Lettera di incarico

Trevi, 24/05/2018

Oggetto: Lettera di nomina quale Contitolare

Il/La sottoscritto/a Studio Legale Associato Felicetti Frascarelli Menghini, p.iva 02287020545, in qualità di titolare del trattamento dei dati ai sensi del GDPR 2016/679 e normativa nazionale in vigore,

NOMINA

Avv. Felicetti Mauro, c.f. FLCMRA53H16D653Y, quale Contitolare per la sede Sede Studio, Piazza della Concordia 1, 06039 Trevi PG, dalla data del 24/05/2018.

Per accettazione dell'incarico
Contitolare
(Avv. Mauro Felicetti)

_____
(firma)

Il titolare del trattamento
(Studio Legale Associato Felicetti Frascarelli Menghini)

_____
(firma)

Lettera di incarico

Trevi, 24/05/2018

Oggetto: Lettera di nomina quale Contitolare

Il/La sottoscritto/a Studio Legale Associato Felicetti Frascarelli Menghini, p.iva 02287020545, in qualità di titolare del trattamento dei dati ai sensi del GDPR 2016/679 e normativa nazionale in vigore,

NOMINA

Avv. Frascarelli Dimitri, c.f. FRSDTR60M12F492M, quale Contitolare per la sede Sede Studio, Piazza della Concordia 1, 06039 Trevi PG, dalla data del 24/05/2018.

Per accettazione dell'incarico
Contitolare
(Avv. Dimitri Frascarelli)

_____
(firma)

Il titolare del trattamento
(Studio Legale Associato Felicetti Frascarelli Menghini)

_____
(firma)

Lettera di incarico

Trevi, 24/05/2018

Oggetto: Lettera di nomina quale Contitolare

Il/La sottoscritto/a Studio Legale Associato Felicetti Frascarelli Menghini, p.iva 02287020545, in qualità di titolare del trattamento dei dati ai sensi del GDPR 2016/679 e normativa nazionale in vigore,

NOMINA

Avv. Menghini Alberto, c.f. MNGLRT65D17D653D, quale Contitolare per la sede Sede Studio, Piazza della Concordia 1, 06039 Trevi PG, dalla data del 24/05/2018.

Per accettazione dell'incarico
Contitolare
(Avv. Alberto Menghini)

_____
(firma)

Il titolare del trattamento
(Studio Legale Associato Felicetti Frascarelli Menghini)

_____
(firma)

Lettera di incarico

Trevi, 24/05/2018

Oggetto: Lettera di nomina al Responsabile esterno del trattamento dati

Il/La sottoscritto/a Studio Legale Associato Felicetti Frascarelli Menghini, p.iva 02287020545, in qualità di titolare del trattamento dei dati ai sensi del GDPR 2016/679 e della normativa nazionale in vigore,

NOMINA

S.P.E.E.D. S.n.c. Di Carter & C., p.iva 01576100547 Responsabile esterno del trattamento dei dati per la sede Sede Studio
, Piazza della Concordia 1, 06039 Trevi PG, dalla data del 24/05/2018, con strumenti elettronici o comunque automatizzati o con strumenti diversi, per l'ambito di attribuzioni, competenze e funzioni assegnate.
In qualità di Responsabile del trattamento dei dati ha il compito e la responsabilità di adempiere a tutto quanto necessario per il rispetto delle disposizioni vigenti in materia e di osservare scrupolosamente quanto in essa previsto, nonchè le istruzioni impartite dal Titolare.

REQUISITI DELL'INCARICO

MATERIA DISCIPLINATA	Consulenza ed assistenza in materia fiscale e tributaria, redazione contabilità aziendale, contenzioso tributario, (ecc.)
DURATA DEL TRATTAMENTO	• I dati saranno trattati per tutto il tempo necessario allo svolgimento del rapporto commerciale in essere e per i successivi dieci anni dalla data di acquisizione degli stessi.
DESCRIZIONE DEI TRATTAMENTI	
FINALITÀ	• Adempimento di obblighi di legge connessi a rapporti commerciali • Adempimento di obblighi fiscali o contabili • Attività di consulenza • Gestione contabile o di tesoreria • Gestione dei Clienti (contratti, ordini, arrivi, fatture) • Gestione dei fornitori (contratti, ordini, arrivi, fatture) • Gestione del contenzioso (contratti, ordini, arrivi, fatture)
TIPO DI DATI PERSONALI	• Adesione a partiti od organizzazioni a carattere politico • Codice fiscale ed altri numeri di identificazione personale (carte sanitarie) • Dati identificativi (ragione o denominazione sociale, ovvero nome e cognome delle persone fisiche, indirizzo sede, telefono, fax, e-mail, dati

	fiscali, ecc.) • Dati relativi all'attività economica e commerciale • Documento di identità / Tessera sanitaria • Nominativo, indirizzo o altri elementi di identificazione personale (nome, cognome, età, sesso, luogo e data di nascita, indirizzo privato, indirizzo di lavoro)
CATEGORIE DI INTERESSATI	• Clienti ed utenti • Consulenti e liberi professionisti, anche in forma associata • Enti • Fornitori • Soggetti o organismi pubblici
SUB-RESPONSABILI	

ELENCO ATTIVITA' DI TRATTAMENTO IN CUI È COINVOLTA COME CONTATTO/PERSONA AUTORIZZATA

Il soggetto nominato avrà il compito di trattare i dati personali riferiti alle seguenti attività di trattamento, in cui è coinvolto come contatto/persona autorizzata:

Sede Studio
Gestione Clienti

- Gestione Clienti
  Archivio informazioni relativo alla gestione dei Clienti

Gestione Fornitori

- Gestione dei fornitori
  Gestore dei contratti di fornitura

COMPITI ED ISTRUZIONI PER I RESPONSABILI DEL TRATTAMENTO DEI DATI PERSONALI
in applicazione del considerando art. 28 del Regolamento UE 2016/679 e della normativa nazionale in vigore

PRINCIPI GENERALI DA OSSERVARE
Ogni trattamento di dati personali deve avvenire, nel rispetto primario dei seguenti principi di ordine generale:

per ciascun trattamento di propria competenza, il Responsabile deve fare in modo che siano sempre rispettati i seguenti presupposti:

- i dati devono essere trattati:
  - secondo il principio di liceità, vale a dire conformemente alle disposizioni del Regolamento, nonché alle disposizioni del Codice Civile, per cui, più in particolare, il trattamento non deve essere contrario a norme imperative, all'ordine pubblico ed al buon costume;
  - secondo il principio fondamentale di correttezza, il quale deve ispirare chiunque tratti qualcosa che appartiene alla sfera altrui;

- i dati devono essere raccolti solo per scopi:
  - determinati, vale a dire che non è consentita la raccolta come attività fine a se stessa;
  - espliciti, nel senso che il soggetto interessato va informato sulle finalità del trattamento;
  - legittimi, cioè, oltre al trattamento, come è evidente, anche il fine della raccolta dei dati deve essere lecito;
  - compatibili con il presupposto per il quale sono inizialmente trattati, specialmente nelle operazioni di comunicazione e diffusione degli stessi;

- i dati devono, inoltre, essere:
  - esatti, cioè, precisi e rispondenti al vero e, se necessario, aggiornati;
  - pertinenti, ovvero, il trattamento è consentito soltanto per lo svolgimento delle funzioni istituzionali, in relazione all'attività che viene svolta;
  - completi: non nel senso di raccogliere il maggior numero di informazioni possibili, bensì di contemplare specificamente il concreto interesse e diritto del soggetto interessato;
  - non eccedenti in senso quantitativo rispetto allo scopo perseguito, ovvero devono essere raccolti solo i dati che siano al contempo strettamente necessari e sufficienti in relazione al fine, cioè la cui mancanza risulti di ostacolo al raggiungimento dello scopo stesso;
  - conservati per un periodo non superiore a quello necessario per gli scopi del trattamento e comunque in base alle disposizioni aventi ad oggetto le modalità ed i tempi di conservazione degli atti amministrativi. Trascorso detto periodo i dati vanno resi anonimi o cancellati e la loro comunicazione e diffusione non è più consentita.

In particolare, i dati idonei a rivelare lo stato di salute o la vita sessuale sono conservati separatamente da altri dati personali trattati per finalità che non richiedono il loro utilizzo.
Ciascun trattamento deve, inoltre, avvenire nei limiti imposti dal principio fondamentale di riservatezza e nel rispetto della dignità della persona dell'interessato al trattamento, ovvero deve essere effettuato eliminando ogni occasione di impropria conoscibilità dei dati da parte di terzi.
Se il trattamento di dati è effettuato in violazione dei principi summenzionati e di quanto disposto dal Regolamento è necessario provvedere al "blocco" dei dati stessi, vale a dire alla sospensione temporanea di ogni operazione di trattamento, fino alla regolarizzazione del medesimo trattamento (ad esempio fornendo l'informativa omessa), ovvero alla cancellazione dei dati se non è possibile regolarizzare.

COMPITI PARTICOLARI DEL RESPONSABILE

Lettera di incarico

Il Responsabile del trattamento dei dati personali, operando nell'ambito dei principi sopra ricordati, deve attenersi ai seguenti compiti di carattere particolare, come previsto dall'art.28 e dall'art.30 comma 2 del Regolamento GDPR:

a) identificare e censire i trattamenti di dati personali, le banche dati e gli archivi gestiti con supporti informatici e/o cartacei necessari all'espletamento delle attività istituzionalmente rientranti nella propria sfera di competenza;

b) predisporre il registro delle attività di trattamento da esibire in caso di ispezioni delle Autorità e contenente almeno le seguenti informazioni:
   - il nome e i dati di contatto del Responsabile, del Titolare del trattamento e del Responsabile della protezione dei dati;
   - le categorie dei trattamenti effettuati;
   - se del caso, i trasferimenti di dati personali verso Paesi terzi;
   - descrizione delle misure di sicurezza tecniche ed organizzative applicate a protezione dei dati;

c) definire, per ciascun trattamento di dati personali, la durata del trattamento e la cancellazione o rendere anonimi i dati obsoleti, nel rispetto della normativa vigente in materia di prescrizione e tenuta archivi;

d) ogni qualvolta si raccolgano dati personali, provvedere a che venga fornita l'informativa ai soggetti interessati;

e) assicurare che la comunicazione a terzi e la diffusione dei dati personali avvenga entro i limiti stabiliti per i soggetti pubblici, ovvero, solo se prevista da una norma di legge o regolamento o se comunque necessaria per lo svolgimento di funzioni istituzionali. Così, per i dati relativi ad attività di studio e di ricerca, il Responsabile è tenuto ad attenersi alla disciplina che dispone in merito ai casi in cui è possibile la comunicazione o diffusione anche a privati di dati personali diversi da quelli sensibili e giudiziari;

f) adempiere agli obblighi di sicurezza, quali:
   - adottare, tramite il supporto del Responsabile del Sistema Informativo Aziendale, tutte le preventive misure di sicurezza, ritenute idonee al fine di ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta;
   - definire una politica di sicurezza per assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e servizi afferenti il trattamento dei dati;
   - assicurarsi la capacità di ripristinare tempestivamente la disponibilità e l'accesso ai dati in caso di incidente fisico o tecnico;
   - testare, verificare e valutare regolarmente l'efficacia delle misure tecniche ed organizzative applicate;

g) far osservare gli adempimenti previsti in caso di nuovi trattamenti e cancellazione di trattamenti;

h) su scelta del titolare del trattamento, cancellare o restituirgli tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento e cancellare le copie esistenti, salvo che il diritto dell'Unione o degli Stati membri preveda la conservazione dei dati;

i) collaborare con il Titolare per l'evasione delle richieste degli interessati e delle istanze del Garante per la protezione dei dati personali;

j) garantire che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;

k) collaborare alla individuazione dei soggetti terzi che trattano dati personali di cui è Titolare l'Organizzazione, ai fini della nomina in qualità di Responsabili esterni al trattamento;

l) comunicare tempestivamente al Titolare ogni notizia rilevante ai fini della tutela della riservatezza.

m) dare riscontro preventivo dell'eventuale trasferimento dei dati verso paesi extra UE, la cui normativa non è equiparabile a quella Europea, applicando preventivamente garanzie adeguate a tale trasferimento;

n) ricorrere ad un altro responsabile, per gestire attività di trattamento specifiche, solo previa autorizzazione scritta, specifica o generale, del titolare del trattamento (articolo 28 comma 2 Regolamento GDPR).

Il Responsabile del trattamento risponde al Titolare per ogni violazione o mancata attivazione di quanto previsto dalla normativa in materia di tutela dei dati personali relativamente al settore di competenza.
Resta fermo, in ogni caso, che la responsabilità penale per l'eventuale uso non corretto dei dati oggetto di tutela è a carico della singola persona cui l'uso illegittimo sia imputabile.

L'incarico di Responsabile del trattamento dei dati è attribuito personalmente e non è suscettibile di delega. Esso decade automaticamente alla scadenza o alla revoca dell'incarico affidato.
Per tutto quanto non espressamente previsto nel presente atto, si rinvia alle disposizioni generali vigenti in materia di protezione dei dati personali.

Una copia del presente atto di nomina viene restituita al Titolare, debitamente firmata per accettazione.

Per accettazione dell'incarico
Il Responsabile del trattamento
(S.P.E.E.D. S.n.c. Di Carter & C.)

_____
(firma)

Il titolare del trattamento
(Studio Legale Associato Felicetti Frascarelli Menghini)

_____
(firma)

Lettera di incarico

Trevi, 24/05/2018

Oggetto: Lettera di nomina quale persona autorizzata al trattamento dati

Il/La sottoscritto/a Studio Legale Associato Felicetti Frascarelli Menghini, p.iva 02287020545, titolare del trattamento dei dati dello/a Studio Legale Associato Felicetti Frascarelli Menghini Studio Associato, con sede legale in Piazza della Concordia 1, 06039 Trevi (PG), **conferisce** al Sig.ra Flamini Simona, c.f. FLMSMN78D70D653F, per la sede Sede Studio, Piazza della Concordia 1, 06039 Trevi PG, dalla data del 24/05/2018, l'**incarico** di compiere le operazioni di trattamento di seguito elencate, con l'avvertimento che dovrà operare osservando le direttive del *titolare/responsabile*.

A tal fine, vengono fornite informazioni ed istruzioni per l'assolvimento del compito assegnato:

- il trattamento dei dati deve essere effettuato in modo lecito e corretto;
- i dati personali devono essere raccolti e registrati unicamente per finalità inerenti l'attività svolta;
- è necessaria la verifica costante dei dati ed il loro aggiornamento;
- è necessaria la verifica costante della completezza e pertinenza dei dati trattati;
- devono essere rispettate le misure di sicurezza predisposte dal *titolare/responsabile*;
- in ogni operazione del trattamento deve essere garantita la massima riservatezza ed in particolare:
  a) divieto di comunicazione e/o diffusione dei dati senza la preventiva autorizzazione del *titolare/responsabile*;
  b) l'accesso ai dati dovrà essere limitato all'espletamento delle proprie mansioni ed esclusivamente negli orari di lavoro;
  c) la fase di raccolta del consenso dovrà essere preceduta dalla informativa ed il consenso al trattamento degli interessati rilasciato in forma scritta;
- in caso di interruzione, anche temporanea, del lavoro verificare che i dati trattati non siano accessibili a terzi non autorizzati;
- le proprie credenziali di autenticazione devono essere riservate;
- svolgere le attività previste dai trattamenti secondo le direttive del responsabile del trattamento dei dati; non modificare i trattamenti esistenti o introdurre nuovi trattamenti senza l'esplicita autorizzazione del responsabile del trattamento dei dati;

- rispettare e far rispettare le norme di sicurezza per la protezione dei dati personali;
- informare il responsabile in caso di incidente di sicurezza che coinvolga dati particolari e non;
- raccogliere, registrare e conservare i dati presenti negli atti e documenti contenuti nei fascicoli di studio e nei supporti informatici avendo cura che l'accesso ad essi sia possibile solo ai soggetti autorizzati;
- eseguire qualsiasi altra operazione di trattamento nei limiti delle proprie mansioni e nel rispetto delle norme di legge;
- qualsiasi altra informazione può essere fornita dal Titolare che provvede anche alla formazione.

Gli obblighi relativi alla riservatezza, alla comunicazione ed alla diffusione dovranno essere osservati anche in seguito a modifica dell'incarico e/o cessazione del rapporto di lavoro.

ELENCO ATTIVITA' DI TRATTAMENTO IN CUI È COINVOLTA COME CONTATTO/PERSONA AUTORIZZATA

Sede Studio
Gestione Clienti

- Gestione Clienti
  Archivio informazioni relativo alla gestione dei Clienti

Gestione Fornitori

- Gestione dei fornitori
  Gestore dei contratti di fornitura

Per conoscenza ed accettazione
Persona autorizzata al trattamento dati
(Sig.ra Simona Flamini)

_____
(firma)

Il titolare del trattamento
(Studio Legale Associato Felicetti Frascarelli Menghini)

_____
(firma)

Lettera di incarico

Trevi, 24/05/2018

Oggetto: Lettera di nomina quale persona autorizzata al trattamento dati

Il/La sottoscritto/a Studio Legale Associato Felicetti Frascarelli Menghini, p.iva 02287020545, titolare del trattamento dei dati dello/a Studio Legale Associato Felicetti Frascarelli Menghini Studio Associato, con sede legale in Piazza della Concordia 1, 06039 Trevi (PG), **conferisce** al Avv. Campana Gianluca, c.f. CMPGLC78T25D653M, per la sede Sede Studio, Piazza della Concordia 1, 06039 Trevi PG, dalla data del 24/05/2018, l'**incarico** di compiere le operazioni di trattamento di seguito elencate, con l'avvertimento che dovrà operare osservando le direttive del *titolare/responsabile*.

A tal fine, vengono fornite informazioni ed istruzioni per l'assolvimento del compito assegnato:

- il trattamento dei dati deve essere effettuato in modo lecito e corretto;
- i dati personali devono essere raccolti e registrati unicamente per finalità inerenti l'attività svolta;
- è necessaria la verifica costante dei dati ed il loro aggiornamento;
- è necessaria la verifica costante della completezza e pertinenza dei dati trattati;
- devono essere rispettate le misure di sicurezza predisposte dal *titolare/responsabile*;
- in ogni operazione del trattamento deve essere garantita la massima riservatezza ed in particolare:
  a) divieto di comunicazione e/o diffusione dei dati senza la preventiva autorizzazione del *titolare/responsabile*;
  b) l'accesso ai dati dovrà essere limitato all'espletamento delle proprie mansioni ed esclusivamente negli orari di lavoro;
  c) la fase di raccolta del consenso dovrà essere preceduta dalla informativa ed il consenso al trattamento degli interessati rilasciato in forma scritta;
- in caso di interruzione, anche temporanea, del lavoro verificare che i dati trattati non siano accessibili a terzi non autorizzati;
- le proprie credenziali di autenticazione devono essere riservate;
- svolgere le attività previste dai trattamenti secondo le direttive del responsabile del trattamento dei dati; non modificare i trattamenti esistenti o introdurre nuovi trattamenti senza l'esplicita autorizzazione del responsabile del trattamento dei dati;

- rispettare e far rispettare le norme di sicurezza per la protezione dei dati personali;
- informare il responsabile in caso di incidente di sicurezza che coinvolga dati particolari e non;
- raccogliere, registrare e conservare i dati presenti negli atti e documenti contenuti nei fascicoli di studio e nei supporti informatici avendo cura che l'accesso ad essi sia possibile solo ai soggetti autorizzati;
- eseguire qualsiasi altra operazione di trattamento nei limiti delle proprie mansioni e nel rispetto delle norme di legge;
- qualsiasi altra informazione può essere fornita dal Titolare che provvede anche alla formazione.

Gli obblighi relativi alla riservatezza, alla comunicazione ed alla diffusione dovranno essere osservati anche in seguito a modifica dell'incarico e/o cessazione del rapporto di lavoro.

ELENCO ATTIVITA' DI TRATTAMENTO IN CUI È COINVOLTA COME CONTATTO/PERSONA AUTORIZZATA

Sede Studio
Gestione Clienti

- Gestione Clienti
  Archivio informazioni relativo alla gestione dei Clienti

Gestione Fornitori

- Gestione dei fornitori
  Gestore dei contratti di fornitura

Per conoscenza ed accettazione
Persona autorizzata al trattamento dati
(Avv. Gianluca Campana)

_____
(firma)

Il titolare del trattamento
(Studio Legale Associato Felicetti Frascarelli Menghini)

_____
(firma)

REGISTRO DELLE ATTIVITA'
DI TRATTAMENTO DATI PERSONALI

ai sensi dell'art. 30 del GDPR 2016/679 e della normativa nazionale in vigore

Azienda/Organizzazione	**Studio Legale Associato Felicetti Frascarelli Menghini Studio Associato**

REGISTRO	Gestione Clienti

SEDE	Sede Studio Piazza della Concordia 1, 06039 Trevi - PG

Data revisione: 01/12/2023

Il presente registro è una rappresentazione dell'organizzazione sotto il profilo delle attività di trattamento dati. Esso ha lo scopo di informare, dare consapevolezza e condivisione interna del processo di gestione del dato.

Ai sensi dell'art. 30 del GDPR, il Registro riporta le seguenti informazioni:

- dati di contatto del titolare del trattamento e, dove applicabile, del contitolare del trattamento e del Responsabile della protezione dei dati;
- **finalità del trattamento**, le finalità per le quali sono trattati tali dati;
- categorie di interessati;
- categorie di dati personali;
- categorie di destinatari a cui i dati personali sono stati o saranno comunicati;
- ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale;
- ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
- ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative.

