrementare la sicurezza nel trattamento dei dati, la cui adozione è stata programmata (vedi Piano di Miglioramento), ovvero per adeguarsi alle novità introdotte dal Regolamento CE 679/2016

8.1 La protezione di aree e locali

Per quanto concerne il rischio d'area, legato ad eventi di carattere distruttivo, gli edifici ed i locali nei quali si svolge il trattamento si veda l'Allegato 2.

Gli impianti ed i sistemi di cui è dotata la nostra Organizzazione appaiono soddisfacenti, al fine di garantire le opportune misure di sicurezza, al trattamento di dati personali da essa svolti. Per l'anno 2018, sono quindi previsti semplicemente interventi finalizzati all'aggiornamento delle tecnologie, ove necessario, ed alla manutenzione quando richiesto.

8.2 La custodia e l'archiviazione di atti, documenti e supporti cartacei

Alle persone autorizzate al trattamento vengono impartite precise istruzioni, di accedere ai soli dati, la cui conoscenza sia strettamente necessaria per adempiere ai compiti loro assegnati: in caso di dubbio, è stato loro prescritto di rivolgersi ad un superiore, o direttamente al Titolare o al Responsabile. Di conseguenza, alle stesse persone è prescritto di prelevare dagli archivi i soli atti e documenti che vengono loro affidati per lo svolgimento delle mansioni lavorative, che devono controllare e custodire, durante l'intero ciclo necessario per lo svolgimento delle operazioni di trattamento, per poi restituirli all'archivio, al termine di tale ciclo.

Cautele particolari sono previste per gli atti, documenti e supporti contenenti dati sensibili: in questi casi viene prescritto di provvedere al controllo ed alla custodia in modo tale che ai dati non possano accedere persone prive di autorizzazione. A tale fine, gli incaricati, in base alle loro mansioni, sono stati dotati di:

- armadi e cassetti sia muniti di serratura che non
- stanze chiudibili a chiave

Gli incaricati devono riporre i documenti, contenenti dati sensibili negli archivi controllati prima di assentarsi dal posto di lavoro, anche temporaneamente. Per quanto concerne l'archiviazione, il Titolare ha adibito apposite aree, nelle quali conservare ordinatamente documenti, atti e supporti contenenti dati.

Gli archivi contenenti dati sensibili sono controllati mediante l'adozione dei seguenti accorgimenti: le persone vengono autorizzate preventivamente ad accedere agli archivi.

Gli strumenti e le attrezzature, di cui è dotato il Titolare per la custodia e l'archiviazione di atti, documenti e supporti cartacei, con particolare riferimento a quelli contenenti dati sensibili o giudiziari, appaiono soddisfacenti al fine di garantire la necessaria sicurezza ai dati. Per l'anno 2018 sono quindi previsti semplicemente interventi di miglioramento gestionale, ove necessario (vedi Cap. 9).

8.3 Pseudonimizzazione

Consiste nel trattamento dei dati personali in modo tale che non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile.

Nella nostra azienda **NON E'** messa in atto la pseudonomizzazione

8.4 Le misure logiche di sicurezza

Il sistema di autenticazione informatica viene adottato per disciplinare gli accessi agli strumenti elettronici presenti nell'organizzazione del Titolare. Viene impostata e gestita una procedura di autenticazione, che permette di verificare l'identità della persona e quindi di accertare che la stessa è in possesso delle credenziali di autenticazione per accedere allo strumento elettronico. In particolare, sulla base di quanto richiesto dalla normativa, il controllo avviene attraverso:

- un insieme di politiche e di regole di accesso che stabiliscono le modalità (lettura, modifica, aggiornamento, ecc.) secondo le quali i vari soggetti possono accedere ai dati
- un insieme di procedure di controllo (meccanismi di sicurezza) che controllano se la richiesta di accesso è consentita o negata, in base alle regole stabilite

Il tutto è dettagliato nell'***Allegato 4. INFRASTRUTTURE CONTENENTI DATI E RELATIVE MISURE DI SICUREZZA LOGICO-INFORMATICHE***

In particolare:

User-ID e sistemi di parole chiave (password)

Per i trattamenti effettuati con strumenti elettronici (elaboratori in rete locale, programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato), si adotta un sistema di autenticazione informatica per disciplinare gli accessi a tutti gli strumenti elettronici tramite l'utilizzo di User ID e Password a livello di:

- User ID e Password all'accensione del PC come utente o come amministratore
- User ID e Password per l'accesso ai programmi applicativi gestionali