Titolare trattamento dati	Ragione sociale	Studio Legale Associato Felicetti Frascarelli Menghini
	P. Iva	02287020545
	E-mail	
	PEC	
	N° telefono	

Contitolare trattamento dati	Cognome	Felicetti
	Nome	Mauro
	E-mail	mauro.felicetti@studioffm.it
	PEC	mauro.felicetti@avvocatispoleto.legalmail.it
	N° telefono	0742 780573

Contitolare trattamento dati	Cognome	Frascarelli
	Nome	Dimitri
	E-mail	dimitri.frascarelli@studioffm.it
	PEC	dimitri.frascarelli@avvocatispoleto.legalmail.it
	N° telefono	0742 780573

Contitolare trattamento dati	Cognome	Menghini
	Nome	Alberto
	E-mail	alberto.menghini@studioffm.it
	PEC	alberto.menghini@avvocatispoleto.legalmail.it
	N° telefono	0742 780573

VALUTAZIONE DEL RISCHIO E MATRICE DI RISCHIO

Un rischio è uno scenario che descrive un evento e le sue conseguenze, stimato in termini di gravità e probabilità. L'entità dei rischi viene ricavata assegnando un opportuno valore alla **probabilità di accadimento (P)** ed alle **conseguenze** di tale evento **(C)**. Dalla combinazione di tali grandezze si ricava la matrice di rischio la cui entità è data dalla relazione:

LR = P X C

LR = livello di rischio
P = probabilità di accadimento
C = conseguenze

Alla **probabilità di accadimento dell'evento P** è associato un indice numerico rappresentato nella seguente tabella:

PROBABILITA' DELL'EVENTO	
1	Improbabile
2	Poco probabile
3	Probabile
4	M. Probabile
5	Quasi certo

Alle **conseguenze** (C) è associato un indice numerico rappresentato nella seguente tabella:

CONSEGUENZE	
1	Trascurabili
2	Marginali
3	Limitate
4	Gravi
5	Gravissime

MATRICE DEI RISCHI

La matrice che scaturisce dalla combinazione di **probabilità** e **conseguenze** è rappresentata in figura seguente:

Probabilità						
	5	5	10	15	20	25
	4	4	8	12	16	20
	3	3	6	9	12	15
	2	2	4	6	8	10
	1	1	2	3	4	5
		1	2	3	4	5
		Conseguenze				

Entità Rischio	Valori di riferimento
Accettabile	*(1 ≤ **LR** ≤ 3)*
Medio - basso	*(4 ≤ **LR** ≤ 6)*
Rilevante	*(8 ≤ **LR** ≤ 12)*
Alto	*(15 ≤ **LR** ≤ 25)*

Si ricava, così, per ogni attività di trattamento un Livello di Rischio (di potenziale perdita, divulgazione, modifica, distruzione non autorizzata di dati).

ELENCO ATTIVITA' INSERITE NEL REGISTRO

- Gestione Clienti

TRATTAMENTO: Gestione Clienti

Struttura	• Amministrazione • Sede legale • Sede operativa

Personale coinvolto	
Persone autorizzate	Studio Legale Associato Felicetti Frascarelli Menghini (Titolare) S.P.E.E.D. S.n.c. Di Carter & C. (Commercialista) Avv. Menghini Alberto (Titolare, Socio, Rappresentante legale) Avv. Frascarelli Dimitri (Titolare, Socio, Rappresentante legale) Avv. Campana Gianluca (Collaboratore) Avv. Felicetti Mauro (Titolare, Socio, Rappresentante legale) Sig.ra Flamini Simona (Collaboratore)
Partners - Responsabili esterni	Key Seven S.n.c. Di Lallement Eric, p.iva 02469320549 (Fornitore) • Potenziale visione dei dati durante interventi di assistenza tecnica e/o consulenza Anthea S.r.l., p.iva 02513960548 (Fornitore) • Potenziale visione dei dati durante interventi di assistenza tecnica e/o consulenza
Altro	

Processo di trattamento	
Descrizione	Archivio informazioni relativo alla gestione dei Clienti
Fonte dei dati personali	Raccolti direttamente
Base giuridica per il trattamento per dati comuni (art. 6 GDPR)	Contratto
Base giuridica per il trattamento per dati particolari (art. 9 GDPR)	Consenso
Finalità del trattamento	Acquisizione di prove Adempimento di obblighi fiscali o contabili Amministrazione della giustizia (procedimenti giudiziari civili, penali, amministrativi e tributari) Attività di consulenza Compilazione schede di notificazione Contratto di assunzione Difesa del suolo, tutela dell'ambiente e della sicurezza della popolazione Documentazione di beni e patrimoni (tenuta di beni mobili e immobiliari, archivi catastali) Elaborazione, stampa, imbustamento e spedizione delle fatture Erogazione del servizio fornito

	Gestione del contenzioso (contratti, ordini, arrivi, fatture) Gestione del patrimonio mobiliare e immobiliare Gestione del personale per conto dei clienti Gestione della clientela (contratti, ordini, spedizioni e fatture) Informazione scientifica e giuridica Protezione della proprietà Protezione e incolumità degli individui Relazioni con il pubblico Servizi a tutela di consumatori e utenti
Tipo di dati personali	Abitudini di vita o di consumo (viaggi, spostamenti, preferenze o esigenze alimentari) Adesione a partiti od organizzazioni a carattere politico Adesione a sindacati o organizzazioni a carattere sindacale Beni, proprietà, possessi (proprietà, possessi e locazioni; beni e servizi forniti o ottenuti) Codice fiscale ed altri numeri di identificazione personale (carte sanitarie) Convinzioni religiose, adesioni ad organizzazioni a carattere religioso Curriculum di studi e accademico, pubblicazioni, articoli, monografie, relazioni, materiale audiovisivo, titoli di studio, ecc. Dati biometrici Dati identificativi (ragione o denominazione sociale, ovvero nome e cognome delle persone fisiche, indirizzo sede, telefono, fax, e-mail, dati fiscali, ecc.) Dati identificativi dell'orientamento sessuale Dati relativi all'attività economica e commerciale Dati relativi alla famiglia e a situazioni personali Dati relativi alla famiglia e a situazioni personali (stato civile, minori, figli, soggetti a carico, consanguinei, altri appartenenti al nucleo familiare) Documento di identità / Tessera sanitaria Giudiziari Immagini/Video/Audio Indirizzi e-mail Lavoro (occupazione attuale e precedente, informazioni sul reclutamento, sul tirocinio o sulla formazione professionale, informazioni sulla sospensione o interruzione del rapporto di lavoro o sul passaggio ad altra occupazione, curriculum vitae Nome e cognome Nominativo, indirizzo o altri elementi di identificazione personale (nome, cognome, età, sesso, luogo e data di nascita, indirizzo privato, indirizzo di lavoro) Numeri di telefono Opinioni politiche Origini razziali o etniche Particolari (sensibili) Personali Altro
Categorie di interessati	Clienti ed utenti Potenziali clienti Familiari dell'interessato
Categorie di destinatari	Agenzia delle Entrate Altre amministrazioni pubbliche Autorità di vigilanza e controllo Banche e istituti di credito Call center per assistenza clienti Camere di commercio, industria, artigianato ed agricoltura Centrali dei rischi Consulenti e liberi professionisti anche in forma associata Enti bilaterali e casse edili

	Enti locali Enti previdenziali ed assistenziali Enti pubblici economici Enti pubblici non economici Familiari dell'interessato Fondi di assistenza sanitaria integrativa Fondi di previdenza complementare Forze armate Forze di polizia Imprese di assicurazione Interessati Organismi sanitari, personale medico e paramedico Medico competente Ordini e collegi professionali Organi costituzionali o di rilievo costituzionale Organismi paritetici in materia di lavoro Organismi per i collegi professionali Organizzazioni sindacali e patronati Persone autorizzate Rappresentante dei lavoratori per la sicurezza Società che effettuano servizi di recapito postale Società di gestione per il controllo delle frodi Soggetti che svolgono attività di archiviazione della documentazione Studi legali Uffici giudiziari Istituti e scuole di ogni ordine e grado e università
Informativa	Si
Profilazione	Non presente
Dati particolari	Si
Consenso minori	Si
Frequenza trattamento	Giornaliera
Termine cancellazione dati	I dati saranno trattati per tutto il tempo necessario allo svolgimento dell'incarico professionale in essere e per i successivi dieci anni dalla data di cessazione dello stesso.
Trasferimento dati (paesi terzi)	Non presente

Modalità di elaborazione dati: Mista - elettronica e cartacea	
Strumenti	PC Moduli cartacei Posta Elettronica Cellulare Tablet Stampante
Archiviazione	Armadio chiuso a chiave
Strutture informatiche di archiviazione	
PC Mauro	Struttura interna
Sede di riferimento	Sede Studio
Personale con diritti di accesso	Avv. Felicetti Mauro, c.f. FLCMRA53H16D653Y (Titolare, Socio, Rappresentante legale)
Note	
Software utilizzati	
PC Dimitri	Struttura interna
Sede di riferimento	Sede Studio
Personale con diritti di accesso	Avv. Frascarelli Dimitri, c.f. FRSDTR60M12F492M (Titolare, Socio, Rappresentante legale)
Note	PC Marca Nipogi, Mod. AM01

Software utilizzati	
PC Alberto	Struttura interna
Sede di riferimento	Sede Studio
Personale con diritti di accesso	Avv. Menghini Alberto, c.f. MNGLRT65D17D653D (Titolare, Socio, Rappresentante legale)
Note	PC Marca Nipogi, Mod. AM01
Software utilizzati	
PC Gianluca	Struttura interna
Sede di riferimento	Sede Studio
Personale con diritti di accesso	Avv. Campana Gianluca, c.f. CMPGLC78T25D653M (Collaboratore)
Note	
Software utilizzati	
PC Simona	Struttura interna
Sede di riferimento	Sede Studio
Personale con diritti di accesso	Sig.ra Flamini Simona, c.f. FLMSMN78D70D653F (Collaboratore)
Note	
Software utilizzati	
Stampante Multifunzione Canon imageRUNNER ADVANCE C2220i	Struttura interna
Sede di riferimento	Sede Studio
Personale con diritti di accesso	Avv. Felicetti Mauro, c.f. FLCMRA53H16D653Y (Titolare, Socio, Rappresentante legale) Avv. Frascarelli Dimitri, c.f. FRSDTR60M12F492M (Titolare, Socio, Rappresentante legale) Avv. Menghini Alberto, c.f. MNGLRT65D17D653D (Titolare, Socio, Rappresentante legale) Avv. Campana Gianluca, c.f. CMPGLC78T25D653M (Collaboratore) Sig.ra Flamini Simona, c.f. FLMSMN78D70D653F (Collaboratore)
Note	
Software utilizzati	
Stampante Canon i-SENSYS LBP6650dn	Struttura interna
Sede di riferimento	Sede Studio
Personale con diritti di accesso	Avv. Felicetti Mauro, c.f. FLCMRA53H16D653Y (Titolare, Socio, Rappresentante legale) Avv. Frascarelli Dimitri, c.f. FRSDTR60M12F492M (Titolare, Socio, Rappresentante legale) Avv. Menghini Alberto, c.f. MNGLRT65D17D653D (Titolare, Socio, Rappresentante legale) Avv. Campana Gianluca, c.f. CMPGLC78T25D653M (Collaboratore) Sig.ra Flamini Simona, c.f. FLMSMN78D70D653F (Collaboratore)
Note	
Software utilizzati	
Posta elettronica Tin.it	Struttura esterna
Azienda proprietaria	Telecom Italia S.p.a.
Personale con diritti di accesso	Avv. Menghini Alberto, c.f. MNGLRT65D17D653D (Titolare, Socio, Rappresentante legale)

Note	
Software utilizzati	
Dominio / Posta Elettronica "studioffm.it"	Struttura esterna
Azienda proprietaria	Levita S.r.l.
Personale con diritti di accesso	Avv. Felicetti Mauro, c.f. FLCMRA53H16D653Y (Titolare, Socio, Rappresentante legale) Avv. Frascarelli Dimitri, c.f. FRSDTR60M12F492M (Titolare, Socio, Rappresentante legale) Avv. Menghini Alberto, c.f. MNGLRT65D17D653D (Titolare, Socio, Rappresentante legale) Avv. Campana Gianluca, c.f. CMPGLC78T25D653M (Collaboratore) Sig.ra Flamini Simona, c.f. FLMSMN78D70D653F (Collaboratore)
Note	
Software utilizzati	
Posta Elettronica Certificata "avvocatispoleto.legalmail.it"	Struttura esterna
Azienda proprietaria	Infocert S.p.a.
Personale con diritti di accesso	Avv. Felicetti Mauro, c.f. FLCMRA53H16D653Y (Titolare, Socio, Rappresentante legale) Avv. Frascarelli Dimitri, c.f. FRSDTR60M12F492M (Titolare, Socio, Rappresentante legale) Avv. Menghini Alberto, c.f. MNGLRT65D17D653D (Titolare, Socio, Rappresentante legale) Avv. Campana Gianluca, c.f. CMPGLC78T25D653M (Collaboratore) Sig.ra Flamini Simona, c.f. FLMSMN78D70D653F (Collaboratore)
Note	
Software utilizzati	
Nas QNAP	Struttura interna
Sede di riferimento	Sede Studio
Personale con diritti di accesso	Avv. Felicetti Mauro, c.f. FLCMRA53H16D653Y (Titolare, Socio, Rappresentante legale) Avv. Frascarelli Dimitri, c.f. FRSDTR60M12F492M (Titolare, Socio, Rappresentante legale) Avv. Menghini Alberto, c.f. MNGLRT65D17D653D (Titolare, Socio, Rappresentante legale) Avv. Campana Gianluca, c.f. CMPGLC78T25D653M (Collaboratore) Sig.ra Flamini Simona, c.f. FLMSMN78D70D653F (Collaboratore)
Note	
Software utilizzati	
Strutture informatiche di backup	
HD Esterno	Struttura interna
Sede di riferimento	Sede Studio
Frequenza di backup	1 Giorni
Tempo di storicizzazione	7 Giorni
Personale con diritti di accesso	Avv. Felicetti Mauro, c.f. FLCMRA53H16D653Y (Titolare, Socio, Rappresentante legale) Avv. Frascarelli Dimitri, c.f. FRSDTR60M12F492M (Titolare, Socio,

	Rappresentante legale) Avv. Menghini Alberto, c.f. MNGLRT65D17D653D (Titolare, Socio, Rappresentante legale) Avv. Campana Gianluca, c.f. CMPGLC78T25D653M (Collaboratore) Sig.ra Flamini Simona, c.f. FLMSMN78D70D653F (Collaboratore)
Note	
Software utilizzati	
Nas QNAP	Struttura interna
Sede di riferimento	Sede Studio
Frequenza di backup	1 Giorni
Tempo di storicizzazione	7 Giorni
Personale con diritti di accesso	Avv. Felicetti Mauro, c.f. FLCMRA53H16D653Y (Titolare, Socio, Rappresentante legale) Avv. Frascarelli Dimitri, c.f. FRSDTR60M12F492M (Titolare, Socio, Rappresentante legale) Avv. Menghini Alberto, c.f. MNGLRT65D17D653D (Titolare, Socio, Rappresentante legale) Avv. Campana Gianluca, c.f. CMPGLC78T25D653M (Collaboratore) Sig.ra Flamini Simona, c.f. FLMSMN78D70D653F (Collaboratore)
Note	
Software utilizzati	

VALUTAZIONE DEL LIVELLO DI RISCHIO		
PROBABILITÀ	**CONSEGUENZE**	**LIVELLO DI RISCHIO**
Poco probabile	Gravi	Rilevante

MISURE DI SICUREZZA TECNICHE ED ORGANIZZATIVE

- E' applicata una gestione della password degli utenti

Pericoli associati	Rischi
Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)	- Perdita - Distruzione non autorizzata - Modifica non autorizzata - Divulgazione non autorizzata - Accesso dati non autorizzato
Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)	- Perdita - Distruzione non autorizzata - Modifica non autorizzata - Divulgazione non autorizzata - Accesso dati non autorizzato
Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)	- Perdita - Distruzione non autorizzata - Modifica non autorizzata

- E' eseguita la DPIA	
Pericoli associati	**Rischi**
Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)	- Perdita - Distruzione non autorizzata - Modifica non autorizzata - Divulgazione non autorizzata - Accesso dati non autorizzato
Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)	- Perdita - Distruzione non autorizzata - Modifica non autorizzata

- E' presente una politica per la sicurezza e la protezione dei dati	
Pericoli associati	**Rischi**
Eventi naturali (terremoti, eruzioni vulcaniche, ecc.)	- Perdita - Distruzione non autorizzata
Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)	- Perdita - Distruzione non autorizzata - Modifica non autorizzata - Divulgazione non autorizzata - Accesso dati non autorizzato
Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)	- Perdita - Distruzione non autorizzata - Modifica non autorizzata

- I documenti vengono firmati digitalmente	
Pericoli associati	**Rischi**
Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)	- Perdita - Distruzione non autorizzata - Modifica non autorizzata

- Impianto elettrico dotato di misure salvavita atte anche ad evitare cortocircuiti e possibili incendi	
Pericoli associati	**Rischi**
Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.)	- Perdita - Distruzione non autorizzata - Modifica non autorizzata - Divulgazione non autorizzata - Accesso dati non autorizzato
Agenti fisici (incendio, allagamento, attacchi esterni)	- Perdita - Distruzione non autorizzata

- Le password sono costituite da almeno otto caratteri alfanumerici	
Pericoli associati	**Rischi**
Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)	- Perdita - Distruzione non autorizzata - Modifica non autorizzata - Divulgazione non autorizzata

	- Accesso dati non autorizzato
Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)	- Perdita - Distruzione non autorizzata - Modifica non autorizzata

- L'impianto elettrico è certificato ed a norma	
Pericoli associati	**Rischi**
Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.)	- Perdita - Distruzione non autorizzata - Modifica non autorizzata - Divulgazione non autorizzata - Accesso dati non autorizzato
Agenti fisici (incendio, allagamento, attacchi esterni)	- Perdita - Distruzione non autorizzata

- Porte dotate di serratura in tutti i locali contenenti fisicamente le banche dati elettroniche e cartacee	
Pericoli associati	**Rischi**
Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)	- Perdita - Distruzione non autorizzata - Modifica non autorizzata

- Sono definiti i ruoli e le responsabilità	
Pericoli associati	**Rischi**
Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)	- Perdita - Distruzione non autorizzata - Modifica non autorizzata

- Sono definiti i termini di conservazione e le condizioni di impiego dei dati.	
Pericoli associati	**Rischi**
Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)	- Perdita - Distruzione non autorizzata - Modifica non autorizzata
Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)	- Perdita - Distruzione non autorizzata - Modifica non autorizzata - Divulgazione non autorizzata - Accesso dati non autorizzato

- Sono utilizzati software antivirus e anti intrusione	
Pericoli associati	**Rischi**
Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)	- Perdita - Distruzione non autorizzata - Modifica non autorizzata - Divulgazione non autorizzata - Accesso dati non autorizzato
Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)	- Perdita - Distruzione non autorizzata

	- Modifica non autorizzata

- Viene eseguita opportuna manutenzione	
Pericoli associati	**Rischi**
Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)	- Perdita - Distruzione non autorizzata - Modifica non autorizzata - Divulgazione non autorizzata - Accesso dati non autorizzato

REGISTRO DELLE ATTIVITA'
DI TRATTAMENTO DATI PERSONALI

ai sensi dell'art. 30 del GDPR 2016/679 e della normativa nazionale in vigore

Azienda/Organizzazione	**Studio Legale Associato Felicetti Frascarelli Menghini Studio Associato**

REGISTRO	Gestione Fornitori

SEDE	Sede Studio Piazza della Concordia 1, 06039 Trevi - PG

Data revisione: 01/12/2023

Il presente registro è una rappresentazione dell'organizzazione sotto il profilo delle attività di trattamento dati. Esso ha lo scopo di informare, dare consapevolezza e condivisione interna del processo di gestione del dato.

Ai sensi dell'art. 30 del GDPR, il Registro riporta le seguenti informazioni:

- dati di contatto del titolare del trattamento e, dove applicabile, del contitolare del trattamento e del Responsabile della protezione dei dati;
- **finalità del trattamento**, le finalità per le quali sono trattati tali dati;
- categorie di interessati;
- categorie di dati personali;
- categorie di destinatari a cui i dati personali sono stati o saranno comunicati;
- ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale;
- ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
- ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative.

Titolare trattamento dati	Ragione sociale	Studio Legale Associato Felicetti Frascarelli Menghini
	P. Iva	02287020545
	E-mail	
	PEC	
	N° telefono	

Contitolare trattamento dati	Cognome	Felicetti
	Nome	Mauro
	E-mail	mauro.felicetti@studioffm.it
	PEC	mauro.felicetti@avvocatispoleto.legalmail.it
	N° telefono	0742 780573

Contitolare trattamento dati	Cognome	Frascarelli
	Nome	Dimitri
	E-mail	dimitri.frascarelli@studioffm.it
	PEC	dimitri.frascarelli@avvocatispoleto.legalmail.it
	N° telefono	0742 780573

Contitolare trattamento dati	Cognome	Menghini
	Nome	Alberto
	E-mail	alberto.menghini@studioffm.it
	PEC	alberto.menghini@avvocatispoleto.legalmail.it
	N° telefono	0742 780573

VALUTAZIONE DEL RISCHIO E MATRICE DI RISCHIO

Un rischio è uno scenario che descrive un evento e le sue conseguenze, stimato in termini di gravità e probabilità. L'entità dei rischi viene ricavata assegnando un opportuno valore alla **probabilità di accadimento (P)** ed alle **conseguenze** di tale evento **(C)**. Dalla combinazione di tali grandezze si ricava la matrice di rischio la cui entità è data dalla relazione:

LR = P X C

LR = livello di rischio
P = probabilità di accadimento
C = conseguenze

Alla **probabilità di accadimento dell'evento P** è associato un indice numerico rappresentato nella seguente tabella:

PROBABILITA' DELL'EVENTO	
1	Improbabile
2	Poco probabile
3	Probabile
4	M. Probabile
5	Quasi certo

Alle **conseguenze** (C) è associato un indice numerico rappresentato nella seguente tabella:

CONSEGUENZE	
1	Trascurabili
2	Marginali
3	Limitate
4	Gravi
5	Gravissime

MATRICE DEI RISCHI

La matrice che scaturisce dalla combinazione di **probabilità** e **conseguenze** è rappresentata in figura seguente:

Probabilità						
	5	5	10	15	20	25
	4	4	8	12	16	20
	3	3	6	9	12	15
	2	2	4	6	8	10
	1	1	2	3	4	5
		1	2	3	4	5
		Conseguenze				

Entità Rischio	Valori di riferimento
Accettabile	*(1 ≤ **LR** ≤ 3)*
Medio - basso	*(4 ≤ **LR** ≤ 6)*
Rilevante	*(8 ≤ **LR** ≤ 12)*
Alto	*(15 ≤ **LR** ≤ 25)*

Si ricava, così, per ogni attività di trattamento un Livello di Rischio (di potenziale perdita, divulgazione, modifica, distruzione non autorizzata di dati).