I ruoli e le responsabilità di ogni utente o di ogni profilo utente con accesso a sistemi informatici e ai dati sono chiaramente definite nell'***Allegato 6 - AUTORIZZAZIONI***. Le regole per la gestione delle credenziali sono definite nell'***Allegato 4. INFRASTRUTTURE CONTENENTI DATI E RELATIVE MISURE DI SICUREZZA LOGICO-INFORMATICHE.***

Ogni utente è responsabile della riservatezza delle proprie password e nel caso in cui sia riconosciuto un accesso fortuito o fraudolento realizzato da persone non autorizzate, verrà registrato come un incidente/non conformità e si procederà alla modifica. Secondo il regolamento CE 679/2016, la frequenza di modifica della password in nessun caso dovrà essere superiore a 6 mesi, e per tutta la loro validità si conserveranno in forma intelligibile. In qualsiasi momento sarà possibile avere un rapporto aggiornato degli utenti, profili utente e accessi autorizzati per ciascuno di loro, facendone richiesta all'amministratore di sistema.

Per chiarimenti e delucidazioni sulla comprensione ed applicazione di tali regole, il personale si può rivolgere direttamente al Titolare/Responsabile del trattamento.

Procedura per la conservazione e la gestione in sicurezza dei dati

I dati personali devono essere protetti dai rischi, anche accidentali, di distruzione, perdita o modifica non consentita.

La Riservatezza dei dati resta sotto la responsabilità dell'utente che ha accesso ai dati stessi. Ogni utente farà in modo che le informazioni disponibili non possano essere visualizzate da persone non autorizzate. Nel periodo in cui non sia possibile trovare i documenti con i dati personali nei rispettivi archivi, perché è in fase di revisione o in processo di gestione, prima o dopo l'archiviazione, la persona che si occupa di questo processo dovrà custodire il documento e prevenirne l'accesso a terzi non autorizzati.

Uso e riutilizzo di supporti di memorizzazione informatici e supporti cartacei

Tutti i supporti che contengono dati al termine del trattamento devono essere distrutti in modo che non sia consentito il recupero delle informazioni ivi contenute. Nel caso in cui tali supporti debbano essere riutilizzati preventivamente occorre procedere alla cancellazione in modo permanente ed irrecuperabile delle informazioni ivi contenute. In particolare, si applicano le seguenti regole:

- Quando una qualsiasi periferica che abbia o abbia avuto informazione digitale archiviata deve essere abbandonata o sostituita, il responsabile informatico la preleva
- Se possibile, procede con la formattazione
- Se si tratta di un supporto digitale senza possibilità di formattazione procede con la distruzione física rendendo quindi impossibile fisicamente il recupero o la lettura del contenuto precedentemente salvato
- Gli Hard Disk inattivi sono ritirati, smontati, aperti e ne sono distrutti i dischi elettromagnetici e successivamente ne sono riciclate le componenti

Tale procedura, previa formazione di una copia, deve essere adottata anche nel caso in cui i supporti contenenti dati debbano per qualsiasi ragione essere spostati al di fuori del perimetro aziendale o, comunque al di fuori del controllo diretto della nostra Organizzazione (per esempio per i Responsabili del trattamento in outosurcing). Specifiche procedure potranno essere adottate per l'uso di supporti rimovibili in relazione alla sensibilità dei dati in essi trattati.

I supporti di memorizzazione rimovibili (ad es. hard disk estraibili, cd-rom, dvd, memorie usb, memory stick, flash disk, ecc.) che contengono dati devono essere etichettati nel rispetto della Policy per la classificazione dei dati. Ai supporti di memorizzazione rimovibili, in relazione alla natura dei dati contenuti, si applicano gli stessi principi di sicurezza e le medesime misure previste per i supporti fissi, sopra specificate.

I supporti che contengono od hanno contenuto dati personali e/o particolari possono essere riutilizzati o ceduti previa autorizzazione del responsabile della risorsa nel rispetto dei presenti criteri generali. In particolare, i supporti utilizzati per il trattamento, anche temporaneo, di dati particolari devono essere previamente cancellati in modo tale che permanentemente non sia tecnicamente consentito il recupero di tali dati.

Nel caso in cui i supporti rimovibili o apparecchiature che contengono dati debbano essere affidati a terzi per motivi diversi dal trattamento (ad esempio per manutenzione), ove non sia possibile la rimozione di tali dati, occorre adottare le stesse misure di sicurezza previste per previste per i supporti fissi.