ELENCO ATTIVITA' INSERITE NEL REGISTRO

- Gestione dei fornitori

TRATTAMENTO: Gestione dei fornitori

Struttura	• Amministrazione • Sede legale • Sede operativa

Personale coinvolto	
Persone autorizzate	Studio Legale Associato Felicetti Frascarelli Menghini (Titolare) S.P.E.E.D. S.n.c. Di Carter & C. (Commercialista) Avv. Menghini Alberto (Titolare, Socio, Rappresentante legale) Avv. Frascarelli Dimitri (Titolare, Socio, Rappresentante legale) Avv. Campana Gianluca (Collaboratore) Avv. Felicetti Mauro (Titolare, Socio, Rappresentante legale) Sig.ra Flamini Simona (Collaboratore)
Partners - Responsabili esterni	Key Seven S.n.c. Di Lallement Eric, p.iva 02469320549 (Fornitore) • Potenziale visione dei dati durante interventi di assistenza tecnica e/o consulenza Anthea S.r.l., p.iva 02513960548 (Fornitore) • Potenziale visione dei dati durante interventi di assistenza tecnica e/o consulenza
Altro	

Processo di trattamento	
Descrizione	Gestore dei contratti di fornitura
Fonte dei dati personali	Raccolti direttamente
Base giuridica per il trattamento per dati comuni (art. 6 GDPR)	Contratto
Base giuridica per il trattamento per dati particolari (art. 9 GDPR)	
Finalità del trattamento	Adempimento di obblighi di legge connessi a rapporti commerciali Adempimento di obblighi fiscali o contabili Elaborazione, stampa, imbustamento e spedizione delle fatture Erogazione del servizio fornito Gestione dei fornitori (contratti, ordini, arrivi, fatture) Gestione del contenzioso (contratti, ordini, arrivi, fatture)
Tipo di dati personali	Nominativo, indirizzo o altri elementi di identificazione personale (nome, cognome, età, sesso, luogo e data di nascita, indirizzo privato, indirizzo di lavoro) Codice fiscale ed altri numeri di identificazione personale (carte sanitarie) Dati identificativi (ragione o denominazione sociale, ovvero nome e cognome delle persone fisiche, indirizzo sede, telefono, fax, e-

	mail, dati fiscali, ecc.) Dati relativi all'attività economica e commerciale Documento di identità / Tessera sanitaria Indirizzi e-mail Numeri di telefono Nome e cognome
Categorie di interessati	Fornitori
Categorie di destinatari	Banche e istituti di credito Consulenti e liberi professionisti anche in forma associata Società che effettuano servizi di recapito postale Società che effettuano il servizio di logistica di magazzino e trasporto
Informativa	Si
Profilazione	Non presente
Dati particolari	Non presenti
Consenso minori	Non necessario
Frequenza trattamento	Giornaliera
Termine cancellazione dati	I dati saranno trattati per tutto il tempo necessario allo svolgimento del rapporto commerciale in essere e per i successivi dieci anni dalla data di cessazione dello stesso.
Trasferimento dati (paesi terzi)	Non presente

Modalità di elaborazione dati: Mista - elettronica e cartacea	
Strumenti	PC Moduli cartacei Stampante Cellulare Tablet Posta Elettronica
Archiviazione	Armadio chiuso a chiave
Strutture informatiche di archiviazione	
PC Mauro	Struttura interna
Sede di riferimento	Sede Studio
Personale con diritti di accesso	Avv. Felicetti Mauro, c.f. FLCMRA53H16D653Y (Titolare, Socio, Rappresentante legale)
Note	
Software utilizzati	
PC Dimitri	Struttura interna
Sede di riferimento	Sede Studio
Personale con diritti di accesso	Avv. Frascarelli Dimitri, c.f. FRSDTR60M12F492M (Titolare, Socio, Rappresentante legale)
Note	PC Marca Nipogi, Mod. AM01
Software utilizzati	
PC Alberto	Struttura interna
Sede di riferimento	Sede Studio
Personale con diritti di accesso	Avv. Menghini Alberto, c.f. MNGLRT65D17D653D (Titolare, Socio, Rappresentante legale)
Note	PC Marca Nipogi, Mod. AM01
Software utilizzati	
PC Gianluca	Struttura interna
Sede di riferimento	Sede Studio
Personale con diritti di accesso	Avv. Campana Gianluca, c.f. CMPGLC78T25D653M (Collaboratore)

Note	
Software utilizzati	
PC Simona	Struttura interna
Sede di riferimento	Sede Studio
Personale con diritti di accesso	Sig.ra Flamini Simona, c.f. FLMSMN78D70D653F (Collaboratore)
Note	
Software utilizzati	
Nas QNAP	Struttura interna
Sede di riferimento	Sede Studio
Personale con diritti di accesso	Avv. Felicetti Mauro, c.f. FLCMRA53H16D653Y (Titolare, Socio, Rappresentante legale) Avv. Frascarelli Dimitri, c.f. FRSDTR60M12F492M (Titolare, Socio, Rappresentante legale) Avv. Menghini Alberto, c.f. MNGLRT65D17D653D (Titolare, Socio, Rappresentante legale) Avv. Campana Gianluca, c.f. CMPGLC78T25D653M (Collaboratore) Sig.ra Flamini Simona, c.f. FLMSMN78D70D653F (Collaboratore)
Note	
Software utilizzati	
Stampante Multifunzione Canon imageRUNNER ADVANCE C2220i	Struttura interna
Sede di riferimento	Sede Studio
Personale con diritti di accesso	Avv. Felicetti Mauro, c.f. FLCMRA53H16D653Y (Titolare, Socio, Rappresentante legale) Avv. Frascarelli Dimitri, c.f. FRSDTR60M12F492M (Titolare, Socio, Rappresentante legale) Avv. Menghini Alberto, c.f. MNGLRT65D17D653D (Titolare, Socio, Rappresentante legale) Avv. Campana Gianluca, c.f. CMPGLC78T25D653M (Collaboratore) Sig.ra Flamini Simona, c.f. FLMSMN78D70D653F (Collaboratore)
Note	
Software utilizzati	
Stampante Canon i-SENSYS LBP6650dn	Struttura interna
Sede di riferimento	Sede Studio
Personale con diritti di accesso	Avv. Felicetti Mauro, c.f. FLCMRA53H16D653Y (Titolare, Socio, Rappresentante legale) Avv. Frascarelli Dimitri, c.f. FRSDTR60M12F492M (Titolare, Socio, Rappresentante legale) Avv. Menghini Alberto, c.f. MNGLRT65D17D653D (Titolare, Socio, Rappresentante legale) Avv. Campana Gianluca, c.f. CMPGLC78T25D653M (Collaboratore) Sig.ra Flamini Simona, c.f. FLMSMN78D70D653F (Collaboratore)
Note	
Software utilizzati	
Posta elettronica Tin.it	Struttura esterna
Azienda proprietaria	Telecom Italia S.p.a.

Personale con diritti di accesso	Avv. Menghini Alberto, c.f. MNGLRT65D17D653D (Titolare, Socio, Rappresentante legale)
Note	
Software utilizzati	
Dominio / Posta Elettronica "studioffm.it"	Struttura esterna
Azienda proprietaria	Levita S.r.l.
Personale con diritti di accesso	Avv. Felicetti Mauro, c.f. FLCMRA53H16D653Y (Titolare, Socio, Rappresentante legale) Avv. Frascarelli Dimitri, c.f. FRSDTR60M12F492M (Titolare, Socio, Rappresentante legale) Avv. Menghini Alberto, c.f. MNGLRT65D17D653D (Titolare, Socio, Rappresentante legale) Avv. Campana Gianluca, c.f. CMPGLC78T25D653M (Collaboratore) Sig.ra Flamini Simona, c.f. FLMSMN78D70D653F (Collaboratore)
Note	
Software utilizzati	
Posta Elettronica Certificata "avvocatispoleto.legalmail.it"	Struttura esterna
Azienda proprietaria	Infocert S.p.a.
Personale con diritti di accesso	Avv. Felicetti Mauro, c.f. FLCMRA53H16D653Y (Titolare, Socio, Rappresentante legale) Avv. Frascarelli Dimitri, c.f. FRSDTR60M12F492M (Titolare, Socio, Rappresentante legale) Avv. Menghini Alberto, c.f. MNGLRT65D17D653D (Titolare, Socio, Rappresentante legale) Avv. Campana Gianluca, c.f. CMPGLC78T25D653M (Collaboratore) Sig.ra Flamini Simona, c.f. FLMSMN78D70D653F (Collaboratore)
Note	
Software utilizzati	
Strutture informatiche di backup	
Nas QNAP	Struttura interna
Sede di riferimento	Sede Studio
Frequenza di backup	1 Giorni
Tempo di storicizzazione	7 Giorni
Personale con diritti di accesso	Avv. Felicetti Mauro, c.f. FLCMRA53H16D653Y (Titolare, Socio, Rappresentante legale) Avv. Frascarelli Dimitri, c.f. FRSDTR60M12F492M (Titolare, Socio, Rappresentante legale) Avv. Menghini Alberto, c.f. MNGLRT65D17D653D (Titolare, Socio, Rappresentante legale) Avv. Campana Gianluca, c.f. CMPGLC78T25D653M (Collaboratore) Sig.ra Flamini Simona, c.f. FLMSMN78D70D653F (Collaboratore)
Note	
Software utilizzati	
HD Esterno	Struttura interna
Sede di riferimento	Sede Studio

Frequenza di backup	1 Giorni
Tempo di storicizzazione	7 Giorni
Personale con diritti di accesso	Avv. Felicetti Mauro, c.f. FLCMRA53H16D653Y (Titolare, Socio, Rappresentante legale) Avv. Frascarelli Dimitri, c.f. FRSDTR60M12F492M (Titolare, Socio, Rappresentante legale) Avv. Menghini Alberto, c.f. MNGLRT65D17D653D (Titolare, Socio, Rappresentante legale) Avv. Campana Gianluca, c.f. CMPGLC78T25D653M (Collaboratore) Sig.ra Flamini Simona, c.f. FLMSMN78D70D653F (Collaboratore)
Note	
Software utilizzati	

VALUTAZIONE DEL LIVELLO DI RISCHIO		
PROBABILITÀ	**CONSEGUENZE**	**LIVELLO DI RISCHIO**
Poco probabile	Limitate	Medio-basso

MISURE DI SICUREZZA TECNICHE ED ORGANIZZATIVE

- E' applicata una gestione della password degli utenti

Pericoli associati	Rischi
Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)	- Perdita - Distruzione non autorizzata - Modifica non autorizzata - Divulgazione non autorizzata - Accesso dati non autorizzato
Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)	- Perdita - Distruzione non autorizzata - Modifica non autorizzata - Divulgazione non autorizzata - Accesso dati non autorizzato
Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)	- Perdita - Distruzione non autorizzata - Modifica non autorizzata

- E' presente una politica per la sicurezza e la protezione dei dati

Pericoli associati	Rischi
Eventi naturali (terremoti, eruzioni vulcaniche, ecc.)	- Perdita - Distruzione non autorizzata
Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)	- Perdita - Distruzione non autorizzata - Modifica non autorizzata - Divulgazione non autorizzata - Accesso dati non autorizzato
Azioni non autorizzate (Errori volontari o involontari,	- Perdita

virus, uso non autorizzato di strumentazione, ecc.)	- Distruzione non autorizzata - Modifica non autorizzata

- Impianto elettrico dotato di misure salvavita atte anche ad evitare cortocircuiti e possibili incendi	
Pericoli associati	**Rischi**
Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.)	- Perdita - Distruzione non autorizzata - Modifica non autorizzata - Divulgazione non autorizzata - Accesso dati non autorizzato
Agenti fisici (incendio, allagamento, attacchi esterni)	- Perdita - Distruzione non autorizzata

- L'impianto elettrico è certificato ed a norma	
Pericoli associati	**Rischi**
Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.)	- Perdita - Distruzione non autorizzata - Modifica non autorizzata - Divulgazione non autorizzata - Accesso dati non autorizzato
Agenti fisici (incendio, allagamento, attacchi esterni)	- Perdita - Distruzione non autorizzata

- Le password sono costituite da almeno otto caratteri alfanumerici	
Pericoli associati	**Rischi**
Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)	- Perdita - Distruzione non autorizzata - Modifica non autorizzata - Divulgazione non autorizzata - Accesso dati non autorizzato
Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)	- Perdita - Distruzione non autorizzata - Modifica non autorizzata

- Porte dotate di serratura in tutti i locali contenenti fisicamente le banche dati elettroniche e cartacee	
Pericoli associati	**Rischi**
Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)	- Perdita - Distruzione non autorizzata - Modifica non autorizzata

- Sono definiti i ruoli e le responsabilità	
Pericoli associati	**Rischi**
Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)	- Perdita - Distruzione non autorizzata - Modifica non autorizzata

- Sono definiti i termini di conservazione e le condizioni di impiego dei dati.	
Pericoli associati	**Rischi**
Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)	- Perdita - Distruzione non autorizzata - Modifica non autorizzata
Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)	- Perdita - Distruzione non autorizzata - Modifica non autorizzata - Divulgazione non autorizzata - Accesso dati non autorizzato

- Sono utilizzati software antivirus e anti intrusione	
Pericoli associati	**Rischi**
Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)	- Perdita - Distruzione non autorizzata - Modifica non autorizzata - Divulgazione non autorizzata - Accesso dati non autorizzato
Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)	- Perdita - Distruzione non autorizzata - Modifica non autorizzata

- Viene eseguita opportuna manutenzione	
Pericoli associati	**Rischi**
Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)	- Perdita - Distruzione non autorizzata - Modifica non autorizzata - Divulgazione non autorizzata - Accesso dati non autorizzato

VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI

ai sensi del GDPR 2016/679 e normativa nazionale in vigore

Azienda/Organizzazione	**Studio Legale Associato Felicetti Frascarelli Menghini Studio Associato**

TITOLARE	Felicetti Mauro

SEDE	Sede Studio Piazza della Concordia 1, 06039 Trevi - PG

Data revisione: 01/12/2023

VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI

La DPIA, acronimo di Data Protection Impact Assessment, è una valutazione preliminare, eseguita dal titolare del trattamento dei dati personali, relativa agli impatti a cui andrebbe incontro un trattamento laddove dovessero essere violate le misure di protezione dei dati.

In linea con l'approccio basato sul rischio adottato dal regolamento generale sulla protezione dei dati, non è obbligatorio svolgere una valutazione d'impatto sulla protezione dei dati per ciascun trattamento; è necessario realizzare una valutazione d'impatto sulla protezione dei dati soltanto quando la tipologia di trattamento "può presentare un rischio elevato per i diritti e le libertà delle persone fisiche" (articolo 35 del Regolamento 2016/679).

OBBLIGO DPIA

Ai sensi dell'articolo 35, paragrafo 3 del Regolamento 2016/679 la valutazione è stata effettuata nei casi in cui un trattamento può presentare rischi elevati, ossia quando:

a. una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;
b. il trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'articolo 10;
c. la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

CRITERI DA CONSIDERARE PER OBBLIGO DPIA

Nel percorso di analisi sono stati presi in considerazione i seguenti 9 criteri:

1. Valutazione o assegnazione di un punteggio
2. Processo decisionale automatizzato che ha effetto giuridico o incide in modo analogo significativamente
3. Monitoraggio sistematico
4. Dati sensibili o aventi carattere altamente personale
5. Trattamento di dati su larga scala
6. Creazione di corrispondenze o combinazione di insieme di dati
7. Dati relativi ad interessati vulnerabili
8. Uso innovativo o applicazione di nuove soluzioni tecnologiche
9. Trattamento che impedisce agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto

Nel caso in cui un'attività di trattamento dati soddisfa due o più criteri viene eseguita la valutazione d'impatto sulla protezione dei dati.

REVISIONE

Secondo le buone prassi, la valutazione d'impatto sulla protezione dei dati viene

riesaminata continuamente e rivalutata con regolarità.

ALGORITMO VALUTAZIONE

1° STEP: identificazione dei trattamenti

Il primo step consiste nel censire tutte le attività di trattamento di dati personali specificandone:

- dati identificativi (Sede, struttura, funzioni),
- finalità,
- tipologia di dati personali trattati,
- categorie di interessati,
- destinatari,
- modalità di elaborazione dati (cartacea, elettronica, mista),
- termine cancellazione dati,
- eventuale trasferimento paesi terzi,
- misure di sicurezza.

2° STEP: valutazione del rischio e individuazione criteri per DPIA

Un rischio è uno scenario che descrive un evento e le sue conseguenze, stimato in termini di gravità e probabilità. L'entità dei rischi viene ricavata assegnando un opportuno valore alla **probabilità di accadimento (P)** ed alle **conseguenze** di tale evento **(C)**. Dalla combinazione di tali grandezze si ricava la matrice di rischio la cui entità è data dalla relazione:

$$LR = P \times C$$

LR = livello di rischio
P = probabilità di accadimento
C = conseguenze

Alla **probabilità di accadimento dell'evento P** è associato un indice numerico rappresentato nella seguente tabella:

PROBABILITA' DELL'EVENTO	
1	Improbabile
2	Poco probabile
3	Probabile
4	M. Probabile
5	Quasi certo

Alle **conseguenze** (C) è associato un indice numerico rappresentato nella seguente tabella:

CONSEGUENZE	
1	Trascurabili
2	Marginali
3	Limitate
4	Gravi
5	Gravissime

MATRICE DEI RISCHI

La matrice che scaturisce dalla combinazione di **probabilità** e **conseguenze** è rappresentata in figura seguente:

Probabilità						
	5	5	10	15	20	25
	4	4	8	12	16	20
	3	3	6	9	12	15
	2	2	4	6	8	10
	1	1	2	3	4	5
		1	2	3	4	5
		Conseguenze				

Entità Rischio	Valori di riferimento
Accettabile	*(1 ≤ LR ≤ 3)*
Medio - basso	*(4 ≤ LR ≤ 6)*
Rilevante	*(8 ≤ LR ≤ 12)*
Alto	*(15 ≤ LR ≤ 25)*

Si ricava, così, per ogni attività di trattamento un Livello di Rischio (di potenziale perdita, divulgazione, modifica, distruzione non autorizzata di dati).

In questo step viene anche ricercata la presenza di criteri di obbligo DPIA:

1. Valutazione o assegnazione di un punteggio
2. Processo decisionale automatizzato che ha effetto giuridico o incide in modo analogo significativamente
3. Monitoraggio sistematico

4. Dati sensibili o aventi carattere altamente personale
5. Trattamento di dati su larga scala
6. Creazione di corrispondenze o combinazione di insieme di dati
7. Dati relativi ad interessati vulnerabili
8. Uso innovativo o applicazione di nuove soluzioni tecnologiche
9. Trattamento che impedisce agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto

Se vi è presenza di almeno due criteri e/o il Livello di Rischio risulta ALTO, l'attività richiede la DPIA.

3 STEP: DPIA – valutazione del rischio normalizzato

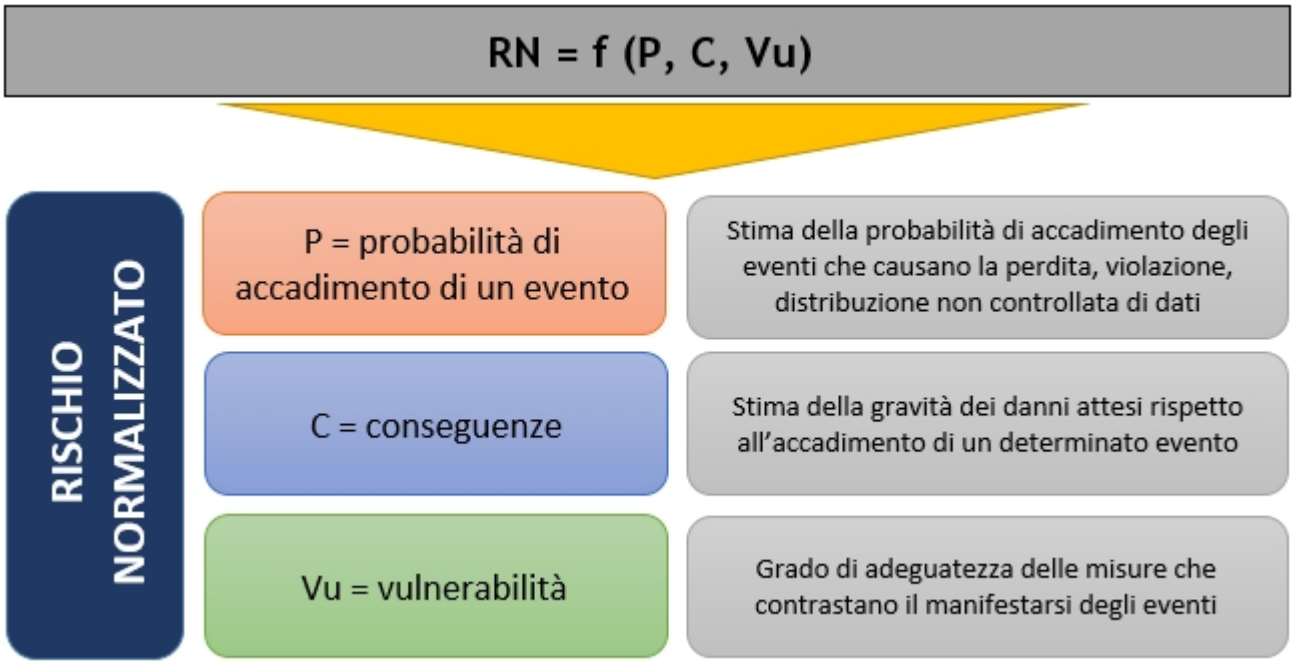
Ai sensi dell'art. 35 del GDPR, vengono individuate tutte le attività di trattamento che in prima analisi presentano un livello di rischio alto e/o prevendono due o più criteri di obbligo DPIA.
Nel caso in cui, quindi, l'indice di rischio si colloca nel range 15 ÷ 25, l'attività necessita di una valutazione di impatto mediante un'analisi approfondita di alcuni aspetti.
La DPIA si basa su un'analisi dei rischi più dettagliata cercando di dare un peso ai possibili controlli applicabili, ricavando, così, un indice di rischio "normalizzato" rispetto al contesto aziendale.

Il rischio viene calcolato in funzione dei 3 fattori seguenti:

RN = f (P, C, Vu)

Dove:

P = probabilità
C = conseguenze generate dall'evento
V = vulnerabilità rispetto al grado di adeguatezza delle misure



In prima battuta viene ricavato il rischio intrinseco Ri come prodotto della

probabilità P e delle conseguenze C, in base agli indici numerici assegnati ad entrambi i fattori.

Alla **probabilità P** è associato un indice numerico rappresentato nella seguente tabella:

Probabilità	
1	Improbabile
2	Poco probabile
3	Probabile
4	Quasi certo

Alle **conseguenze** (C) è associato un indice numerico rappresentato nella seguente tabella:

CONSEGUENZE	
1	Trascurabili
2	Marginali
3	Limitate
4	Gravi

Rispetto al 1 STEP, la matrice ha un range ridotto, essendo una matrice 4 x 4:

PROBABILITÀ	4	4	8	12	16
	3	3	6	9	12
	2	2	4	6	8
	1	1	2	3	4
		1	2	3	4
		CONSEGUENZE			

RISCHIO INTRINSECO	
Ri = P x C	**Valori di riferimento**
Molto basso	*(1 ≤ **Ri** ≤ 2)*
Basso	*(3 ≤ **Ri** ≤ 4)*
Rilevante	*(6 ≤ **Ri** ≤ 9)*
Elevato	*(12 ≤ **Ri** ≤ 16)*

Il rischio intrinseco viene ricavato prendendo in considerazione tutti i possibili Pericoli e Rischi.
Di seguito la suddivisione delle aree di pericolo con i rischi generati.

PERICOLO	RISCHI
Agenti fisici (incendio, allagamento, attacchi esterni)	• Perdita • Distruzione non autorizzata
Eventi naturali (terremoti, eruzioni vulcaniche, ecc.)	• Perdita • Distruzione non autorizzata
Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.)	• Perdita • Distruzione non autorizzata • Modifica non autorizzata • Divulgazione non autorizzata • Accesso dati non autorizzato
Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)	• Perdita • Distruzione non autorizzata • Modifica non autorizzata • Divulgazione non autorizzata • Accesso dati non autorizzato
Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)	• Perdita • Distruzione non autorizzata • Modifica non autorizzata • Divulgazione non autorizzata • Accesso dati non autorizzato
Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)	• Perdita • Distruzione non autorizzata • Modifica non autorizzata • Divulgazione non autorizzata • Accesso dati non autorizzato

Per ricavare il Rischio Normalizzato RN, viene introdotto il fattore Vulnerabilità Vu che fornisce un'indicazione circa l'adeguatezza delle misure di sicurezza attuate per ogni rischio.

Alla **Vulnerabilità** (Vu) è associato un indice numerico rappresentato nella seguente tabella:

VULNERABILITA'		Valore
1	Adeguate	0,25
2	Parzialmente adeguate	0,5
3	Inadeguate	1

Per ogni rischio vengono indicate le misure di sicurezza adottate, per ognuna delle quali viene definito il grado di adeguatezza, assegnando uno dei possibili valori:

- 0,25;
- 0,5;
- 1.

Per ricavare il valore del rischio normalizzato RN viene moltiplicato il Rischio Intrinseco Ri con il valore peggiore assegnato alle misure di sicurezza relativamente a quel rischio.

Vu	1	1 < ***RN*** ≤ 2	3 ≤ ***RN*** ≤ 4	6 ≤ ***RN*** ≤ 9	12 ≤ ***RN*** ≤ 16
	0,5	0,5 < ***RN*** ≤ *1*	1,5 ≤ ***RN*** ≤ 2	3 < ***RN*** ≤ 5	6 ≤ ***RN*** ≤ 8
	0,25	0,25 ≤ ***RN*** ≤ 0,5	0,75 ≤ ***RN*** ≤ 1	1,5 ≤ ***RN*** < 3	3 ≤ ***RN*** ≤ 4
		1 ≤ ***Ri*** ≤ 2	3 ≤ ***Ri*** ≤ 4	6 ≤ ***Ri*** ≤ 9	12 ≤ ***Ri*** ≤ 16
		Ri			

RISCHIO NORMALIZZATO	
RN = Ri x Vu	Valori di riferimento
Molto basso	0,25 ≤ ***RN*** ≤ 1
Basso	1 < ***RN*** < 3
Rilevante	3 ≤ ***RN*** ≤ 9
Elevato	12 ≤ ***RN*** ≤ 16

Se, a valle dell'analisi DPIA, l'attività ricade comunque in fascia **ALTA**, il Titolare attiva l'iter di consultazione del Garante.

RISULTATI DPIA

Di seguito, viene riportata l'analisi di tutte le attività di trattamento per cui si è resa necessaria la valutazione di impatto sulla protezione dei dati.

Elenco attività sottoposte a DPIA

- Gestione Clienti - Gestione Clienti - Titolare del trattamento

Gestione Clienti - Gestione Clienti - Titolare del trattamento

Struttura	• Amministrazione • Sede legale • Sede operativa

Personale coinvolto	
Titolare del trattamento	Studio Legale Associato Felicetti Frascarelli Menghini
Persone autorizzate	Studio Legale Associato Felicetti Frascarelli Menghini, p.iva 02287020545 S.P.E.E.D. S.n.c. Di Carter & C., p.iva 01576100547 Avv. Menghini Alberto, c.f. MNGLRT65D17D653D Avv. Frascarelli Dimitri, c.f. FRSDTR60M12F492M Avv. Campana Gianluca, c.f. CMPGLC78T25D653M Avv. Felicetti Mauro, c.f. FLCMRA53H16D653Y Sig.ra Flamini Simona, c.f. FLMSMN78D70D653F
Partners - Responsabili esterni	Key Seven S.n.c. Di Lallement Eric, p.iva 02469320549 • Potenziale visione dei dati durante interventi di assistenza tecnica e/o consulenza Anthea S.r.l., p.iva 02513960548 • Potenziale visione dei dati durante interventi di assistenza tecnica e/o consulenza
Altro	

Processo di trattamento	
Descrizione	Archivio informazioni relativo alla gestione dei Clienti
Fonte dei dati personali	Raccolti direttamente
Base giuridica per il trattamento per dati comuni (art. 6 GDPR)	Contratto
Base giuridica per il trattamento per dati particolari (art. 9 GDPR)	Consenso
Finalità del trattamento	Acquisizione di prove Adempimento di obblighi fiscali o contabili Amministrazione della giustizia (procedimenti giudiziari civili, penali, amministrativi e tributari) Attività di consulenza

	Compilazione schede di notificazione Contratto di assunzione Difesa del suolo, tutela dell'ambiente e della sicurezza della popolazione Documentazione di beni e patrimoni (tenuta di beni mobili e immobiliari, archivi catastali) Elaborazione, stampa, imbustamento e spedizione delle fatture Erogazione del servizio fornito Gestione del contenzioso (contratti, ordini, arrivi, fatture) Gestione del patrimonio mobiliare e immobiliare Gestione del personale per conto dei clienti Gestione della clientela (contratti, ordini, spedizioni e fatture) Informazione scientifica e giuridica Protezione della proprietà Protezione e incolumità degli individui Relazioni con il pubblico Servizi a tutela di consumatori e utenti
Tipo di dati personali	Abitudini di vita o di consumo (viaggi, spostamenti, preferenze o esigenze alimentari) Adesione a partiti od organizzazioni a carattere politico Adesione a sindacati o organizzazioni a carattere sindacale Beni, proprietà, possessi (proprietà, possessi e locazioni; beni e servizi forniti o ottenuti) Codice fiscale ed altri numeri di identificazione personale (carte sanitarie) Convinzioni religiose, adesioni ad organizzazioni a carattere religioso Curriculum di studi e accademico, pubblicazioni, articoli, monografie, relazioni, materiale audiovisivo, titoli di studio, ecc. Dati biometrici Dati identificativi (ragione o denominazione sociale, ovvero nome e cognome delle persone fisiche, indirizzo sede, telefono, fax, e-mail, dati fiscali, ecc.) Dati identificativi dell'orientamento sessuale Dati relativi all'attività economica e commerciale Dati relativi alla famiglia e a situazioni personali Dati relativi alla famiglia e a situazioni personali (stato civile, minori, figli, soggetti a carico, consanguinei, altri appartenenti al nucleo familiare) Documento di identità / Tessera sanitaria Giudiziari Immagini/Video/Audio Indirizzi e-mail Lavoro (occupazione attuale e precedente, informazioni sul reclutamento, sul tirocinio o sulla formazione professionale, informazioni sulla sospensione o interruzione del rapporto di lavoro o sul passaggio ad altra occupazione, curriculum vitae Nome e cognome Nominativo, indirizzo o altri elementi di identificazione personale (nome, cognome, età, sesso, luogo e data di nascita, indirizzo privato, indirizzo di lavoro) Numeri di telefono Opinioni politiche Origini razziali o etniche Particolari (sensibili) Personali Altro
Categorie di interessati	Clienti ed utenti Potenziali clienti Familiari dell'interessato

Categorie di destinatari	Agenzia delle Entrate Altre amministrazioni pubbliche Autorità di vigilanza e controllo Banche e istituti di credito Call center per assistenza clienti Camere di commercio, industria, artigianato ed agricoltura Centrali dei rischi Consulenti e liberi professionisti anche in forma associata Enti bilaterali e casse edili Enti locali Enti previdenziali ed assistenziali Enti pubblici economici Enti pubblici non economici Familiari dell'interessato Fondi di assistenza sanitaria integrativa Fondi di previdenza complementare Forze armate Forze di polizia Imprese di assicurazione Interessati Organismi sanitari, personale medico e paramedico Medico competente Ordini e collegi professionali Organi costituzionali o di rilievo costituzionale Organismi paritetici in materia di lavoro Organismi per i collegi professionali Organizzazioni sindacali e patronati Persone autorizzate Rappresentante dei lavoratori per la sicurezza Società che effettuano servizi di recapito postale Società di gestione per il controllo delle frodi Soggetti che svolgono attività di archiviazione della documentazione Studi legali Uffici giudiziari Istituti e scuole di ogni ordine e grado e università
Informativa	Si
Profilazione	Non necessario
Dati particolari	Si
Consenso minori	Si
Frequenza trattamento	Giornaliera
Termine cancellazione dati	I dati saranno trattati per tutto il tempo necessario allo svolgimento dell'incarico professionale in essere e per i successivi dieci anni dalla data di cessazione dello stesso.
Trasferimento dati (paesi terzi)	No
Autorizzazione del Garante	Non presente

Modalità di elaborazione dati: Mista - elettronica e cartacea	
Strumenti	PC Moduli cartacei Posta Elettronica Cellulare Tablet Stampante
Strutture informatiche di archiviazione	
PC Mauro	Struttura interna
Sede di riferimento	Sede Studio
Personale con diritti di accesso	Avv. Felicetti Mauro, c.f. FLCMRA53H16D653Y

Software utilizzati	
PC Dimitri	Struttura interna
Sede di riferimento	Sede Studio
Personale con diritti di accesso	Avv. Frascarelli Dimitri, c.f. FRSDTR60M12F492M
Software utilizzati	
PC Alberto	Struttura interna
Sede di riferimento	Sede Studio
Personale con diritti di accesso	Avv. Menghini Alberto, c.f. MNGLRT65D17D653D
Software utilizzati	
PC Gianluca	Struttura interna
Sede di riferimento	Sede Studio
Personale con diritti di accesso	Avv. Campana Gianluca, c.f. CMPGLC78T25D653M
Software utilizzati	
PC Simona	Struttura interna
Sede di riferimento	Sede Studio
Personale con diritti di accesso	Sig.ra Flamini Simona, c.f. FLMSMN78D70D653F
Software utilizzati	
Stampante Multifunzione Canon imageRUNNER ADVANCE C2220i	Struttura interna
Sede di riferimento	Sede Studio
Personale con diritti di accesso	Avv. Felicetti Mauro, c.f. FLCMRA53H16D653Y Avv. Frascarelli Dimitri, c.f. FRSDTR60M12F492M Avv. Menghini Alberto, c.f. MNGLRT65D17D653D Avv. Campana Gianluca, c.f. CMPGLC78T25D653M Sig.ra Flamini Simona, c.f. FLMSMN78D70D653F
Software utilizzati	
Stampante Canon i-SENSYS LBP6650dn	Struttura interna
Sede di riferimento	Sede Studio
Personale con diritti di accesso	Avv. Felicetti Mauro, c.f. FLCMRA53H16D653Y Avv. Frascarelli Dimitri, c.f. FRSDTR60M12F492M Avv. Menghini Alberto, c.f. MNGLRT65D17D653D Avv. Campana Gianluca, c.f. CMPGLC78T25D653M Sig.ra Flamini Simona, c.f. FLMSMN78D70D653F
Software utilizzati	
Posta elettronica Tin.it	Struttura esterna
Azienda proprietaria	Telecom Italia S.p.a.
Personale con diritti di accesso	Avv. Menghini Alberto, c.f. MNGLRT65D17D653D
Software utilizzati	
Dominio / Posta Elettronica "studioffm.it"	Struttura esterna
Azienda proprietaria	Levita S.r.l.
Personale con diritti di accesso	Avv. Felicetti Mauro, c.f. FLCMRA53H16D653Y Avv. Frascarelli Dimitri, c.f. FRSDTR60M12F492M Avv. Menghini Alberto, c.f. MNGLRT65D17D653D Avv. Campana Gianluca, c.f. CMPGLC78T25D653M Sig.ra Flamini Simona, c.f. FLMSMN78D70D653F
Software utilizzati	
Posta Elettronica Certificata "avvocatispoleto.legalmail.it"	Struttura esterna
Azienda proprietaria	Infocert S.p.a.
Personale con diritti di accesso	Avv. Felicetti Mauro, c.f. FLCMRA53H16D653Y Avv. Frascarelli Dimitri, c.f. FRSDTR60M12F492M Avv. Menghini Alberto, c.f. MNGLRT65D17D653D Avv. Campana Gianluca, c.f. CMPGLC78T25D653M Sig.ra Flamini Simona, c.f. FLMSMN78D70D653F

Software utilizzati	
Nas QNAP	Struttura interna
Sede di riferimento	Sede Studio
Personale con diritti di accesso	Avv. Felicetti Mauro, c.f. FLCMRA53H16D653Y Avv. Frascarelli Dimitri, c.f. FRSDTR60M12F492M Avv. Menghini Alberto, c.f. MNGLRT65D17D653D Avv. Campana Gianluca, c.f. CMPGLC78T25D653M Sig.ra Flamini Simona, c.f. FLMSMN78D70D653F
Software utilizzati	
Strutture informatiche di backup	
HD Esterno	Struttura interna
Sede di riferimento	Sede Studio
Frequenza di backup	1 Giorni
Tempo di storicizzazione	7 Giorni
Personale con diritti di accesso	Avv. Felicetti Mauro, c.f. FLCMRA53H16D653Y Avv. Frascarelli Dimitri, c.f. FRSDTR60M12F492M Avv. Menghini Alberto, c.f. MNGLRT65D17D653D Avv. Campana Gianluca, c.f. CMPGLC78T25D653M Sig.ra Flamini Simona, c.f. FLMSMN78D70D653F
Note	
Software utilizzati	
Nas QNAP	Struttura interna
Sede di riferimento	Sede Studio
Frequenza di backup	1 Giorni
Tempo di storicizzazione	7 Giorni
Personale con diritti di accesso	Avv. Felicetti Mauro, c.f. FLCMRA53H16D653Y Avv. Frascarelli Dimitri, c.f. FRSDTR60M12F492M Avv. Menghini Alberto, c.f. MNGLRT65D17D653D Avv. Campana Gianluca, c.f. CMPGLC78T25D653M Sig.ra Flamini Simona, c.f. FLMSMN78D70D653F
Note	
Software utilizzati	

VALUTAZIONE DEL LIVELLO DI RISCHIO		
PROBABILITÀ	**CONSEGUENZE**	**LIVELLO DI RISCHIO**
Poco probabile	Gravi	Rilevante

MISURE DI SICUREZZA TECNICHE ED ORGANIZZATIVE

- E' applicata una gestione della password degli utenti
- E' eseguita la DPIA
- E' presente una politica per la sicurezza e la protezione dei dati
- I documenti vengono firmati digitalmente
- Impianto elettrico dotato di misure salvavita atte anche ad evitare cortocircuiti e possibili incendi
- Le password sono costituite da almeno otto caratteri alfanumerici
- L'impianto elettrico è certificato ed a norma
- Porte dotate di serratura in tutti i locali contenenti fisicamente le banche dati elettroniche e cartacee
- Sono definiti i ruoli e le responsabilità
- Sono definiti i termini di conservazione e le condizioni di impiego dei dati.
- Sono utilizzati software antivirus e anti intrusione
- Viene eseguita opportuna manutenzione

VALUTAZIONE ADEGUATEZZA DELLE MISURE DI SICUREZZA ADOTTATE

MISURE DI SICUREZZA	PERICOLI ASSOCIATI	LIVELLO DI ADEGUATEZZA
E' applicata una gestione della password degli utenti	• Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT) • Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.) • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)	Adeguate
E' eseguita la DPIA	• Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.) • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)	Adeguate
E' presente una politica per la sicurezza e la protezione dei dati	• Eventi naturali (terremoti, eruzioni vulcaniche, ecc.) • Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.) • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)	Adeguate
I documenti vengono firmati digitalmente	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)	Adeguate
Impianto elettrico dotato di misure salvavita atte anche ad evitare	• Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione	Adeguate

cortocircuiti e possibili incendi	collegamenti di rete, ecc.) • Agenti fisici (incendio, allagamento, attacchi esterni)	
Le password sono costituite da almeno otto caratteri alfanumerici	• Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.) • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)	Adeguate
L'impianto elettrico è certificato ed a norma	• Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.) • Agenti fisici (incendio, allagamento, attacchi esterni)	Adeguate
Porte dotate di serratura in tutti i locali contenenti fisicamente le banche dati elettroniche e cartacee	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)	Adeguate
Sono definiti i ruoli e le responsabilità	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)	Adeguate
Sono definiti i termini di conservazione e le condizioni di impiego dei dati.	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)	Adeguate
Sono utilizzati software antivirus e anti intrusione	• Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.) • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione,	Adeguate

	ecc.)	
Viene eseguita opportuna manutenzione	• Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)	Adeguate

VALUTAZIONE DEI RISCHI

PERICOLO		
Agenti fisici (incendio, allagamento, attacchi esterni)		
RISCHI		
• Perdita • Distruzione non autorizzata		
VALUTAZIONE RISCHIO INTRINSECO		
Probabilità	**Conseguenza**	**Rischio intrinseco - Ri**
Poco probabile	Limitate	Rilevante
VALUTAZIONE RISCHIO NORMALIZZATO *Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi*		
Rischio intrinseco - Ri	**Vulnerabilità - Vu**	**Rischio normalizzato - RN**
Rilevante	0,25	Basso

PERICOLO		
Eventi naturali (terremoti, eruzioni vulcaniche, ecc.)		
RISCHI		
• Perdita • Distruzione non autorizzata		
VALUTAZIONE RISCHIO INTRINSECO		
Probabilità	**Conseguenza**	**Rischio intrinseco - Ri**
Poco probabile	Limitate	Rilevante
VALUTAZIONE RISCHIO NORMALIZZATO *Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi*		
Rischio intrinseco - Ri	**Vulnerabilità - Vu**	**Rischio normalizzato - RN**
Rilevante	0,25	Basso

PERICOLO
Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.)
RISCHI
• Perdita

- Distruzione non autorizzata
- Modifica non autorizzata
- Divulgazione non autorizzata
- Accesso dati non autorizzato

VALUTAZIONE RISCHIO INTRINSECO		
Probabilità	**Conseguenza**	**Rischio intrinseco - Ri**
Poco probabile	Gravi	Rilevante

VALUTAZIONE RISCHIO NORMALIZZATO *Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi*		
Rischio intrinseco - Ri	**Vulnerabilità - Vu**	**Rischio normalizzato - RN**
Rilevante	0,25	Basso

PERICOLO
Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)

RISCHI

- Perdita
- Distruzione non autorizzata
- Modifica non autorizzata
- Divulgazione non autorizzata
- Accesso dati non autorizzato

VALUTAZIONE RISCHIO INTRINSECO		
Probabilità	**Conseguenza**	**Rischio intrinseco - Ri**
Poco probabile	Gravi	Rilevante

VALUTAZIONE RISCHIO NORMALIZZATO *Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi*		
Rischio intrinseco - Ri	**Vulnerabilità - Vu**	**Rischio normalizzato - RN**
Rilevante	0,25	Basso

PERICOLO
Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)

RISCHI

- Perdita
- Distruzione non autorizzata
- Modifica non autorizzata
- Divulgazione non autorizzata
- Accesso dati non autorizzato

VALUTAZIONE RISCHIO INTRINSECO		
Probabilità	**Conseguenza**	**Rischio intrinseco - Ri**
Poco probabile	Gravi	Rilevante

VALUTAZIONE RISCHIO NORMALIZZATO *Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi*		
Rischio intrinseco - Ri	**Vulnerabilità - Vu**	**Rischio normalizzato - RN**
Rilevante	0,25	Basso

PERICOLO		
Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)		
RISCHI		
• Perdita • Distruzione non autorizzata • Modifica non autorizzata		
VALUTAZIONE RISCHIO INTRINSECO		
Probabilità	**Conseguenza**	**Rischio intrinseco - Ri**
Poco probabile	Gravi	Rilevante
VALUTAZIONE RISCHIO NORMALIZZATO *Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi*		
Rischio intrinseco - Ri	**Vulnerabilità - Vu**	**Rischio normalizzato - RN**
Rilevante	0,25	Basso