L'uscita di supporti e documenti contenenti dati, compresi i documenti allegati, tra cui e-mail, dovrà essere autorizzata dal Responsabile. Lo stesso Responsabile autorizza solo l'uscita delle informazioni necessarie richieste che saranno inviate in modo sicuro, e in ogni caso, garantendo che i dati siano ricevuti dal facente richiesta impedendo qualsiasi accesso da parte di terzi.

Per l'uscita di quei dati con alto livello di sicurezza sarà creato un registro di ingressi e uscite per garantire il controllo e la sicurezza dei dati del file. I dati che dovranno essere riportati nel registro di uscita (188 del SGQ) saranno:

<table>
<tr><td>Tipo di supporto</td><td>Tipo di informazione (contenuto)</td></tr>
<tr><td>Data</td><td>Forma di invio</td></tr>
<tr><td>Mittente</td><td rowspan="2">Responsabile (autorizzato)</td></tr>
<tr><td>Numero di documenti</td></tr>
</table>

La distribuzione dei supporti contenenti dati sarà in forma codificata (Vedere SOP-238 sistema di crittografia digitale) o tramite qualsiasi altro meccanismo che garantisca l'inaccessibilità dell'informazione cosi come l'impossibilità di manipolazione della stessa prima di raggiungere il destinatario.

Uso di telefoni e fax

L'uso di telefoni e fax aziendali è consentito esclusivamente per motivi aziendali, ed eccezionalmente per motivi personali. Non possono essere utilizzati né telefoni né fax per trasmettere dati sensibili.

Backup

Viene utilizzato quanto previsto nell'***Allegato 7. ISTRUZIONI DI BACKUP***.

Uso di fotocopiatrici, scanner, masterizzatori

Non è consentito effettuare operazioni di copiatura, salvo le operazioni di backup, di dati personali e sensibili, se non per stretta necessitá d'ufficio e con l'autorizzazione del Responsabile. Le copie di dati personali o sensibili devono essere distrutte al termine della necessitá di trattamento in modo da non consentirne il recupero. L'uso di apparecchiature di copiatura non è generalmente consentito per fini diversi da quelli aziendali. È consentito un uso personale di fotocopiatrici e stampanti, purché effettuato al di fuori del normale orario di lavoro e con moderazione.

In ogni caso l'autore delle copie è responsabile per il contenuto delle stesse obbligandosi a rispettare la normativa vigente (ad esempio quella in materia di diritto d'autore) ed a sollevare da ogni e qualsiasi responsabilità **STUDIO DI CONSULENZA TRIBUTARIA E SOCIETARIA**.

Comportamento in caso di incidente

STUDIO DI CONSULENZA TRIBUTARIA E SOCIETARIA ha attivato un registro di indicenti che riguardano la sicurezza dei dati. Questo registro è utilizzato per raccogliere le non conformità del Sistema di Gestione Qualità ed ha come obiettivo quello di offrire delle evidenze riguardanti i problemi incontrati e relazionati ai dati.

Si definisce incidente qualsiasi evento che possa avere un impatto tale da mettere in pericolo la sicurezza dei dati, dal punto di vista della riservatezza, integrità o disponibilità. Nel caso in cui si tratti di un incidente grave o che comporti un lungo periodo prima di arrivare ad una soluzione, si procederà all'elaborazione di una specifica relazione sulla qualità. Come esempi vengono descritte le seguenti definizioni:

- Riservatezza:
  - Questioni relative alle esigenze degli utenti e dei pazienti in materia di riservatezza dei dati personali
  - Rilevamento di accessi eccessivi o imprevisti
- Integrità:
  - Dati non aggiornati
  - Dati non corretti
- Disponibilità:
  - Incidenti causati da problemi presenti nelle copie di sicurezza o disponibilità di informazioni al personale autorizzato ad usarlo
  - Mancanza di permesso di accesso ai dati da parte di personale che ne ha bisogno per motivi di lavoro

REGOLE GENERALI DA SEGUIRE IN CASO DI INCIDENTE:

- In caso di incidente o di sospetto incidente deve esserne data immediata comunicazione al Titolare e al Responsabile del trattamento. L'utente deve evitare di compiere qualsiasi attività od operazione sul sistema che possa pregiudicare in qualche modo la rilevazione dell'incidente e le indagini conseguenti
- In caso di incidente o sospetto incidente legato alla rete l'utente può scollegare fisicamente la macchina dalla rete. Per nessun motivo la macchina deve essere spenta. L'utente deve fornire agli incaricati della sicurezza tutta la collaborazione e le informazioni richieste relative all'incidente

Antivirus

Il SW antivirus utilizzato è quello descritto nell'***Allegato 4. INFRASTRUTTURE CONTENENTI DATI E RELATIVE MISURE DI SICUREZZA LOGICO-INFORMATICHE***. Questo antivirus viene aggiornato automaticamente attraverso il semplice accesso ad internet. Tale sistema di protezione viene aggiornato ed attivato automaticamente ad ogni avvio degli stessi terminali.