A valle della DPIA l'attività risulta a rischio **Basso**

ANAGRAFICA AZIENDA

Azienda/Organizzazione	**Studio Legale Associato Felicetti Frascarelli Menghini Studio Associato**

SEDE LEGALE	Sede Studio Piazza della Concordia 1, 06039 Trevi - PG

Data revisione: 01/12/2023

DATI AZIENDA

Ragione Sociale	**Studio Legale Associato Felicetti Frascarelli Menghini Studio Associato**
Partita IVA	02287020545
Codice fiscale	02287020545
Sede legale	Piazza della Concordia 1, 06039 Trevi - PG
Contatti	- Tel: 0742 780573 - Email: studio.ffm@tin.it - PEC: dimitri.frascarelli@avvocatispoleto.legalmail.it
Sito web	
Attività economica	Studio Legale
Codici ATECO	• 69.10.10 - Attività degli studi legali
Rappresentante legale	Felicetti Mauro
Codice fiscale	FLCMRA53H16D653Y
Contatti	- Email: mauro.felicetti@studioffm.it - PEC: mauro.felicetti@avvocatispoleto.legalmail.it

SEDI

Nome	**SEDE STUDIO**
Tipo	- Legale - Amministrativa - Operativa
Indirizzo	Piazza della Concordia 1, 06039 Trevi - PG

NOMINE

Soggetto	Studio Legale Associato Felicetti Frascarelli Menghini, p.iva 02287020545
Contatti	
Nomina	**Titolare del trattamento** Sede: Sede Studio

Soggetto	S.P.E.E.D. S.n.c. Di Carter & C., p.iva 01576100547
Contatti	
Nomina	**Responsabile del trattamento esterno** Sede: Sede Studio

Soggetto	, nella persona di Campana Gianluca
Contatti	- Tel: 0742 780573 - Email: gianluca.campana@studio.ffm.it - PEC: gianluca.campana@avvocatispoleto.legalmail.it
Nomina	**Persona autorizzata** Sede: Sede Studio

Soggetto	, nella persona di Felicetti Mauro
Contatti	- Tel: 0742 780573 - Email: mauro.felicetti@studioffm.it

	- PEC: mauro.felicetti@avvocatispoleto.legalmail.it
Nomina	**Contitolare** Sede: Sede Studio

Soggetto	, nella persona di Flamini Simona
Contatti	- Tel: 347 5221946 - Email: simona.flamini@studioffm.it
Nomina	**Persona autorizzata** Sede: Sede Studio

Soggetto	, nella persona di Frascarelli Dimitri
Contatti	- Tel: 0742 780573 - Email: dimitri.frascarelli@studioffm.it - PEC: dimitri.frascarelli@avvocatispoleto.legalmail.it
Nomina	**Contitolare** Sede: Sede Studio

Soggetto	, nella persona di Menghini Alberto
Contatti	- Tel: 0742 780573 - Email: alberto.menghini@studioffm.it - PEC: alberto.menghini@avvocatispoleto.legalmail.it
Nomina	**Contitolare** Sede: Sede Studio

PARTNERS

Nominativo	Campana Gianluca
Tipo Partner	Partner/fornitore
Partita IVA	
Codice fiscale	CMPGLC78T25D653M
Indirizzo residenza	Via Madonna 9, 06039 Trevi - PG
Contatti	- Tel: 0742 780573 - Email: gianluca.campana@studio.ffm.it - PEC: gianluca.campana@avvocatispoleto.legalmail.it

Nominativo	S.P.E.E.D. S.n.c. Di Carter & C.
Tipo Partner	Partner/fornitore
Partita IVA	01576100547
Codice fiscale	
Indirizzo sede legale	Via del Risorgimento 14, 06049 Spoleto - PG
Contatti	

Nominativo	Anthea S.r.l.
Tipo Partner	Partner/fornitore
Partita IVA	02513960548
Codice fiscale	
Indirizzo sede legale	Via Enrico Giustozzi , 06034 Foligno - PG
Contatti	

Nominativo	Key Seven S.n.c. Di Lallement Eric
Tipo Partner	Partner/fornitore
Partita IVA	02469320549
Codice fiscale	
Indirizzo sede legale	Via delle Industrie 60, 06034 Foligno - PG
Contatti	

Nominativo	Flamini Simona
Tipo Partner	Partner/fornitore
Partita IVA	
Codice fiscale	FLMSMN78D70D653F
Indirizzo residenza	Via Martiri della Resistenza 21, 06039 Trevi - PG
Contatti	- Tel: 347 5221946 - Email: simona.flamini@studioffm.it

ARCHIVI INFORMATICI

Nome	**PC Mauro**
Tipo Struttura	Interna
Sede	Sede Studio (Trevi)
Personale con diritti di accesso	Avv. Felicetti Mauro, c.f. FLCMRA53H16D653Y
Note	
Software utilizzati	

Nome	**PC Dimitri**
Tipo Struttura	Interna
Sede	Sede Studio (Trevi)
Personale con diritti di accesso	Avv. Frascarelli Dimitri, c.f. FRSDTR60M12F492M
Note	PC Marca Nipogi, Mod. AM01
Software utilizzati	

Nome	**PC Alberto**
Tipo Struttura	Interna
Sede	Sede Studio (Trevi)
Personale con diritti di accesso	Avv. Menghini Alberto, c.f. MNGLRT65D17D653D
Note	PC Marca Nipogi, Mod. AM01
Software utilizzati	

Nome	**PC Gianluca**
Tipo Struttura	Interna
Sede	Sede Studio (Trevi)
Personale con diritti di accesso	Avv. Campana Gianluca, c.f. CMPGLC78T25D653M
Note	

Software utilizzati	

Nome	**Nas QNAP**
Tipo Struttura	Interna
Sede	Sede Studio (Trevi)
Personale con diritti di accesso	Avv. Felicetti Mauro, c.f. FLCMRA53H16D653Y Avv. Frascarelli Dimitri, c.f. FRSDTR60M12F492M Avv. Menghini Alberto, c.f. MNGLRT65D17D653D Avv. Campana Gianluca, c.f. CMPGLC78T25D653M Sig.ra Flamini Simona, c.f. FLMSMN78D70D653F
Note	
Software utilizzati	

Nome	**Stampante Multifunzione Canon imageRUNNER ADVANCE C2220i**
Tipo Struttura	Interna
Sede	Sede Studio (Trevi)
Personale con diritti di accesso	Avv. Felicetti Mauro, c.f. FLCMRA53H16D653Y Avv. Frascarelli Dimitri, c.f. FRSDTR60M12F492M Avv. Menghini Alberto, c.f. MNGLRT65D17D653D Avv. Campana Gianluca, c.f. CMPGLC78T25D653M Sig.ra Flamini Simona, c.f. FLMSMN78D70D653F
Note	
Software utilizzati	

Nome	**PC Simona**
Tipo Struttura	Interna
Sede	Sede Studio (Trevi)
Personale con diritti di accesso	Sig.ra Flamini Simona, c.f. FLMSMN78D70D653F
Note	
Software utilizzati	

Nome	**Stampante Canon i-SENSYS LBP6650dn**
Tipo Struttura	Interna
Sede	Sede Studio (Trevi)
Personale con diritti di accesso	Avv. Felicetti Mauro, c.f. FLCMRA53H16D653Y Avv. Frascarelli Dimitri, c.f. FRSDTR60M12F492M Avv. Menghini Alberto, c.f. MNGLRT65D17D653D Avv. Campana Gianluca, c.f. CMPGLC78T25D653M Sig.ra Flamini Simona, c.f. FLMSMN78D70D653F
Note	
Software utilizzati	

Nome	**HD Esterno**
Tipo Struttura	Interna
Sede	Sede Studio (Trevi)
Personale con diritti di accesso	Avv. Felicetti Mauro, c.f. FLCMRA53H16D653Y Avv. Frascarelli Dimitri, c.f. FRSDTR60M12F492M Avv. Menghini Alberto, c.f. MNGLRT65D17D653D Avv. Campana Gianluca, c.f. CMPGLC78T25D653M Sig.ra Flamini Simona, c.f. FLMSMN78D70D653F

Note	
Software utilizzati	

Nome	**Posta elettronica Tin.it**
Tipo Struttura	Esterna
Azienda	Telecom Italia S.p.a.
Personale con diritti di accesso	Avv. Menghini Alberto, c.f. MNGLRT65D17D653D
Note	
Software utilizzati	

Nome	**Dominio / Posta Elettronica "studioffm.it"**
Tipo Struttura	Esterna
Azienda	Levita S.r.l.
Personale con diritti di accesso	Avv. Felicetti Mauro, c.f. FLCMRA53H16D653Y Avv. Frascarelli Dimitri, c.f. FRSDTR60M12F492M Avv. Menghini Alberto, c.f. MNGLRT65D17D653D Avv. Campana Gianluca, c.f. CMPGLC78T25D653M Sig.ra Flamini Simona, c.f. FLMSMN78D70D653F
Note	
Software utilizzati	

Nome	**Posta Elettronica Certificata "avvocatispoleto.legalmail.it"**
Tipo Struttura	Esterna
Azienda	Infocert S.p.a.
Personale con diritti di accesso	Avv. Felicetti Mauro, c.f. FLCMRA53H16D653Y Avv. Frascarelli Dimitri, c.f. FRSDTR60M12F492M Avv. Menghini Alberto, c.f. MNGLRT65D17D653D Avv. Campana Gianluca, c.f. CMPGLC78T25D653M Sig.ra Flamini Simona, c.f. FLMSMN78D70D653F
Note	
Software utilizzati	

ORGANIGRAMMA GDPR

Azienda/Organizzazione	**Studio Legale Associato Felicetti Frascarelli Menghini Studio Associato**

SEDE LEGALE	Sede Studio Piazza della Concordia 1, 06039 Trevi - PG

Data revisione: 01/12/2023

Di seguito, è riportato l'organigramma con le funzioni nominate per la gestione della protezione del trattamento dati personali:

SEDE SEDE STUDIO

Titolare del trattamento:	Studio Legale Associato Felicetti Frascarelli Menghini	Data nomina: 24/05/2018

Contitolare del trattamento:	Felicetti**Mauro**	Data nomina: 24/05/2018
	Frascarelli**Dimitri**	Data nomina: 24/05/2018
	Menghini**Alberto**	Data nomina: 24/05/2018

Responsabili esterni del trattamento:	S.P.E.E.D. S.n.c. Di Carter & C.	Data nomina: 24/05/2018

Persone autorizzate:	Campana**Gianluca**	Data nomina: 24/05/2018
	Flamini**Simona**	Data nomina: 24/05/2018

VALUTAZIONE ARCHIVI INFORMATICI

Azienda/Organizzazione	**Studio Legale Associato Felicetti Frascarelli Menghini Studio Associato**

SEDE LEGALE	Sede Studio Piazza della Concordia 1, 06039 Trevi - PG

Data revisione: 01/12/2023

VALUTAZIONE ARCHIVI INFORMATICI

Di seguito, è riportata la valutazione degli archivi informatici in dotazione all'organizzazione.
L'entità dei rischi viene ricavata assegnando un opportuno valore alla **probabilità di accadimento (P)** ed alle **conseguenze** di tale evento **(C)**. Dalla combinazione di tali grandezze si ricava la matrice di rischio la cui entità è data dalla relazione:

LR = P X C

LR = livello di rischio
P = probabilità di accadimento
C = conseguenze

Alla **probabilità di accadimento dell'evento P** è associato un indice numerico rappresentato nella seguente tabella:

PROBABILITA' DELL'EVENTO	
1	Improbabile
2	Poco probabile
3	Probabile
4	M. Probabile
5	Quasi certo

Alle **conseguenze** (C) è associato un indice numerico rappresentato nella seguente tabella:

CONSEGUENZE	
1	Trascurabili
2	Marginali
3	Limitate
4	Gravi
5	Gravissime

MATRICE DEI RISCHI

La matrice che scaturisce dalla combinazione di **probabilità** e **conseguenze** è rappresentata in figura seguente:

Probabilità						
	5	5	10	15	20	25
	4	4	8	12	16	20
	3	3	6	9	12	15
	2	2	4	6	8	10
	1	1	2	3	4	5
		1	2	3	4	5
		Conseguenze				

Entità Rischio	Valori di riferimento
Accettabile	*(1 ≤ LR ≤ 3)*
Medio - basso	*(4 ≤ LR ≤ 6)*
Rilevante	*(8 ≤ LR ≤ 12)*
Alto	*(15 ≤ LR ≤ 25)*

RISULTATI

Nome	PC Mauro
Tipo Struttura	Interna
Sede	Sede Studio (Trevi)
Personale con diritti di accesso	Felicetti Mauro, c.f. FLCMRA53H16D653Y
Note	
Software utilizzati	

MISURE DI SICUREZZA TECNICHE ED ORGANIZZATIVE

Nome	PC Dimitri
Tipo Struttura	Interna
Sede	Sede Studio (Trevi)
Personale con diritti di accesso	Frascarelli Dimitri, c.f. FRSDTR60M12F492M
Note	PC Marca Nipogi, Mod. AM01
Software utilizzati	

MISURE DI SICUREZZA TECNICHE ED ORGANIZZATIVE

Nome	PC Alberto
Tipo Struttura	Interna
Sede	Sede Studio (Trevi)
Personale con diritti di accesso	Menghini Alberto, c.f. MNGLRT65D17D653D
Note	PC Marca Nipogi, Mod. AM01
Software utilizzati	

MISURE DI SICUREZZA TECNICHE ED ORGANIZZATIVE

Nome	PC Gianluca
Tipo Struttura	Interna
Sede	Sede Studio (Trevi)
Personale con diritti di accesso	Campana Gianluca, c.f. CMPGLC78T25D653M
Note	

Software utilizzati	

MISURE DI SICUREZZA TECNICHE ED ORGANIZZATIVE

Nome	**Nas QNAP**
Tipo Struttura	Interna
Sede	Sede Studio (Trevi)
Personale con diritti di accesso	Felicetti Mauro, c.f. FLCMRA53H16D653Y Frascarelli Dimitri, c.f. FRSDTR60M12F492M Menghini Alberto, c.f. MNGLRT65D17D653D Campana Gianluca, c.f. CMPGLC78T25D653M Flamini Simona, c.f. FLMSMN78D70D653F
Note	
Software utilizzati	

MISURE DI SICUREZZA TECNICHE ED ORGANIZZATIVE

Nome	**Stampante Multifunzione Canon imageRUNNER ADVANCE C2220i**
Tipo Struttura	Interna
Sede	Sede Studio (Trevi)
Personale con diritti di accesso	Felicetti Mauro, c.f. FLCMRA53H16D653Y Frascarelli Dimitri, c.f. FRSDTR60M12F492M Menghini Alberto, c.f. MNGLRT65D17D653D Campana Gianluca, c.f. CMPGLC78T25D653M Flamini Simona, c.f. FLMSMN78D70D653F
Note	
Software utilizzati	

MISURE DI SICUREZZA TECNICHE ED ORGANIZZATIVE

Nome	**PC Simona**
Tipo Struttura	Interna
Sede	Sede Studio (Trevi)
Personale con diritti di accesso	Flamini Simona, c.f. FLMSMN78D70D653F
Note	
Software utilizzati	

MISURE DI SICUREZZA TECNICHE ED ORGANIZZATIVE

Nome	**Stampante Canon i-SENSYS LBP6650dn**
Tipo Struttura	Interna
Sede	Sede Studio (Trevi)
Personale con diritti di accesso	Felicetti Mauro, c.f. FLCMRA53H16D653Y Frascarelli Dimitri, c.f. FRSDTR60M12F492M Menghini Alberto, c.f. MNGLRT65D17D653D Campana Gianluca, c.f. CMPGLC78T25D653M Flamini Simona, c.f. FLMSMN78D70D653F
Note	
Software utilizzati	

MISURE DI SICUREZZA TECNICHE ED ORGANIZZATIVE

Nome	**HD Esterno**
Tipo Struttura	Interna
Sede	Sede Studio (Trevi)
Personale con diritti di accesso	Felicetti Mauro, c.f. FLCMRA53H16D653Y Frascarelli Dimitri, c.f. FRSDTR60M12F492M Menghini Alberto, c.f. MNGLRT65D17D653D Campana Gianluca, c.f. CMPGLC78T25D653M Flamini Simona, c.f. FLMSMN78D70D653F
Note	
Software utilizzati	

MISURE DI SICUREZZA TECNICHE ED ORGANIZZATIVE

Nome	**Posta elettronica Tin.it**
Tipo Struttura	Esterna
Azienda	Telecom Italia S.p.a.
Personale con diritti di accesso	Menghini Alberto, c.f. MNGLRT65D17D653D
Note	
Software utilizzati	

MISURE DI SICUREZZA TECNICHE ED ORGANIZZATIVE

Nome	**Dominio / Posta Elettronica "studioffm.it"**
Tipo Struttura	Esterna
Azienda	Levita S.r.l. Key Seven S.n.c. Di Lallement Eric, p.iva 02469320549
Personale con diritti di accesso	Felicetti Mauro, c.f. FLCMRA53H16D653Y Frascarelli Dimitri, c.f. FRSDTR60M12F492M Menghini Alberto, c.f. MNGLRT65D17D653D Campana Gianluca, c.f. CMPGLC78T25D653M Flamini Simona, c.f. FLMSMN78D70D653F
Note	
Software utilizzati	

MISURE DI SICUREZZA TECNICHE ED ORGANIZZATIVE

Nome	**Posta Elettronica Certificata "avvocatispoleto.legalmail.it"**
Tipo Struttura	Esterna
Azienda	Infocert S.p.a.
Personale con diritti di accesso	Felicetti Mauro, c.f. FLCMRA53H16D653Y Frascarelli Dimitri, c.f. FRSDTR60M12F492M Menghini Alberto, c.f. MNGLRT65D17D653D Campana Gianluca, c.f. CMPGLC78T25D653M Flamini Simona, c.f. FLMSMN78D70D653F
Note	
Software utilizzati	

MISURE DI SICUREZZA TECNICHE ED ORGANIZZATIVE

ISTRUZIONI OPERATIVE UTILIZZO SISTEMI INFORMATICI

INDICE

PREMESSA

L'utilizzo delle risorse informatiche e telematiche della nostra Azienda deve sempre ispirarsi al principio della diligenza e correttezza, comportamenti che normalmente si adottano nell'ambito di un rapporto di lavoro. Studio Legale Associato Felicetti Frascarelli Menghini Studio Associato ha adottato una procedura interna diretta ad evitare che comportamenti inconsapevoli possano innescare problemi o minacce alla sicurezza nel trattamento dei dati.

UTILIZZO DEL PERSONAL COMPUTER

Il Personal Computer affidato al dipendente è uno **strumento di lavoro**. Ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza.

L'accesso all'elaboratore è protetto da password che deve essere custodita dall'incaricato con la massima diligenza e non divulgata.

Il custode delle parole chiave riservate, per l'espletamento delle sue funzioni, ha la facoltà in qualunque momento di accedere ai dati trattati da ciascuno, ivi compresi gli archivi di posta elettronica interna ed esterna.

Il custode delle parole chiave riservate potrà accedere ai dati ed agli strumenti informatici esclusivamente per permettere alla stessa azienda, titolare del trattamento, di accedere ai dati trattati da ogni incaricato con le modalità fissate dalla stessa azienda, al solo fine di garantire l'operatività, la sicurezza del sistema ed il normale svolgimento dell'attività aziendale nei casi in cui si renda indispensabile ed indifferibile l'intervento, ad esempio, in caso di prolungata assenza o impedimento dell'incaricato, informando tempestivamente l'incaricato dell'intervento di accesso realizzato.

Non è consentito installare autonomamente programmi provenienti dall'esterno previa autorizzazione esplicita del *Responsabile dei sistemi informatici aziendali*, in quanto sussiste il grave pericolo di portare Virus informatici e di alterare la stabilità delle applicazioni dell'elaboratore.

Non è consentito l'uso di programmi diversi da quelli distribuiti ed installati ufficialmente dal *Responsabile dei sistemi informatici* della Studio Legale Associato Felicetti Frascarelli Menghini Studio Associato. L'inosservanza di questa disposizione, infatti, oltre al rischio di danneggiamenti del sistema per incompatibilità con il software esistente, può esporre l'azienda a gravi responsabilità civili ed anche penali in caso di violazione della normativa a tutela dei diritti d'autore sul software che impone la presenza nel sistema di software regolarmente licenziato o comunque libero e quindi non protetto dal diritto d'autore.

Non è consentito all'utente modificare le caratteristiche impostate sul proprio PC, salvo autorizzazione esplicita del *Responsabile dei sistemi informatici aziendali*.

Il Personal Computer deve essere spento ogni sera prima di lasciare gli uffici o in caso di assenze prolungate dall'ufficio. In ogni caso lasciare un elaboratore incustodito connesso alla rete può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in

seguito l'indebito uso. In ogni caso deve essere attivato lo screen saver e la relativa password.
Non è consentita l'installazione sul proprio PC di alcun dispositivo di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, modem, ecc.), se non con l'autorizzazione espressa del *Responsabile dei sistemi informatici aziendali*.
Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente il *Responsabile dei sistemi informatici aziendali* nel caso in cui vengano rilevati virus.

UTILIZZO DELLA RETE
Le unità di rete sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi. Qualunque file che non sia legato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità. Su queste unità, vengono svolte regolari attività di controllo, amministrazione e backup.
Le password d'ingresso alla rete ed ai programmi sono segrete e vanno comunicate e gestite secondo le procedure impartite. È assolutamente proibito entrare nella rete e nei programmi con altri nomi utente.
Il *Responsabile dei sistemi informatici aziendali* può in qualunque momento procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la Sicurezza sia sui PC degli incaricati sia sulle unità di rete.
Costituisce buona regola la periodica (almeno ogni sei mesi) pulizia degli archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati. È infatti assolutamente da evitare un'archiviazione ridondante.
È cura dell'utente effettuare la stampa dei dati solo se strettamente necessaria e di ritirarla prontamente dai vassoi delle stampanti comuni. È buona regola evitare di stampare documenti o file non adatti (molto lunghi o non supportati, come ad esempio il formato pdf o file di contenuto grafico) su stampanti comuni. In caso di necessità la stampa in corso può essere cancellata.

GESTIONE DELLE PASSWORD
Le password di ingresso alla rete, di accesso ai programmi e dello screen saver, sono previste ed attribuite dal *Responsabile dei sistemi informatici aziendali*.
È necessario procedere alla modifica della password a cura dell'incaricato del trattamento al primo utilizzo e, successivamente, almeno ogni sei mesi; nel caso di trattamento di dati particolari (ex dati sensibili) e di dati giudiziari la periodicità della variazione deve essere ridotta a tre mesi con contestuale comunicazione al *Responsabile dei sistemi informatici aziendali. (n.b.: in molti sistemi la comunicazione di variazione può essere "generata" dallo stesso sistema informatico all'atto della modifica, con invio di e-mail automatica al Responsabile; molti sistemi permettono di "temporizzare" la validità delle password e, quindi, di bloccare l'accesso al personale computer e/o al sistema, qualora non venga autonomamente variata dall'incaricato entro i termini massimi: in questi casi vanno adattate le istruzioni contenute nel presente regolamento)*
Le password possono essere formate da lettere (maiuscole o minuscole) e numeri ricordando che lettere maiuscole e minuscole hanno significati diversi per il sistema; devono essere composte da almeno otto caratteri e non deve contenere riferimenti agevolmente riconducibili all'incaricato.
La password deve essere immediatamente sostituita, dandone comunicazione al *Responsabile dei sistemi informatici aziendali*, nel caso si sospetti che la stessa abbia perso la segretezza.
Qualora l'utente venisse a conoscenza delle password di altro utente, è tenuto a darne immediata notizia alla Direzione o al *Responsabile dei sistemi informatici aziendali*.

UTILIZZO DEI SUPPORTI MAGNETICI
Tutti i supporti magnetici riutilizzabili (dischetti, cassette, cartucce) contenenti dati particolari (ex dati sensibili) e giudiziari devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere recuperato. Una persona esperta potrebbe infatti recuperare i dati memorizzati anche dopo la loro cancellazione.
I supporti magnetici contenenti dati particolari (ex dati sensibili) e giudiziari devono essere

custoditi in archivi chiusi a chiave.

UTILIZZO DI PC PORTATILI
L'utente è responsabile del PC portatile assegnatogli dal *Responsabile dei sistemi informatici aziendali* e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.
Ai PC portatili si applicano le regole di utilizzo previste per i Pc connessi in rete, con particolare attenzione alla rimozione di eventuali file elaborati sullo stesso prima della riconsegna.
I PC portatili utilizzati all'esterno (convegni, visite in azienda, ecc…), in caso di allontanamento, devono essere custoditi in un luogo protetto.

USO DELLA POSTA ELETTRONICA
La casella di posta, assegnata dall'Azienda all'utente, è uno **strumento di lavoro**. Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.
È fatto divieto di utilizzare le caselle di posta elettronica aziendale per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mail-list salvo diversa ed esplicita autorizzazione.
È buona norma evitare messaggi completamente estranei al rapporto di lavoro o alle relazioni tra colleghi. La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti.
Ogni comunicazione inviata o ricevuta che abbia contenuti rilevanti o contenga impegni contrattuali o precontrattuali per Studio Legale Associato Felicetti Frascarelli Menghini Studio Associato deve essere visionata od autorizzata dalla Direzione, o in ogni modo è opportuno fare riferimento alle procedure in essere per la corrispondenza ordinaria.
La documentazione elettronica che costituisce per l'azienda "know how" aziendale tecnico o commerciale protetto, e che, quindi, viene contraddistinta da diciture od avvertenze dirette ad evidenziarne il carattere riservato o segreto a tutela del patrimonio dell'impresa, non può essere comunicata all'esterno senza preventiva autorizzazione della Direzione.
È possibile utilizzare la ricevuta di ritorno per avere la conferma dell'avvenuta lettura del messaggio da parte del destinatario, ma di norma per la comunicazione ufficiale è obbligatorio avvalersi degli strumenti tradizionali (fax, posta, …).
Per la trasmissione di file all'interno di Studio Legale Associato Felicetti Frascarelli Menghini Studio Associato è possibile utilizzare la posta elettronica, prestando attenzione alla dimensione degli allegati.
È obbligatorio controllare i file attachements di posta elettronica prima del loro utilizzo (non eseguire download di file eseguibili o documenti da siti Web o Ftp non conosciuti).
È vietato inviare catene telematiche (o di Sant'Antonio). Se si dovessero ricevere messaggi di tale tipo, si deve comunicarlo immediatamente al *Responsabile dei sistemi informatici aziendali*. Non si devono in alcun caso attivare gli allegati di tali messaggi.

USO DELLA RETE INTERNET E DEI RELATIVI SERVIZI
Il PC abilitato alla navigazione in Internet costituisce uno strumento aziendale necessario allo svolgimento della propria attività lavorativa. È assolutamente proibita la navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa stessa.
È fatto divieto all'utente lo scarico di software gratuito (freeware) e shareware prelevato da siti Internet, se non espressamente autorizzato dal *Responsabile dei sistemi informatici aziendali*.
È tassativamente vietata l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili salvo i casi direttamente autorizzati dalla Direzione e con il rispetto delle normali procedure di acquisto.
È da evitare ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa.
È vietata la partecipazione a Forum non professionali, l'utilizzo di chat line (esclusi gli strumenti autorizzati), di bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi (o nicknames).

OSSERVANZA DELLE DISPOSIZIONI IN MATERIA DI PROTEZIONE DATI PERSONALI
È obbligatorio attenersi alle disposizioni in materia di protezione dati personali e di misure minime di sicurezza, ai sensi del GDPR 2016/679 e della normativa nazionale in vigore.

NON OSSERVANZA DELLA NORMATIVA AZIENDALE
Il mancato rispetto o la violazione delle regole contenute nel presente regolamento è perseguibile con provvedimenti disciplinari nonché con le azioni civili e penali consentite.

AGGIORNAMENTO E REVISIONE
Tutti gli utenti possono proporre, quando ritenuto necessario, integrazioni al presente Regolamento. Le proposte verranno esaminate dalla Direzione.
Il presente Regolamento è soggetto a revisione con frequenza annuale.

Data

La Direzione

ISTRUZIONI OPERATIVE VIDEOSORVEGLIANZA

INDICE

PREMESSA

Il trattamento dei dati personali effettuato mediante l'uso di sistemi di videosorveglianza non forma oggetto di legislazione specifica; si applicano, pertanto, le disposizioni generali in tema di protezione dei dati personali, volte a garantire l'incolumità pubblica e la sicurezza urbana.

L'Azienda Studio Legale Associato Felicetti Frascarelli Menghini Studio Associato ha adottato una procedura interna per il trattamento dei dati personali acquisiti mediante l'uso di sistemi di videosorveglianza, che rispetta i principi di protezione dei dati personali stabiliti dal Regolamento GDPR 2016/679 e dalla normativa nazionale in vigore.

1. DEFINIZIONI

Secondo l'articolo 4 del Regolamento (Ue) 2016/679 (GDPR) e della normativa nazionale in vigore, si definisce:

- 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;
- 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;
- 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.

2. PRINCIPI GENERALI

La videosorveglianza è utilizzata a fini molteplici, alcuni dei quali possono essere raggruppati nei seguenti ambiti generali:

1) protezione e incolumità degli individui, ivi ricompresi i profili attinenti alla sicurezza urbana, all'ordine e sicurezza pubblica, alla prevenzione, accertamento o repressione dei reati svolti dai soggetti pubblici, alla razionalizzazione e miglioramento dei servizi al pubblico volti anche ad

accrescere la sicurezza degli utenti, nel quadro delle competenze ad essi attribuite dalla legge;
2) protezione della proprietà;
3) rilevazione, prevenzione e controllo delle infrazioni svolti dai soggetti pubblici, nel quadro delle competenze ad essi attribuite dalla legge;
4) acquisizione di prove.
La necessità di garantire, in particolare, un livello elevato di tutela dei diritti e delle libertà fondamentali rispetto al trattamento dei dati personali consente la possibilità di utilizzare sistemi di videosorveglianza, purché ciò non determini un'ingerenza ingiustificata nei diritti e nelle libertà fondamentali degli interessati. Naturalmente l'installazione di sistemi di rilevazione delle immagini deve avvenire nel rispetto, oltre che della disciplina in materia di protezione dei dati personali, anche delle altre disposizioni dell'ordinamento applicabili, quali ad es. le vigenti norme dell'ordinamento civile e penale in materia di interferenze illecite nella vita privata, sul controllo a distanza dei lavoratori, in materia di sicurezza presso stadi e impianti sportivi, o con riferimento a musei, biblioteche statali e archivi di Stato, in relazione ad impianti di ripresa sulle navi da passeggeri adibite a viaggi nazionali e, ancora, nell'ambito dei porti, delle stazioni ferroviarie, delle stazioni delle ferrovie metropolitane e nell'ambito delle linee di trasporto urbano.
L'attività di videosorveglianza dev'essere effettuata nel rispetto del principio di proporzionalità nella scelta delle modalità di ripresa e dislocazione (es. tramite telecamere fisse o brandeggiabili, dotate o meno di zoom), nonché nelle varie fasi del trattamento che deve comportare, comunque, un trattamento di dati pertinenti e non eccedenti rispetto alle finalità perseguite.

3. DIRITTI DEGLI INTERESSATI
Deve essere assicurato agli interessati identificabili l'effettivo esercizio dei propri diritti in conformità al regolamento, in particolare il diritto di accedere ai dati che li riguardano, di verificare le finalità, le modalità e la logica del trattamento.
Dev'essere assicurato il "diritto all'oblio", ovvero il diritto di ogni singolo individuo a richiedere la cancellazione dei propri dati personali. Vi è, infatti, l'obbligo di cancellazione da parte del titolare del trattamento se sussiste uno dei motivi seguenti: i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati; l'interessato revoca il consenso su cui si basa il trattamento e se non sussiste altro fondamento giuridico per il trattamento; l'interessato si oppone al trattamento e non sussiste alcun motivo legittimo prevalente per procedere al trattamento; i dati personali sono stati trattati illecitamente; i dati personali devono essere cancellati per adempiere un obbligo legale previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento; i dati personali sono stati raccolti relativamente all'offerta di servizi della società dell'informazione ai minori" (articolo 17 Regolamento 2016/679 e normativa nazionale in vigore).

4. ADEMPIMENTI APPLICABILI A SOGGETTI PUBBLICI E PRIVATI
Secondo quanto afferma il Garante per la Privacy, un sistema di videosorveglianza è a norma quando rispetta i principi di liceità, necessità, proporzionalità e finalità. Attraverso il sistema di videosorveglianza è consentita:
- la registrazione delle immagini se necessarie ad obblighi di legge o per tutelare un interesse legittimo (liceità);
- le riprese devono limitarsi solamente a ciò che è necessario per raggiungere gli scopi prefissati (necessità);
- l'impianto va impiegato solo in luoghi dove è realmente necessario, limitando le riprese alle sole aree interessate ed escludendo la visuale su quelle circostanti (proporzionalità);
- lo scopo della videosorveglianza deve essere esplicito e legittimo nonché limitato alle finalità di pertinenza dei titolari dei dati (finalità).

Il principio generale in materia stabilisce che chiunque installi un sistema di videosorveglianza deve provvedere a segnalarne la presenza, facendo in modo che qualunque soggetto si avvicini all'area interessata dalle riprese sia avvisato della presenza di telecamere già prima di entrare nel loro raggio di azione.

Gli interessati devono essere sempre informati che stanno per accedere in una zona videosorvegliata.
Il supporto con l'informativa:
• deve essere collocato prima del raggio di azione della telecamera, anche nelle sue immediate vicinanze e non necessariamente a contatto con gli impianti;
• deve avere un formato ed un posizionamento tale da essere chiaramente visibile in ogni condizione di illuminazione ambientale, anche quando il sistema di videosorveglianza sia eventualmente attivo in orario notturno;
• può inglobare un simbolo o una stilizzazione di esplicita e immediata comprensione, eventualmente diversificati al fine di informare se le immagini sono solo visionate o anche registrate.
Il Garante ritiene auspicabile che l'informativa, resa in forma semplificata, poi rinvii a un testo completo contenente tutti gli elementi, accessibile anche con strumenti informatici e telematici.
Il Titolare del trattamento ha l'obbligo di effettuare la valutazione dell'impatto sulla protezione dei dati personali (DPIA), nel caso in cui la sorveglianza è sistematica su larga scala di una zona accessibile al pubblico (articolo 35 Regolamento 2016/679 e normativa nazionale in vigore).

5. VERIFICA PRELIMINARE
Le riprese effettuate per fini di sicurezza e tutela dell'ordine pubblico, con particolare riferimento alla prevenzione di reati o atti di vandalismo e alla sicurezza sul lavoro, costituiscono un'eccezione, e non necessitano dell'obbligo di segnalazione.
Normalmente, per installare un sistema di videosorveglianza, non è necessario l'assenso da parte del Garante della privacy; fanno però eccezione tutti i casi in cui sussiste il rischio di ledere i diritti e le libertà fondamentali o la dignità degli individui ripresi.
Ad esempio, devono essere sottoposti alla verifica preliminare di questa Autorità i sistemi di videosorveglianza dotati di *software* che permetta il riconoscimento della persona tramite collegamento o incrocio o confronto delle immagini rilevate (es. morfologia del volto) con altri specifici dati personali, in particolare con dati biometrici, o sulla base del confronto della relativa immagine con una campionatura di soggetti precostituita alla rilevazione medesima.
Un analogo obbligo sussiste con riferimento a sistemi c.d. intelligenti, che non si limitano a riprendere e registrare le immagini, ma sono in grado di rilevare automaticamente comportamenti o eventi anomali, segnalarli, ed eventualmente registrarli. In linea di massima tali sistemi devono considerarsi eccedenti rispetto alla normale attività di videosorveglianza, in quanto possono determinare effetti particolarmente invasivi sulla sfera di autodeterminazione dell'interessato e, conseguentemente, sul suo comportamento. Il relativo utilizzo risulta comunque giustificato solo in casi particolari, tenendo conto delle finalità e del contesto in cui essi sono trattati, da verificare caso per caso.
La conservazione delle immagini deve avere una durata prestabilita e non eccedente le 24 ore; in situazioni particolari, nelle quali sussiste un elevato fattore di rischio, la durata massima si estende ad una settimana. Nel caso si necessita di una conservazione dei dati più lunga sarà invece necessaria la verifica preliminare del Garante.
Comunque, anche fuori dalle predette ipotesi, in tutti i casi in cui i trattamenti effettuati tramite videosorveglianza hanno natura e caratteristiche tali per cui le misure e gli accorgimenti individuati non sono integralmente applicabili, in relazione alla natura dei dati o alle modalità del trattamento o agli effetti che possono determinare, il titolare del trattamento è tenuto a richiedere una verifica preliminare a questa Autorità.

Esclusione della verifica preliminare
Il titolare del trattamento di dati personali effettuato tramite sistemi di videosorveglianza non deve richiedere una verifica preliminare purché siano rispettate tutte le seguenti condizioni:
a) il Garante si sia già espresso con un provvedimento di verifica preliminare in relazione a determinate categorie di titolari o di trattamenti;
b) la fattispecie concreta, le finalità del trattamento, la tipologia e le modalità d'impiego del sistema che si intende adottare, nonché le categorie dei titolari, corrispondano a quelle del trattamento approvato;

c) si rispettino integralmente le misure e gli accorgimenti conosciuti o concretamente conoscibili prescritti.
Resta altresì inteso che nessuna approvazione implicita può desumersi dal semplice inoltro al Garante di documenti relativi a progetti di videosorveglianza (spesso generici e non valutabili a distanza) cui non segua un esplicito riscontro dell'Autorità, in quanto non si applica il principio del silenzio-assenso.
È regola generale che non vanno comunque notificati i trattamenti di dati effettuati per esclusive finalità di sicurezza o di tutela delle persone o del patrimonio ancorché relativi a comportamenti illeciti o fraudolenti, quando immagini o suoni raccolti siano conservati temporaneamente.
Al di fuori di tali precisazioni, il trattamento, che venga effettuato tramite sistemi di videosorveglianza, deve essere preventivamente notificato a questa Autorità.

6. MISURE DI SICUREZZA
Il titolare del trattamento dei dati ha l'obbligo di prendere le misure di sicurezza minime onde evitare la distruzione, la perdita, l'accesso abusivo alle immagini, nonché il loro utilizzo per scopi incoerenti con le finalità previste.
In particolare, i dati raccolti mediante sistemi di videosorveglianza, devono essere protetti con idonee e preventive misure di sicurezza, riducendo al minimo i rischi di distruzione, di perdita, anche accidentale, di accesso non autorizzato, di trattamento non consentito o non conforme alle finalità della raccolta, anche in relazione alla trasmissione delle immagini.
Devono quindi essere adottate specifiche misure tecniche ed organizzative che consentano al titolare di verificare l'attività espletata da parte di chi accede alle immagini o controlla i sistemi di ripresa (se soggetto distinto dal titolare medesimo, nel caso in cui questo sia persona fisica).
È inevitabile che, in considerazione dell'ampio spettro di utilizzazione di sistemi di videosorveglianza, anche in relazione ai soggetti e alle finalità perseguite nonché della varietà dei sistemi tecnologici utilizzati, le misure minime di sicurezza possano variare anche significativamente.

È tuttavia necessario che le stesse siano quanto meno rispettose dei principi che seguono:
a) in presenza di differenti competenze specificatamente attribuite ai singoli operatori devono essere configurati diversi livelli di visibilità e trattamento delle immagini. Laddove tecnicamente possibile, in base alle caratteristiche dei sistemi utilizzati, i predetti soggetti, designati incaricati o, eventualmente, responsabili del trattamento, devono essere in possesso di credenziali di autenticazione che permettano di effettuare, a seconda dei compiti attribuiti ad ognuno, unicamente le operazioni di propria competenza;
b) laddove i sistemi siano configurati per la registrazione e successiva conservazione delle immagini rilevate, deve essere altresì attentamente limitata la possibilità, per i soggetti abilitati, di visionare non solo in sincronia con la ripresa, ma anche in tempo differito, le immagini registrate e di effettuare sulle medesime operazioni di cancellazione o duplicazione;
c) per quanto riguarda il periodo di conservazione delle immagini, devono essere predisposte misure tecniche od organizzative per la cancellazione, anche in forma automatica, delle registrazioni, allo scadere del termine previsto;
d) nel caso di interventi derivanti da esigenze di manutenzione, occorre adottare specifiche cautele; in particolare, i soggetti preposti alle predette operazioni possono accedere alle immagini solo se ciò si renda indispensabile al fine di effettuare eventuali verifiche tecniche ed in presenza dei soggetti dotati di credenziali di autenticazione abilitanti alla visione delle immagini;
e) qualora si utilizzino apparati di ripresa digitali connessi a reti informatiche, gli apparati medesimi devono essere protetti contro i rischi di accesso abusivo di cui all'art. 615-*ter* del codice penale;
f) la trasmissione tramite una rete pubblica di comunicazioni di immagini riprese da apparati di videosorveglianza deve essere effettuata previa applicazione di tecniche crittografiche che ne garantiscano la riservatezza; le stesse cautele sono richieste per la trasmissione di immagini da punti di ripresa dotati di connessioni wireless (tecnologie *wi-fi, wi-max, Gprs*).

7. RESPONSABILI E INCARICATI
Il titolare o il responsabile devono designare per iscritto tutte le persone fisiche, incaricate del trattamento, autorizzate sia ad accedere ai locali dove sono situate le postazioni di controllo, sia ad utilizzare gli impianti e, nei casi in cui sia indispensabile per gli scopi perseguiti, a visionare le immagini. Deve trattarsi di un numero delimitato di soggetti, specie quando il titolare si avvale di collaboratori esterni. Occorre altresì individuare diversi livelli di accesso in corrispondenza delle specifiche mansioni attribuite ad ogni singolo operatore, distinguendo coloro che sono unicamente abilitati a visionare le immagini dai soggetti che possono effettuare, a determinate condizioni, ulteriori operazioni (es. registrare, copiare, cancellare, spostare l'angolo visuale, modificare lo zoom, ecc.).
Vanno osservate le regole ordinarie anche per ciò che attiene all'eventuale designazione di responsabili del trattamento.

***8*. DURATA DELLA CONSERVAZIONE DATI**
I dati personali devono essere adeguati, pertinenti e limitati a quanto necessario per le finalità del loro trattamento. Da qui l'obbligo, in particolare, di assicurare che il periodo di conservazione dei dati personali sia limitato al minimo necessario.
Nei casi in cui sia stato scelto un sistema che preveda la conservazione delle immagini, in applicazione del principio di proporzionalità, anche l'eventuale conservazione temporanea dei dati deve essere commisurata al tempo necessario a raggiungere la finalità perseguita.
Onde assicurare che i dati personali non siano conservati più a lungo del necessario, il titolare del trattamento deve stabilire un termine per la cancellazione o per la verifica periodica.
Generalmente la conservazione deve essere limitata a poche ore o, al massimo, alle ventiquattro ore successive alla rilevazione, fatte salve speciali esigenze di ulteriore conservazione in relazione a festività o chiusura di uffici o esercizi, nonché nel caso in cui si deve aderire ad una specifica richiesta investigativa dell'autorità giudiziaria o di polizia giudiziaria. Solo in alcuni casi, per peculiari esigenze tecniche (mezzi di trasporto) o per la particolare rischiosità dell'attività svolta dal titolare del trattamento (ad esempio, per alcuni luoghi come le banche può risultare giustificata l'esigenza di identificare gli autori di un sopralluogo nei giorni precedenti una rapina), può ritenersi ammesso un tempo più ampio di conservazione dei dati che si ritiene non debba comunque superare la settimana.