Ripristino dati (Dysaster recovery)
Per i server sono previste procedure di backup, attraverso le quali viene periodicamente effettuata una copia di tutti i dati presenti nel sistema.

In particolare, tali misure garantiscono la possibilità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico, fatto salvo il caso di eventi di forza maggiore (per esempio incendio o crollo del palazzo) per i quali, alla data odierna, ci si affida alle attività di mirroring dei sistemi informativi effettuate sempre da parte dell'IT. In particolare dovranno essere considerati almeno i seguenti aspetti:

- le condizioni di attivazione del piano di continuità
- le attività di emergenza che dovranno essere seguite (incluse le istruzioni per il rapporto delle cause dell'interruzione)
- le specifiche attività che dovranno essere eseguite per rimediare temporaneamente l'interruzione (ad esempio lo spostamento di servizi essenziali in locazioni temporanee, l'adozione di processi alternativi temporanei, ecc.)
- le attività che dovranno essere eseguite per il ripristino delle normali attività
- un programma di verifica e di test della procedura
- un programma di formazione per addestrare gli incaricati ad eseguire la procedura correttamente
- l'individuazione dei responsabili per l'esecuzione delle procedure attraverso anche, se ritenuto opportuno, un piano di reperibilità
- la scala dei tempi di reazione e ripristino alla normalità dal verificarsi dell'evento che ha causato l'interruzione

Cessione dati all'esterno
Nei casi in cui i trattamenti di dati vengano affidati all'esterno della struttura del Titolare, in conformità a quanto previsto dal Regolamento CE 679/2016, si adottano i seguenti criteri, atti a garantire che il soggetto destinatario adotti misure di sicurezza conformi a quelle minime previste dal dettato legislativo. Nel dettaglio, il destinatario esterno viene nominato dal Titolare come Responsabile del Trattamento dei dati in outsourcing, mediante apposita lettera sottoscritta. Il destinatario esterno rilascia in questa maniera una dichiarazione con la quale certifica l'adozione delle misure minime di sicurezza, nonché di ulteriori misure eventualmente adottate, a garanzia della sicurezza delle aree e dei locali nei quali si svolge il trattamento dei dati, della corretta archiviazione e custodia di atti, documenti e supporti contenenti dati.
Nel caso sia ritenuto necessario il Responsabile in outsourcing dovrà applicare la procedure di sicurezza interna, dando evidenza dell'approvazione delle stesse.

Le misure logiche di sicurezza, di cui è dotato il Titolare per la protezione dei trattamenti che avvengono con strumenti elettronici appaiono nel loro complesso soddisfacenti, al fine di garantire la necessaria sicurezza ai dati personali trattati. Per l'anno 2018, sono quindi previsti semplicemente interventi finalizzati all'aggiornamento ed alla manutenzione, ove ritenuto necessario (vedi anche Cap. 9).

9. CONTROLLO GENERALE SULLO STATO DELLA SICUREZZA E ATTIVITÀ DI SELF AUDIT

Al Titolare e al Responsabili è affidato il compito di aggiornare le misure organizzative e tecniche di sicurezza al fine di adottare gli strumenti e le conoscenze, resi disponibili dal progresso tecnico, che consentano di ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati, di accesso non autorizzato o di trattamento non consentito.

Al fine di verificare l'efficacia delle misure di sicurezza adottate, il Titolare, in stretta collaborazione con i Responsabil del trattamento, o affidando l'incarico ad Auditor esterni preventivamente qualificati, provvede con frequenza almeno annuale, ovvero con controlli a campione, ad effettuare una o più delle seguenti attività:

- verificare l'accesso fisico ai locali dove si svolge il trattamento
- verificare l'aggiornamento tecnologico delle risorse disponibili per il trattamento dati
- verificare la correttezza delle procedure di archiviazione e custodia di atti, documenti e supporti contenenti dati

➔ verificare il livello di formazione delle persone auorizzate al trattameno dei dati

I medesimi controlli potranno essere richiesti ed effettuati anche nei confronti di eventuali partner esterni, ovvero nei confronti dei Responsabili in outsourcing. Di tali attività vengono conservarte opportune registrazioni. Il rapporto di audit ha lo scopo di dare un parere sulla adeguatezza delle misure e dei controlli, identificando le carenze e proponendo le misure correttive o complementari. Dovrà anche includere dati, fatti e osservazioni su cui si basano i pareri e le raccomandazioni proposte. Il rapporto di audit deve essere analizzato dai Responsabili del trattamento che dovranno trasmetterne i risultati al Titolare affinchè possa adottare le opportune misure correttive. Tale Rapporto rimane a disposizione dell'Autorità Garante.

Inoltre, sarà effettuato un audit ogni volta che vengono apportate modifiche sostanziali nel sistema di informazioni che potrebbero influire sul rispetto delle misure di sicurezza, con l'obiettivo di verificare l'adattamento, l'adeguatezza e l'efficacia.

10. ANALISI DEL TITOLARE DEL TRATTAMENTO E PIANO DI MIGLIORAMENTO

Almeno una volta all'anno, il Titolare del trattamento, in collaborazione con la Funzione IT, nonché con i vari Responsabili di funzione che ritiene coinvolgere, effettua un'analisi di dettaglio sullo stato di applicazione e di adeguatezza del Sistema di gestione della Protezione dei Dati. In particolare tale analisi tiene conto dei seguenti aspetti:

➔ INPUT
- ☑ Analisi dell'ambiente che tiene conto di ciò che influenza internamente o esternamente la protezione dei dati
- ☑ Rrisultati delle precedenti analisi del Titolare del trattamento
- ☑ Informazioni di ritorno dagli interessati e dagli stakeholders
- ☑ Informazioni dal sistema di audit attuato
- ☑ Informazioni in merito ai controlli, monitoraggi, misure, test, metodi ed analisi che sono necessari per garantire il corretto trattamento dei dati
- ☑ Dati misurabili sul raggiungimento degli obiettivi determinati a livello di Piano di miglioramento
- ☑ Informazioni su eventuali non conformità emesse e sullo stato delle relative azioni correttive
- ☑ I risultati dell'analisi del rischio e della valutazione di impatto
- ☑ Analisi sulla necessità di far progredire il sistema di gestione per la protezione dei dati messo in atto