In tutti i casi in cui si voglia procedere a un allungamento dei tempi di conservazione per un periodo superiore alla settimana, una richiesta in tal senso deve essere sottoposta ad una verifica preliminare del GARANTE, e comunque essere ipotizzato dal titolare come eccezionale nel rispetto del principio di proporzionalità. La congruità di un termine di tempo più ampio di conservazione va adeguatamente motivata con riferimento ad una specifica esigenza di sicurezza perseguita, in relazione a concrete situazioni di rischio riguardanti eventi realmente incombenti e per il periodo di tempo in cui venga confermata tale eccezionale necessità. La relativa congruità può altresì dipendere dalla necessità di aderire ad una specifica richiesta di custodire o consegnare una copia specificamente richiesta dall'autorità giudiziaria o dalla polizia giudiziaria in relazione ad un'attività investigativa in corso.
Il sistema impiegato deve essere programmato in modo da operare al momento prefissato l'integrale cancellazione automatica delle informazioni allo scadere del termine previsto da ogni supporto, anche mediante sovra-registrazione, con modalità tali da rendere non riutilizzabili i dati cancellati. In presenza di impianti basati su tecnologia non digitale o comunque non dotati di capacità di elaborazione tali da consentire la realizzazione di meccanismi automatici di expiring dei dati registrati, la cancellazione delle immagini dovrà comunque essere effettuata nel più breve tempo possibile per l'esecuzione materiale delle operazioni dalla fine del periodo di conservazione fissato dal titolare.

9. SOGGETTI PUBBLICI
I soggetti pubblici sono tenuti a rispettare, al pari di ogni titolare di trattamento effettuato tramite sistemi di videosorveglianza, i principi enunciati.
Anche per i soggetti pubblici sussiste l'obbligo di fornire previamente l'informativa agli interessati. Pertanto, coloro che accedono o transitano in luoghi dove sono attivi sistemi di

videosorveglianza devono essere previamente informati in ordine al trattamento dei dati personali. A tal fine, anche i soggetti pubblici possono utilizzare il modello semplificato di informativa che:
• deve essere collocato prima del raggio di azione della telecamera, anche nelle sue immediate vicinanze e non necessariamente a contatto con gli impianti;
• deve avere un formato ed un posizionamento tale da essere chiaramente visibile in ogni condizione di illuminazione ambientale, anche quando il sistema di videosorveglianza sia eventualmente attivo in orario notturno;
• può inglobare un simbolo o una stilizzazione di esplicita e immediata comprensione, eventualmente diversificati al fine di informare se le immagini sono solo visionate o anche registrate.

Recenti disposizioni legislative in materia di sicurezza hanno attribuito ai sindaci il compito di sovrintendere alla vigilanza ed all'adozione di atti che sono loro attribuiti dalla legge e dai regolamenti in materia di ordine e sicurezza pubblica, nonché allo svolgimento delle funzioni affidati ad essi dalla legge in materia di sicurezza e di polizia giudiziaria. Al fine di prevenire e contrastare determinati pericoli che minacciano l'incolumità pubblica e la sicurezza urbana, il sindaco può altresì adottare provvedimenti, anche contingibili e urgenti, nel rispetto dei principi generali dell'ordinamento. Infine, il sindaco, quale ufficiale del Governo, concorre ad assicurare la cooperazione della polizia locale con le forze di polizia statali, nell'ambito delle direttive di coordinamento impartite dal Ministero dell'interno.
Da tale quadro emerge che sussistono specifiche funzioni attribuite sia al sindaco, quale ufficiale del Governo, sia ai comuni, rispetto alle quali i medesimi soggetti possono utilizzare sistemi di videosorveglianza in luoghi pubblici o aperti al pubblico al fine di tutelare la sicurezza urbana.
In ogni caso, si ribadisce l'auspicio che, l'informativa, benché non obbligatoria, venga comunque resa, specie laddove i comuni ritengano opportuno rendere noto alla cittadinanza l'adozione di misure e accorgimenti, quali l'installazione di sistemi di videosorveglianza, volti al controllo del territorio e alla protezione degli individui.

In applicazione dei richiamati principi di liceità, finalità e proporzionalità, l'utilizzo di sistemi di videosorveglianza risulta lecito con riferimento alle attività di controllo volte ad accertare l'utilizzo abusivo di aree impiegate come discariche di materiali e di sostanze pericolose solo se non risulta possibile, o si riveli non efficace, il ricorso a strumenti e sistemi di controllo alternativi.
Analogamente, l'utilizzo di sistemi di videosorveglianza è lecito se risultano inefficaci o inattuabili altre misure nei casi in cui si intenda monitorare il rispetto delle disposizioni concernenti modalità, tipologia ed orario di deposito dei rifiuti.
Avvertenze per i sistemi di videosorveglianza posti in essere da enti pubblici e da enti territoriali
Anche gli enti territoriali e, in generale, i soggetti pubblici operanti sul territorio effettuano attività di videosorveglianza in forma integrata, tramite la compartecipazione ad un medesimo sistema di rilevazione, al fine di economizzare risorse e mezzi impiegati nell'espletamento delle più diverse attività istituzionali.
Questa Autorità ha già individuato un quadro di specifiche garanzie in ordine alle corrette modalità che vengono qui ulteriormente richiamate, in particolare con riferimento all'attività del controllo sul territorio da parte dei comuni, anche relativamente a quanto disposto in materia di videosorveglianza comunale.
In particolare:
a) l'utilizzo condiviso, in forma integrale o parziale, di sistemi di videosorveglianza tramite la medesima infrastruttura tecnologica deve essere configurato con modalità tali da permettere ad ogni singolo ente e, in taluni casi, anche alle diverse strutture organizzative dell'ente, l'accesso alle immagini solo nei termini strettamente funzionali allo svolgimento dei propri compiti istituzionali, evitando di tracciare gli spostamenti degli interessati e di ricostruirne il percorso effettuato in aree che esulano dalla competenza territoriale dell'ente;
b) nei casi in cui un "centro" unico gestisca l'attività di videosorveglianza per conto di diversi soggetti pubblici, i dati personali raccolti dovranno essere trattati in forma differenziata e

rigorosamente distinta, in relazione alle competenze istituzionali della singola pubblica amministrazione.
Il titolare del trattamento è tenuto a richiedere una verifica preliminare all'Autorità fuori dalle predette ipotesi, ed in tutti i casi in cui i trattamenti effettuati tramite sistemi integrati di videosorveglianza hanno natura e caratteristiche tali per cui le misure e gli accorgimenti sopra individuati non siano integralmente applicabili, in relazione alla natura dei dati o alle modalità del trattamento, agli effetti che possono determinare o, a maggior ragione, con riferimento a quei sistemi per i quali già la richiede (es. sistemi di raccolta delle immagini associate a dati biometrici o c.d. intelligenti, cioè in grado di rilevare automaticamente comportamenti o eventi anomali, segnalarli, ed eventualmente registrarli).

10. SOGGETTI PRIVATI

L'installazione di sistemi di videosorveglianza viene sovente effettuata da persone fisiche per fini esclusivamente personali. In tal caso va chiarito che la disciplina del Regolamento GDPR non trova applicazione qualora i dati non siano comunicati sistematicamente a terzi ovvero diffusi, risultando comunque necessaria l'adozione di cautele a tutela dei terzi. In tali ipotesi possono rientrare, a titolo esemplificativo, strumenti di videosorveglianza idonei ad identificare coloro che si accingono ad entrare in luoghi privati (videocitofoni ovvero altre apparecchiature che rilevano immagini o suoni, anche tramite registrazione), oltre a sistemi di ripresa installati nei pressi di immobili privati ed all'interno di condomini e loro pertinenze (quali posti auto e *box*).
Benché non trovi applicazione la disciplina del Regolamento GDPR, al fine di evitare di incorrere nel reato di interferenze illecite nella vita privata (*art. 615-bis c.p.*), l'angolo visuale delle riprese deve essere comunque limitato ai soli spazi di propria esclusiva pertinenza (ad esempio antistanti l'accesso alla propria abitazione) escludendo ogni forma di ripresa, anche senza registrazione di immagini, relativa ad aree comuni (cortili, pianerottoli, scale, garage comuni) ovvero ad ambiti antistanti l'abitazione di altri condomini.

11. OSSERVANZA DELLE DISPOSIZIONI IN MATERIA DI PROTEZIONE DATI PERSONALI

È obbligatorio attenersi alle disposizioni in materia di protezione dati personali e di misure minime di sicurezza, ai sensi del GDPR 2016/679 e della normativa nazionale in vigore.

12. NON OSSERVANZA DELLA NORMATIVA AZIENDALE

Il mancato rispetto o la violazione delle regole contenute nel presente regolamento è perseguibile con provvedimenti disciplinari nonché con le azioni civili e penali consentite.

13. AGGIORNAMENTO E REVISIONE

Tutti gli utenti possono proporre, quando ritenuto necessario, integrazioni al presente Regolamento. Le proposte verranno esaminate dalla Direzione.

Il presente Regolamento è soggetto a revisione con frequenza annuale.

Data

La Direzione

ISTRUZIONE OPERATIVA DATA BREACH

L'art. 33 del **Regolamento Europeo 679/2016** (**GDPR**) e la normativa nazionale in vigore, impone al titolare del trattamento di notificare all'autorità di controllo la violazione di dati personali (**data breach**) entro 72 ore dal momento in cui ne viene a conoscenza.

L'obbligo di notifica scatta se la violazione, ragionevolmente, comporta un rischio per i diritti e le libertà delle persone fisiche, qualora, poi, il rischio fosse elevato, allora, oltre alla notifica, il titolare è tenuto a darne comunicazione all'interessato.

Il termine per adempiere alla notifica è brevissimo, 72 ore dal momento in cui il titolare ne viene a conoscenza, mentre, l'eventuale comunicazione agli interessati, deve essere fatta senza indugio.

L'eventuale ritardo nella notificazione deve essere giustificato, il mancato rispetto dell'obbligo di notifica, invece, pone l'autorità di controllo nella condizione di applicare le misure correttive a sua disposizione ovvero: l'esercizio dei poteri previsti dall'art.58 GDPR (avvertimenti, ammonimenti, ingiunzioni, imposizione di limiti al trattamento, ordine di rettifica, revoca di certificazioni, ordine di sospendere flussi dati), la imposizione di sanzioni amministrative secondo l'art. 83 GDPR e della normativa nazionale in vigore.

Per **"Violazione di dati"** si intende 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 (Art. 4 p.12 del GDPR).

La violazione di dati è un particolare tipo di incidente di sicurezza, per effetto del quale, il titolare non è in grado di garantire il rispetto dei principi prescritti dall'art. 5 del GDPR per il trattamento dei dati personali.

Preliminarmente, dunque, il titolare deve poter identificare l'incidente di sicurezza in genere, quindi, comprendere che l'incidente ha impatto sulle informazioni e, infine, che tra le informazioni coinvolte dall'incidente vi sono dati personali.

L'art. 33 p.5 del GDPR prescrive al titolare di documentare qualsiasi violazione dei dati personali, al fine di consentire all'autorità di controllo di verificare il rispetto della norma.

L'art. 33 p.2 GDPR prevede espressamente il dovere per il responsabile, quando viene a conoscenza di una violazione, di informare, senza ingiustificato ritardo, il titolare.

E' importante che sia dimostrabile il momento della scoperta dell'incidente, poiché da quel momento decorrono le 72 ore per la notifica.

Si possono distinguere tre tipi di violazioni:

1. violazione di riservatezza, ovvero quando si verifica una divulgazione o un accesso a dati personali non autorizzato o accidentale;
2. violazione di integrità, ovvero quando si verifica un'alterazione di dati personali non autorizzata o accidentale;
3. violazione di disponibilità, ovvero quando si verifica perdita, inaccessibilità, o distruzione, accidentale o non autorizzata, di dati personali.

Una violazione potrebbe comprendere una o più tipologie.

Per comprendere quando notificare la violazione è opportuno effettuare una valutazione dell'entità dei rischi:

- **Rischio assente**: la notifica al Garante non è obbligatoria.
- **Rischio presente**: è necessaria la notifica al Garante.

- **Rischio elevato**: In presenza di rischi "elevati", è necessaria la comunicazione agli interessati. Nel momento in cui il titolare del trattamento adotta sistemi di crittografia dei dati, e la violazione non comporta l'acquisizione della chiave di decrittografia, la comunicazione ai soggetti interessati non sarà un obbligo.

I rischi per i diritti e le libertà degli interessati possono essere considerati "elevati" quando la violazione può, a titolo di esempio:

- coinvolgere un rilevante quantitativo di dati personali e/o di soggetti interessati;
- riguardare categorie particolari di dati personali;
- comprendere dati che possono accrescere ulteriormente i potenziali rischi (es. dati di localizzazione, finanziari, relativi alle abitudini e preferenze);
- comportare rischi imminenti e con un'elevata probabilità di accadimento (es. rischio di perdita finanziaria in caso di furto di dati relativi a carte di credito);
- impattare su soggetti che possono essere considerati vulnerabili per le loro condizioni (es. pazienti, minori, soggetti indagati).

Per la notifica della violazione e la comunicazione al Garante occorre compilare gli appositi moduli messi a disposizione.

ISTRUZIONI OPERATIVE INCARICATI DEL TRATTAMENTO

INDICE

PREMESSA

Il presente documento contiene le istruzioni operative per gli Incaricati del trattamento dei dati personali dell'Azienda Studio Legale Associato Felicetti Frascarelli Menghini Studio Associato, conformemente al Regolamento (Ue) 2016/679 (GDPR) ed alla normativa nazionale in vigore. I dipendenti, i collaboratori, i consulenti, i volontari ed in generale tutte le persone autorizzate ad accedere ai dati personali e preposte allo svolgimento delle operazioni di trattamento relativa ai dati, devono ispirarsi a un principio generale di diligenza e correttezza. Ogni utilizzo dei dati in possesso dell'Azienda diverso da finalità strettamente professionali, è espressamente vietato. Di seguito vengono esposte le regole comportamentali da seguire per evitare e prevenire condotte che anche inconsapevolmente potrebbero comportare rischi alla sicurezza del sistema informativo e all'immagine dell'Azienda.

1. DEFINIZIONI

Secondo l'articolo 4 del Regolamento (Ue) 2016/679 (GDPR) e la normativa nazionale in vigore, si definisce:

- 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;
- 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;
- 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.

2. ADEMPIMENTI

Ciascun incaricato del trattamento deve:
- rispettare i principi generali del Regolamento (Ue) 2016/679 (GDPR) e della normativa nazionale in vigore, con particolare riferimento alla liceità e correttezza del proprio agire, all'obbligo di procedere alla raccolta e alla registrazione dei dati per scopi determinati, espliciti e legittimi;
- rispettare l'obbligo di riservatezza e segretezza e conseguentemente il divieto di comunicazione e diffusione dei dati trattati nel corso dell'incarico svolto;
- utilizzare i dati, cui abbia accesso, solamente per finalità compatibili all'esecuzione delle proprie mansioni o dei compiti affidati, per cui è autorizzato ad accedere alle informazioni e ad utilizzare gli strumenti aziendali;
- rispettare le misure di sicurezza idonee adottate dalla società, atte a salvaguardare la riservatezza e l'integrità dei dati;
- segnalare eventuali malfunzionamenti di strumenti elettronici, perdite di dati o esigenze (sia di natura organizzativa, sia tecnica), che possano migliorare lo svolgimento delle operazioni affidate;
- accedere ai dati strettamente necessari all'esercizio delle proprie funzioni e competenze;
- in caso di interruzione del lavoro, anche temporanea, verificare che i dati trattati non siano accessibili a terzi non autorizzati;
- mantenere riservate le proprie credenziali di autenticazione;
- svolgere le attività previste dai trattamenti secondo le direttive del responsabile del trattamento dei dati; non modificare i trattamenti esistenti o introdurre nuovi trattamenti senza l'esplicita autorizzazione del responsabile del trattamento dei dati;
- rispettare e far rispettare le norme di sicurezza per la protezione dei dati personali;
- informare il responsabile in caso di incidente di sicurezza che coinvolga dati particolari e non;
- raccogliere, registrare e conservare i dati presenti negli atti e documenti contenuti nei fascicoli di studio e nei supporti informatici avendo cura che l'accesso ad essi sia possibile solo ai soggetti autorizzati;
- eseguire qualsiasi altra operazione di trattamento nei limiti delle proprie mansioni e nel rispetto delle norme di legge.

3. MODALITÀ DI SVOLGIMENTO DELLE OPERAZIONI

Le principali operazioni degli incaricati del trattamento sono:
- identificazione dell'interessato:

al momento della raccolta dei dati personali, qualora sia necessario individuare l'identità del soggetto che fornisce le informazioni, è obbligatorio richiedere un documento di identità o di riconoscimento, al fine di verificare la identità e di procedere correttamente alla raccolta e alla

registrazione delle informazioni;

- verifica del controllo dell'esattezza del dato e della corretta digitazione:

al momento della registrazione dei dati raccolti, occorre prestare attenzione alla digitazione e all'inserimento dei dati identificativi e degli altri dati riferiti all'interessato, al fine di evitare errori, che potrebbero generare problemi nella corretta gestione dell'anagrafica e nello svolgimento delle operazioni, che caratterizzano il processo di trattamento;

- Norme logistiche per l'accesso fisico ai locali:

I locali, ove sono custoditi i dati personali (ed in particolare quelli di natura sensibile), devono essere soggetti a controllo e a verifica, al fine di evitare che durante l'orario di lavoro possano essere conosciuti o accessibili da parte di soggetti non autorizzati. Si raccomanda, in caso di allontanamento dal proprio ufficio o dalla propria postazione di lavoro, di adottare tutte le accortezze e precauzioni al fine di impedire l'accesso fisico a chi non sia legittimato, soprattutto se esterno all'organizzazione di appartenenza. Laddove si esegue il trattamento di Dati Personali, deve essere possibile ricoverare in luogo sicuro i documenti cartacei ed i supporti rimovibili contenenti tali dati. Pertanto le porte degli uffici ed almeno un armadio per ufficio devono essere dotati di serratura con chiave. Al termine dell'orario lavorativo, ove la dinamica delle attività ed il numero di occupanti lo consentano, è necessario chiudere sempre a chiave gli uffici nei quali vengono svolti trattamenti di Dati Personali.

- Rilevazione presenze

Ove possibile, si raccomanda di dotare le sedi dell'Azienda di un servizio di rilevazione delle presenze e di un servizio di reception / sorveglianza. In questo caso, ogni Incaricato è tenuto ad utilizzare sempre i sistemi di rilevazione presenze disponibili, allo scopo di segnalare la propria presenza e legittimare le attività in corso di svolgimento.

4. ISTRUZIONI PER L'USO DEGLI STRUMENTI INFORMATICI

Come principio generale, sia i dispositivi di memorizzazione del proprio PC sia le unità di rete, devono contenere informazioni strettamente professionali e non possono essere utilizzate per scopi diversi (immagini, video e documenti personali).
Di seguito sono riportate le indicazioni per la gestione dei diversi strumenti informatici per il trattamento dati:

a) Gestione strumenti elettronici (pc fissi e portatili)

Ciascun incaricato è responsabile del corretto utilizzo e della custodia degli strumenti elettronici in dotazione (a titolo esemplificativo personal computer, periferiche, lettori di smart card). Si devono adottare le misure di sicurezza per la tutela della riservatezza, consistenti nell'evitare che l'accesso ai dati possa avvenire da parte di soggetti estranei all'organizzazione o non specificamente autorizzati. Al fine di verificare il corretto utilizzo degli strumenti in dotazione potranno essere svolti controlli a campione mediante la raccolta e l'analisi di dati aggregati e anonimi. Inoltre, nel caso di provato o constatato uso illecito o non consentito degli strumenti elettronici, risultante dalla verifica delle informazioni in modalità aggregata e anonima, può essere necessario procedere alla verifica delle registrazioni delle sessioni di lavoro, al fine di sanzionare condotte illecite, anche su richiesta dell'autorità giudiziaria, cui le informazioni potranno essere comunicate, senza alcuna ulteriore informativa all'interessato.
Per la gestione della sessione di lavoro sul pc (fisso e portatile), è necessario che:
• al termine delle ore di servizio, il PC deve essere spento, a meno che non stia svolgendo elaborazioni particolari. In tal caso gli uffici debbono tassativamente essere chiusi a chiave;
• Se l'incaricato si assenta momentaneamente dalla propria postazione deve accertarsi che l'eventuale sessione di lavoro aperta non sia accessibile da altre persone. Pertanto deve chiudere la sessione di lavoro sul PC facendo Logout, oppure in alternativa deve avere attivo un salvaschermo (screen- saver) protetto dalle credenziali di autenticazione;
• Relativamente all'utilizzo dello screen-saver, occorre osservare le seguenti norme:

- Non deve mai essere disattivato;
- Il suo avvio automatico deve essere previsto non oltre i primi 10 minuti di inattività del PC;

- Deve essere messo in funzione manualmente ogni volta che si lascia il PC incustodito ed acceso;

• Quando si esegue la stampa di un documento contenente dati personali, in particolare su una stampante condivisa, occorre ritirare tempestivamente i documenti stampati per evitare l'accesso a soggetti non abilitati al trattamento.
Per l'utilizzo dei PC portatili valgono le regole elencate per i PC connessi alla rete, con le seguenti ulteriori raccomandazioni:
• prima della riconsegna, rimuovere eventuali file ivi elaborati;
• quando il PC portatile è nei locali dell'Azienda, non lasciarlo mai incustodito; in caso di brevi assenze assicurarlo alla scrivania o ad elementi "sicuri" dell'arredamento (maniglie, intelaiature…) utilizzando gli appositi cavi in acciaio dotati di lucchetto;
• quando il PC portatile è all'esterno dell'Azienda, evitare di lasciarlo incustodito;
• per assenze prolungate, anche qualora l'ambiente venga ritenuto "affidabile", è necessario custodire il portatile in modo opportuno es. cassaforte;
• in caso di furto di un portatile è necessario avvertire tempestivamente il responsabile del Servizio Informatico, onde prevenire possibili intrusioni ai sistemi aziendali;
• in caso di viaggio aereo trasportare tassativamente il portatile come bagaglio a mano;
• eseguire periodicamente salvataggi dei dati e non tenere tali backup insieme al PC portatile.