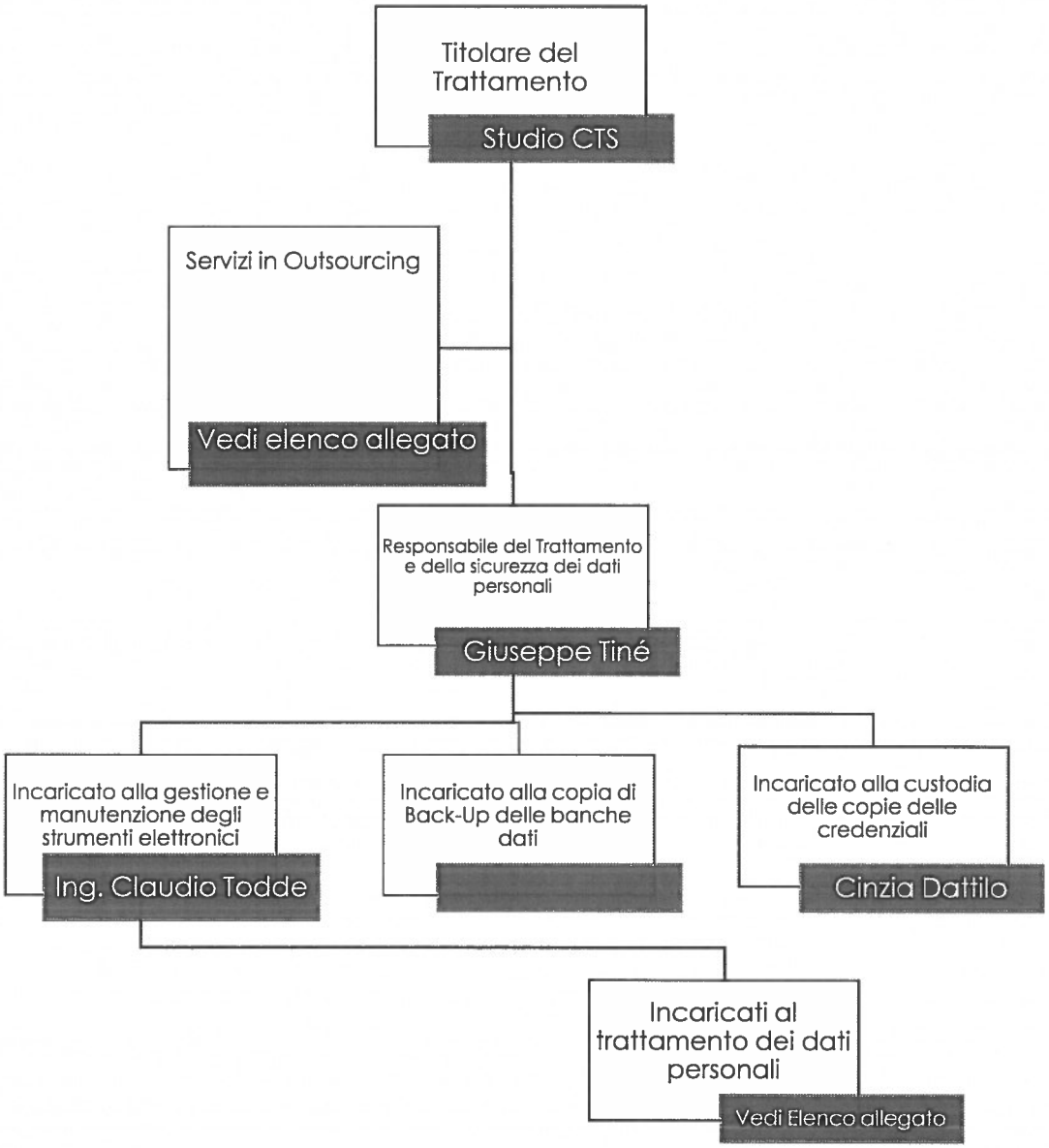
➔ OUTPUT
- ☑ Attività per il progresso del sistema di gestione per la protezione dei dati
- ☑ Cambiamenti al sistema di gestione per la protezione dei dati messo in atto
- ☑ Esigenza di risorse umane, risorse economiche/finanziarie, di infrastrutture (hardware e/o software), di ambienti di lavoro adeguati, di nuove tecnologie, di nuove tecniche per la protezione dei dati

In riferimento a quanto esposto, viene riportato il programma individuato da **STUDIO DI CONSULENZA TRIBUTARIA E SOCIETARIA** per il continuo miglioramento del Sistema di Gestione della Protezione dei Dati implementato.

Tale Piano viene costantemente aggiornato in relazione alle attività implementate ed a eventuali modifiche necessarie e comunque almeno una volta all'anno, da parte del Titolare.

Allegato 1. ORGANIGRAMMA

Ai sensi del Regolamento CE 679/2016



ELENCO INCARICATI AL TRATTAMENTO DEI DATI PERSONALI		***SERVIZI IN OUTSOURCING***	
COGNOME NOME	***COGNOME NOME***	***NOME O RAGIONE SOCIALE***	***INCARICO***
Stefania Porta		Studio T&G Snc	Elaborazione paghe
Hernan Zarco		Stratrash Srl	Sicurezza sul lavoro

Luogo e Data	

Studio di Consulenza Tributaria e Societaria

Allegato 2 - ELENCO DELLE SEDI IN CUI VENGONO TRATTATI I DATI RELATIVE MISURE DI SICUREZZA FISICA

Ai sensi del Regolamento CE 679/2016

SEDE	***SEDE PRINCIPALE / LEGALE***
INDIRIZZO	Viale Majno 10
TEL.	02 77878001
FAX.	02 77878077
MAIL	segreteria@studiocts.net
P.I/C.F.	

MISURE DI SICUREZZA	
ACCESSO	Controllato
REGISTRAZIONE ACCESSI	=
ACCESSO CONSENTITO AL PUBBLICO	Sì
SISTEMA ANTINCENDIO	Estintori
FINESTRE CON INFERRIATE	=
ARMADI IGNIFUGHI CON SERRATURA	=
ARMADI IGNIFUGHI SENZA SERRATURA	=
ARMADI NON IGNIFUGHI CON SERRATURA	Sì
ARMADI NON IGNIFUGHI SENZA SERRATURA	Sì
CASSAFORTE	Sì
CHIUSURA	Porta con chiave
ALLARME	Presente
VIDEOSORVEGLIANZA	Sì
SCAFFALATURE	Sì
DISPOSITIVI UPS	Sì

Allegato 3. ELENCO DEGLI ARCHIVI DEI DATI OGGETTO DEL TRATTAMENTO

Ai sensi del Regolamento CE 679/2016

NOME BANCA DATI	*CLIENTI*	*DIPENDENTI / SOCI*	*FORNITORI*
DESCRIZIONE	Dati anagrafici e contrattuali dei clienti	Dati anagrafici, contrattuali, dati inerenti lo stato di salute, l'appartenenza a sindacati, dati giudiziari	Dati anagrafici e contrattuali dei fornitori
FUNZIONE	Gestione commerciale, amministrativa e contabile	Gestione amministrativa e contabile del rapporto di lavoro	Gestione commerciale, amministrativa e contabile
TIPO DI DATI	Art. 4 , Art. 9 e Art. 10	Art. 4 , Art. 9 e Art. 10	Art. 4 , Art. 9 e Art. 10
CATEGORIA INTERESSATI	Clienti attivi e/o potenziali	Dipendenti	Fornitori e Partner commerciali
TITOLARE DEL TRATTAMENTO	**STUDIO DI CONSULENZA TRIBUTARIA E SOCIETARIA** nella persona del Legale Rappresentante sig **LEGALE RAPPRESENTANTE**	**STUDIO DI CONSULENZA TRIBUTARIA E SOCIETARIA** nella persona del Legale Rappresentante sig **LEGALE RAPPRESENTANTE**	**STUDIO DI CONSULENZA TRIBUTARIA E SOCIETARIA** nella persona del Legale Rappresentante sig **LEGALE RAPPRESENTANTE**
RESPONSABILE DEL TRATTAMENTO	Giuseppe Tiné	Giuseppe Tiné	Giuseppe Tiné
RESPONSABILI ESTERNI DEL TRATTAMENTO	Nessuno	Startrush Srl e Studio T&G Snc	Nessuno
FINALITA' DEL TRATTAMENTO	➢ Erogazione del servizio richiesto ➢ In relazione alle esigenze contrattuali ed ai conseguenti adempimenti degli obblighi legali e fiscali, nonché per consentire una efficace gestione dei rapporti finanziari e commerciali ➢ Espletamento di obblighi di legge in generale ➢ Finalità amministrative e commerciali	➢ Elaborazione, liquidazione e corresponsione della retribuzione, degli emolumenti, dei compensi dovuti e della relativa contabilizzazione ➢ Gestione del rapporto del lavoro in generale ➢ Laddove previsto, adempimento o assolvimento di obblighi derivanti dal Contratto Individuale, dal Contratto Collettivo, dalle Leggi, dai Regolamenti e dalla Normativa Comunitaria in materia di previdenza ed assistenza anche integrativa e complementare, di igiene e sicurezza del lavoro e in materia fiscale, ovvero posti a tutela della salute, dell'ordine e della sicurezza pubblica ➢ Laddove previsto, tutela dei diritti in sede giudiziaria ➢ Laddove previsto, gestione dello sviluppo e della formazione tecnica e manageriale	➢ In relazione alle esigenze contrattuali ed ai conseguenti adempimenti degli obblighi legali e fiscali, nonché per consentire una efficace gestione dei rapporti finanziari e commerciali ➢ Espletamento di obblighi di legge in generale ➢ Finalità amministrative e commerciali

Allegato 3. ELENCO DEGLI ARCHIVI DEI DATI OGGETTO DEL TRATTAMENTO

Ai sensi del Regolamento CE 679/2016

NOME BANCA DATI	*CLIENTI*		*DIPENDENTI / SOCI*		*FORNITORI*	
ARCHIVIO	ACCESSO CONTROLLATO	ACCESSO NON CONTROLATO	ACCESSO CONTROLLATO	ACCESSO NON CONTROLATO	ACCESSO CONTROLLATO	ACCESSO NON CONTROLATO
Schedari ed altri supporti cartacei	x		x		x	
Elaboratori di Rete	x		x		x	
Elaboratori non in rete	=		=		=	
SISTEMA DI ARCHIVIAZIONE	Server		Server		Server	
NOTE						

Allegato 4. INFRASTRUTTURE CONTENENTI DATI E RELATIVE MISURE DI SICUREZZA LOGICO-INFORMATICHE

Ai sensi del Regolamento CE 679/2016

INFRASTRUTTURA	PC/SERVER/STAMPANTE/MULTIFUNZIONE	
MODELLO E MARCA	TX 150 FUJITSU / N° 2 Server Fujitsu RX300S6 storage Fujitsu DX60S2 Nas Fujitsu KS12017	
SISTEMA OPERATIVO	WMWARE - WIW SERVER 2012 - Linux	
SEDE O UFFICIO	VIALE MAJNO 10 20129 - MILANO	
PERSONA/E AUTORIZZATA/E ALL'UTILIZZO	CLAUDIO TODDE	
LETTORE CD/DVD	//	
PORTE USB O SIMILARI	4	
ANTIVIRUS E FREQUENZA DI AGGIORNAMENTO	NOD 32 (giornaliero)	
FIREWALL	CLAVISTER E 80	
USER-ID	NOME.COGNOME	
PASSWORD	LUNGHEZZA	Minimo 8 caratteri o il massimo consentito dal sistema, non deve essere ripetitiva né riutilizzata
	COMPOSIZIONE	I caratteri scelti devono essere alfanumerici (sono accettate sia lettere maiuscole che minuscole, numeri o simboli) e deve di includere almeno un simbolo tra quelli seguenti: (. \ + * ? [^] $ ( ) { } = ! < > | : -)
	CAMBIO PSW	90 giorni (3 mesi): Art. 9-10 180 giorni (6 mesi): Art. 4 *Nota: non è possibile impostare la stessa password per due volte consecutive*
	AUTOMODIFICA	Consentita
ELABORATORI IN RETE?	si	
NOTE		

Studio di Consulenza Tributaria e Societaria

Allegato 5. PIANO DI FORMAZIONE E ADDESTRAMENTO

Ai sensi del Regolamento CE 679/2016

COGNOME E NOME	NECESSITÀ FORMATIVA / DESCRIZIONE CORSO PREVISTO	DATA PREVISTA	DATA EFFETTIVA
Tutti gli incaricati	Informazione e aggiornamento sulla disciplina vigente e sulle relative responsabilità di applicazione delle regole organizzative e tecniche per la sicurezza – Corso: CE 679/2016 Sistema di Gestione della Protezione dei Dati (4 ore)	Entro 09/18	

LUOGO E DATA		IL RESPONSABILE DEL TRATTAMENTO	

Allegato 6. AUTORIZZAZIONI AL TRATTAMENTO

Ai sensi del Regolamento CE 679/2016

BANCA DATI / OPERAZIONI AUTORIZZATE / SOGGETTI AUTORIZZATI	CLIENTI				FORNITORI				PERSONALE				SOCI/AZIONISTI			
	INSERIMENTO	ACCESSO E/O ESTRAZIONE	MODIFICA	ELIMINAZIONE	INSERIMENTO	ACCESSO E/O ESTRAZIONE	MODIFICA	ELIMINAZIONE	INSERIMENTO	ACCESSO E/O ESTRAZIONE	MODIFICA	ELIMINAZIONE	INSERIMENTO	ACCESSO E/O ESTRAZIONE	MODIFICA	ELIMINAZIONE
Stefania Porta	X	X	X	X	X	X	X	X								
Hernan Zarco	X	X	X	X	X	X	X	X								

Allegato 6. AUTORIZZAZIONI AL TRATTAMENTO

Ai sensi del Regolamento CE 679/2016

Allegato 7. ISTRUZIONI DI BACK UP

Ai sensi del Regolamento CE 679/2016

SUPPORTO DI BACK-UP	PERIODICITÀ DEL BACK-UP	N° COPIE EFFETTUATE OGNI VOLTA	N° SUPPORTI UTILIZZATI
QUANTUM ULTRIUM	Cinque giorni su sette	1	5

ID SUPPORTO	LUOGO DI CONSERVAZIONE	INCARICATO ALLA COPIA	INCARICATO ALLA VERIFICA
01 ÷ 05	Viale Majno 10 - 20129 MILANO	Valentina Nobile	CLAUDIO TODDE
	IN CASSAFORTE		

NOTE	
	Back – up effettuato giornalmente da martedi al sabato su cassetta giornaliera Quantum. Nello specifico: un incaricato estrae dal lettore la cassetta con il backup giornaliero e la sostituisce con una contenente il backp di 7 giorni antecedenti. Tra i 90 e 180 giorni un backup viene conservato in cassaforte a parte in modo da poter risalire ai dati di 3-6 mesi antecedenti.

IL RESPONSABILE DEL TRATTAMENTO	INCARICATO ALLA GESTIONE E MANUTENZIONE STRUMENTI ELETTRONICI