b) Gestione username e password

L'accesso al PC, sia esso collegato in rete o meno, è protetto da un sistema di autenticazione che richiede all'Incaricato di inserire sulla videata di accesso all'elaboratore un codice utente (username) ed una parola chiave (password). L'adozione ed il corretto utilizzo della combinazione username / password è fondamentale per il corretto utilizzo del PC, in quanto:
• tutela l'utilizzatore ed in generale l'Azienda da accessi illeciti, atti di vandalismo e, in generale, violazioni e danneggiamenti del proprio patrimonio informativo;
• tutela l'Incaricato da false imputazioni, garantendo che nessuno possa operare a suo nome e che, con il suo profilo (ossia con le sue user id e password) solo lui possa svolgere determinate azioni;
• è necessario per gestire correttamente gli accessi a risorse condivise.
Ciascun incaricato deve scegliere le password in base ai seguenti criteri:
• devono essere lunghe almeno otto caratteri;
• non devono fare riferimento ad informazioni agevolmente riconducibili ai soggetti utilizzatori o ai loro famigliari;
• devono contenere una combinazione di numeri e/o segni speciali, lettere, maiuscole e minuscole;
• non deve essere uguali alle precedenti.
Per la corretta gestione della password è necessario:
• Almeno ogni 3 mesi è obbligatorio cambiare la password;
• Ogni password ricevuta va modificata al primo utilizzo;
• La password venga conservata in un luogo sicuro;
• Non rivelare o condividere la password con i colleghi di lavoro, famigliari e amici, soprattutto attraverso il telefono;
• Non utilizzare la funzione, offerta da alcuni software, di salvare automaticamente la password per successivi utilizzi delle applicazioni.

c) Installazione di hardware e software

L'installazione di hardware e software, nonché la modifica dei parametri di configurazione, possono essere eseguiti solamente dalle persone del Servizio Informatico su mandato del Responsabile del trattamento per i Sistemi Elettronici. Pertanto si raccomanda agli utenti dei PC di rispettare i seguenti divieti:
• Non utilizzare sul PC dispositivi personali, o comunque non aziendali, quali lettori dispositivi di memorizzazione dei dati;
• Non installare sistemi per connessione esterne (es : modem, wifi); tali connessioni, aggirando i sistemi preposti alla sicurezza della rete aziendale, aumentano sensibilmente i rischi di

intrusioni e di attacchi dall'esterno;
• Non installare programmi, anche in versione demo. In particolare, è vietata l'installazione di giochi, programmi in prova (shareware), programmi gratuiti (freeware), programmi pirata, e in generale tutti i software non autorizzati dal Servizio Informatico;
• Non modificare i parametri di configurazione del proprio PC senza espressa autorizzazione e senza il supporto di personale tecnico qualificato.
Si ricorda che normalmente la condivisione di aree e di risorse del proprio PC è vietata. Può essere autorizzata dal Servizio Informatico, solo in casi eccezionali e solo per il tempo strettamente necessario allo svolgimento delle attività di lavoro. In questi casi devono essere adottate password di lettura e scrittura e la condivisione deve operare solo su singole directory del PC, e non sull'intero disco rigido.

d) Gestione posta elettronica aziendale

Il servizio di posta elettronica viene fornito per permettere la comunicazione con soggetti terzi interni ed esterni per le finalità della Azienda e in stretta connessione con l'effettiva attività e mansioni del lavoratore o del volontario che utilizza tale funzionalità.
Al fine di non compromettere la sicurezza dell'azienda e di prevenire conseguenze legali a carico della stessa, bisogna adottare le seguenti norme comportamentali:
• Se si ricevono mail da destinatari sconosciuti contenenti file di qualsiasi tipo, procedere alla loro immediata eliminazione;
• È fatto divieto di utilizzare le caselle di posta elettronica per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mail list, salvo diversa ed esplicita autorizzazione;
• La casella di posta elettronica assegnata deve essere mantenuta in ordine, cancellando i documenti inutili specialmente se contengono allegati ingombranti come dimensione.
Nell'ipotesi in cui la email debba essere utilizzata per la trasmissione di dati particolari (ex dati sensibili), si raccomanda di prestare attenzione a che:
• l'indirizzo del destinatario sia stato correttamente digitato,
• l'oggetto del messaggio non contenga direttamente il riferimento a stati, fatti o qualità idonei a rivelare dati di natura sensibile;
• nel corpo del messaggio sia presente un'intestazione standardizzata in cui si avverta della confidenzialità/riservatezza del messaggio;

e) Gestione del salvataggio dei dati

• Per i dati ed i documenti che risiedono sui server gestiti centralmente, come ad esempio cartelle di rete e database, il Servizio Informatico esegue i salvataggi con la possibilità di ripristinare in toto oppure selettivamente eventuali files distrutti, ad esempio per guasti hardware oppure per cancellazioni involontarie.

• Per i dati ed i documenti che risiedono esclusivamente sul PC, ogni Incaricato deve eseguire almeno una volta alla settimana la copia (salvataggio, o backup). Questo allo scopo di garantire la disponibilità ed il ripristino dei Dati Personali nel caso di una generica compromissione delle risorse (cancellazioni accidentali, guasti, furti…). L'Incaricato deve verificare che i supporti informatici utilizzati per il backup, che normalmente sono dischi magnetici esterni, CD, DVD oppure flash disks (chiavette) siano funzionali e non corrotti.

f) Gestione dei supporti rimovibili

I supporti rimovibili, come ad esempio dischi magnetici esterni, penne USB o CD riscrivibili, quando contengono dati personali devono essere custoditi in luogo protetto e non accessibile (cassaforte, armadio chiuso a chiave, etc.). Quando non sono più utilizzati devono essere distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri Incaricati non autorizzati al trattamento degli stessi dati, soltanto dopo essere stati

formattati. Tali operazioni vengono effettuate a cura del servizio Sistemi. Il trasferimento di file contenenti dati personali, dati particolari (ex dati sensibili) e giudiziari su supporti rimovibili, è da eseguire unicamente in via transitoria, ponendo la massima attenzione alla destinazione di trasferimento e cancellando i file appena possibile. I dati particolari (ex dati sensibili)/giudiziari devono essere crittografati.

g) Gestione protezione dai virus informatici

Per prevenire eventuali danneggiamenti al software causati dalla presenza o dall'azione di programmi virus informatici, su ogni elaboratore dell'Azienda è stato installato un software antivirus aziendale che si aggiorna automaticamente all'ultima versione disponibile.
L'antivirus aziendale non deve mai essere disattivato o sostituito con altro antivirus non ufficialmente fornito.
Nel caso il programma antivirus installato sul proprio PC riscontri la presenza di un virus, oppure si sospetti la presenza di un virus non rilevato dal programma antivirus è necessario darne immediatamente segnalazione al responsabile del Servizio Informatico.
Si raccomanda di non scaricare e né tantomeno aprire file provenienti via e-mail da mittenti sconosciuti. Tali file, possono essere portatori di virus e compromettere la funzionalità del PC, l'integrità dei dati in essa contenuti e soprattutto l'integrità dei sistemi collegati al PC stesso.

5. ISTRUZIONI PER L'USO DEGLI STRUMENTI "NON ELETTRONICI"

Per "non elettronici" si intendono sia documenti cartacei sia documenti di altro tipo come ad esempio microfilm, microfiches e lucidi. I documenti di questo tipo contenenti dati particolari (ex dati sensibili) o giudiziari devono essere protetti in appositi armadi dotati di chiavi. Tutti i documenti contenenti dati particolari (ex dati sensibili) o giudiziari che si ritiene debbano essere eliminati devono essere distrutti e non gettati nei cestini.
Per proteggere i dati personali è opportuno evitare il deposito di documenti di qualsiasi genere negli ambienti di transito o pubblici (corridoi o sale riunioni), come pure l'abbandono in vista sulle scrivanie quando ci si debba assentare dal proprio posto di lavoro. Nel caso di dati particolari (ex dati sensibili) e/o giudiziari, il rispetto di queste norme è obbligatorio.

a) distruzione delle copie cartacee

Coloro che sono preposti alla duplicazione di documentazione (con stampanti o fotocopiatrici o altre periferiche) ovvero che utilizzando strumenti per la riproduzione cartacea di documenti digitali, sono tenuti a procedere alla relativa distruzione del supporto, qualora si verifichino errori o la riproduzione non sia corretta, evitando di riutilizzare i fogli, salva l'ipotesi di uso esclusivamente personale per eventuali appunti o brutte copie, da distruggere immediatamente quando non più necessarie;

b) Misure di sicurezza

Il trattamento sicuro di documenti contenenti Dati Personali richiede la presenza di misure di sicurezza con le quali l'Incaricato possa interagire ed una serie di accorgimenti direttamente gestibili dall'Incaricato stesso. In particolare, si richiede:
• la presenza e l'uso tassativo di armadi e cassetti dotati di serratura adeguata;
• la presenza e l'uso tassativo, ove si richieda la distruzione di documenti contenenti dati particolari (ex dati sensibili) e giudiziari, di un tritadocumenti.

c) Prescrizioni per gli incaricati

L'Incaricato deve attenersi alle seguenti prescrizioni:
• in nessun caso è concesso l'accesso a documentazione contenente Dati Personali per motivi non dettati da esigenze di lavoro strettamente connesse ai trattamenti dichiarati, autorizzati e tutelati dal Titolare;
• la documentazione contenente Dati Personali che, per ragioni di praticità operativa, risiede sulle scrivanie degli Incaricati, deve comunque essere rimossa al termine dell'orario di lavoro;
• l'accesso ai supporti deve essere limitato al tempo necessario a svolgere i Trattamenti previsti;
• i supporti devono essere archiviati in ambiente ad accesso controllato;
• i documenti contenenti dati personali, non devono essere lasciati incustoditi in un ambiente non controllato (ad es. a seguito della stampa dei documenti su stampante di rete);
• il numero di copie di documenti contenenti Dati Personali deve essere strettamente funzionale alle esigenze di lavoro;
• cassetti ed armadi contenenti documentazione riservata debbono tassativamente essere chiusi a chiave fuori dell'orario di lavoro;
• l'accesso fuori orario lavorativo a documenti contenti Dati particolari (ex dati sensibili) /giudiziari può avvenire da parte di personale Incaricato, o tramite autorizzazione di quest'ultimo, unicamente previa registrazione dell'accesso a tali documenti;
• la distruzione di documenti contenenti Dati Personali deve essere operata, ove possibile, direttamente dal personale Incaricato;
• ove non siano disponibili strumenti per la distruzione dei documenti (trita documenti), o il volume di questi sia tale da imporre il ricorso al servizio di macero, il personale Incaricato che avvia al macero la documentazione è tenuto a confezionare tale documentazione in modo che il pacco risulti anonimo e solido;
• quando gli atti e i documenti contenenti dati personali, dati particolari (ex dati sensibili) o giudiziari sono affidati agli Incaricati per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono controllati e custoditi dagli Incaricati fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate;
• l'accesso agli archivi contenenti dati particolari (ex dati sensibili) o giudiziari deve essere controllato. Le persone ammesse, a qualunque titolo, dopo l'orario di chiusura, sono identificate e registrate. Quando gli archivi non sono dotati di strumenti elettronici per il controllo degli accessi o di incaricati della vigilanza, le persone che vi accedono devono essere preventivamente autorizzate.
• è severamente vietato utilizzare documenti contenenti Dati personali, dati particolari (ex dati sensibili) o giudiziari come carta da riciclo o da appunti.

6. ADDETTI ALLA MANUTENZIONE

Le seguenti istruzioni devono essere osservate dai preposti in qualità di addetti alla gestione o manutenzione che trattano dati di titolarità per i quali è nominato un responsabile del trattamento nonché dagli addetti di ditte specializzate che svolgano interventi tecnici di gestione e manutenzione degli strumenti elettronici:
• Effettuare operazioni di manutenzione e supporto per verifica corretto funzionamento (monitoraggio e diagnostica) su flussi dei dati;
• gestire le credenziali di autenticazione dei soggetti incaricati del trattamento su indicazione dell'Amministratore di sistema;
• gestire i profili di autorizzazione degli incaricati al trattamento dei dati, su specifiche impartite dai responsabili di funzione/BU, su indicazione dell'Amministratore di sistema;
• provvedere alla disattivazione/variazione delle utenze, ivi compreso l'account di posta elettronica, assegnate al personale cessato dal servizio o che abbia modificato il proprio ambito di trattamento, su richiesta specifica dei responsabili ovvero della Direzione Risorse Umane e su indicazione dell'Amministratore di sistema;
• custodire la documentazione cartacea, prodotta nello svolgimento dei propri compiti istituzionali;

L’accesso agli addetti alla gestione e manutenzione è consentito unicamente ai soli dati personali la cui conoscenza sia strettamente necessaria per adempiere alle operazioni di manutenzione dei programmi o del sistema informatico.
A ciascun addetto alla manutenzione, previa sottoscrizione di apposito atto per accettazione, è pertanto consentito eseguire le operazioni strettamente necessarie a tali scopi e/o richieste dal titolare, secondo le seguenti istruzioni operative:
• Nel caso in cui sia necessario effettuare stampe di prova per controllare il funzionamento di stampanti o per verificare il funzionamento di strumenti o programmi installati, non utilizzare files già esistenti ma creare files di prova.
• Nel caso si renda strettamente necessario accedere a files contenenti dati (ad esempio per il recupero di un testo) limitare l’accesso ai dati per il tempo strettamente necessario all’assolvimento delle operazioni di manutenzione.
• Per effettuare operazioni di manutenzione sui database aziendali che prevedano la raccolta e la conservazione dei dati, tali dati dovranno essere custoditi in modo tale da non essere accessibili da soggetti non autorizzati.
• Devono inoltre essere adottate le misure di sicurezza minime previste dal codice in materia di protezione dei dati personali;
• E’ necessario informare al più presto il titolare o il responsabile del trattamento qualora si dovessero riscontrare malfunzionamenti o non conformità.
• Tutti i dati personali contenuti nei data base devono essere protetti da password;
• Nel caso in cui sia necessario accedere ai dati attraverso gli strumenti elettronici in dotazione agli incaricati, attenersi alle seguenti indicazioni:
o in presenza dell’incaricato, far digitare la password dall’incaricato stesso evitando di venirne a conoscenza;
o in assenza dell’incaricato rivolgersi alla persona individuata dall’incaricato quale proprio fiduciario il quale provvederà all’inserimento della password.
• Nei casi in cui sia necessario accedere ai dati personali attraverso il server, rivolgersi all’amministratore di sistema o provvedere, in collaborazione con l’amministratore di sistema stesso, alla creazione di credenziali di autenticazione da utilizzarsi esclusivamente per l’accesso da parte degli addetti alla manutenzione/gestione dei sistemi informatici;
• L’amministratore di sistema ha facoltà, in qualunque momento di controllare e verificare l’operato degli addetti alla manutenzione;
• Qualora si renda necessario prelevare apparecchiature elettroniche per effettuare attività di ripristino o interventi di manutenzione che comportino il reset di password precedentemente individuate, la nuova password di accesso sarà comunicata all’incaricato il quale provvederà a cambiarla al termine delle operazioni di manutenzione;
• l’accesso al sistema informatico da parte degli addetti alla manutenzione/gestione del sistema è consentito unicamente previo inserimento di password e ID;
• E’ assolutamente vietato comunicare o diffondere i dati personali di qualsiasi natura provenienti dai database gestiti dalla società, se non previa espressa comunicazione scritta;
• Nel caso in cui ci si avvalga di soggetti esterni per interventi specialistici che comportino trattamento di dati personali deve essere rilasciata una dichiarazione scritta dell’intervento effettuato che ne attesta la conformità alle disposizioni in materia di misure minime di sicurezza

7. OSSERVANZA DELLE DISPOSIZIONI IN MATERIA DI PROTEZIONE DATI PERSONALI

È obbligatorio attenersi alle disposizioni in materia di protezione dati personali e di misure minime di sicurezza, ai sensi del GDPR 2016/679 e della normativa nazionale in vigore.

8. NON OSSERVANZA DELLA NORMATIVA AZIENDALE

Il mancato rispetto o la violazione delle regole contenute nel presente regolamento è perseguibile con provvedimenti disciplinari nonché con le azioni civili e penali consentite.

9. AGGIORNAMENTO E REVISIONE

Tutti gli utenti possono proporre, quando ritenuto necessario, integrazioni al presente

Regolamento. Le proposte verranno esaminate dalla Direzione.
Il presente Regolamento è soggetto a revisione con frequenza annuale.

Data

La Direzione

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

VIOLAZIONE DI DATI PERSONALI

MODELLO DI NOTIFICA AL GARANTE

I titolari di trattamento di dati personali sono tenuti a notificare al Garante le violazioni dei dati personali (*data breach*) che comportano accidentalmente o in modo illecito la distruzione, la perdita, la modificazione, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati, anche nell'ambito delle comunicazioni elettroniche, a meno che sia improbabile che la violazione presenti un rischio per i diritti e le libertà degli interessati.

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Notifica di una violazione dei dati personali

(art. 33 del Regolamento (UE) 2016/679 – RGPD e art. 26 del d.lgs. 51/2018)

Tipo di notifica

○ Preliminare[1] ○ Completa ○ Integrativa[2]

Effettuata ai sensi del ○ art.33 RGPD ○ art.26 d.lgs 51/2018

Sez. A - Dati del soggetto che effettua la notifica

Cognome: Nome:

E-mail:

Recapito telefonico per eventuali comunicazioni:

Funzione rivestita:

Sez. B - Titolare del trattamento

Denominazione[3]:

Codice Fiscale/P.IVA: Soggetto privo di C.F./P.IVA ☐

Stato:

Indirizzo:

CAP : Città: Provincia:

Telefono :

Email :

PEC :

1 Il titolare del trattamento avvia il processo di notifica pur in assenza di un quadro completo della violazione con riserva di effettuare una successiva notifica integrativa. E' obbligatoria la compilazione delle sezioni A, B, B1 e C.

2 Il titolare del trattamento integra una precedente notifica (inserire il numero di fascicolo assegnato alla precedente notifica, se noto)

3 Indicare nome e cognome nel caso di persona fisica

Sez. B1 - Dati di contatto per informazioni relative alla violazione

Indicare i riferimenti del soggetto da contattare per ottenere maggiori informazioni circa la violazione

◯ Responsabile della protezione dei dati[4] - prot. n.

◯ Altro Soggetto[5]

Cognome: Nome:

E-mail:

Recapito telefonico per eventuali comunicazioni:

Funzione rivestita:

Sez. B2 - Ulteriori soggetti coinvolti nel trattamento

Indicare i riferimenti di ulteriori soggetti coinvolti ed il ruolo svolto (contitolare o responsabile del trattamento[6], rappresentante del titolare non stabilito nell'Ue)

Denominazione[7]:

Codice Fiscale/P.IVA: Soggetto privo di C.F./P.IVA ☐

Ruolo: ◯ Contitolare ◯ Responsabile ◯ Rappresentante

Denominazione:

Codice Fiscale/P.IVA: Soggetto privo di C.F./P.IVA ☐

Ruolo: ◯ Contitolare ◯ Responsabile ◯ Rappresentante

Denominazione:

Codice Fiscale/P.IVA: Soggetto privo di C.F./P.IVA ☐

Ruolo: Contitolare ◯ Responsabile ◯ Rappresentante

4 Qualora designato, indicare il numero di protocollo assegnato alla comunicazione dei dati di contatto del RPD
5 In assenza di un RPD, indicare i riferimenti di un punto di contatto designato per la notifica in questione
6 In tale tipologia rientra anche il Responsabile individuato ai sensi art. 28, par. 4
7 Indicare nome e cognome nel caso di persona fisica

Sez. C - Informazioni di sintesi sulla violazione

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

1. **Indicare quando è avvenuta la violazione.**

- ◯ Il
- ◯ Dal (La violazione è ancora in corso)
- ◯ Dal al
- ◯ In un tempo non ancora determinato

Ulteriori informazioni circa le date in cui è avvenuta la violazione

2. **Momento in cui il titolare del trattamento è venuto a conoscenza della violazione**

Data: Ora:

3. **Modalità con la quale il titolare del trattamento è venuto a conoscenza della violazione**

- ◯ Il titolare è stato informato dal responsabile del trattamento
- ◯ Altro[8]

4. In caso di notifica oltre le 72 ore, quali sono i motivi del ritardo?[9]

5. Breve descrizione della violazione

8 Ad esempio: Segnalazione da parte di un interessato, comunicazione da parte di terzi, ecc.

9 Da compilare solo per notifiche tardive.

6. Natura della violazione

☐ a) Perdita di confidenzialità[10]

☐ b) Perdita di integrità[11]

☐ c) Perdita di disponibilità[12]

7. Causa della violazione

☐ Azione intenzionale interna

☐ Azione accidentale interna

☐ Azione intenzionale esterna

☐ Azione accidentale esterna

☐ Sconosciuta

☐ Altro (specificare)

8. Categorie di dati personali oggetto di violazione

☐ Dati anagrafici (nome, cognome, sesso, data di nascita, codice fiscale, altro...)

☐ Dati di contatto (indirizzo postale o di posta elettronica, numero di telefono fisso o mobile)

☐ Dati di accesso e di identificazione (username, password, customer ID, altro...)

☐ Dati di pagamento (numero di conto corrente, dettagli della carta di credito, altro...)

☐ Dati relativi alla fornitura di un servizio di comunicazione elettronica (dati di traffico, dati relativi alla navigazione internet, altro...)

☐ Dati relativi a condanne penali e ai reati o a connessione misure di sicurezza o di prevenzione

☐ Dati di profilazione

10 Diffusione/ accesso non autorizzato o accidentale

11 Modifica non autorizzata o accidentale

12 Impossibilità di accesso,perdita, distruzione non autorizzata o accidentale

☐ Dati relativi a documenti di identificazione/riconoscimento (carta d'identità, passaporto, patente, CNS, altro...)

☐ Dati di localizzazione

☐ Dati che rivelino l'origine razziale o etnica

☐ Dati che rivelino opinioni politiche

☐ Dati che rivelino convinzioni religiose o filosofiche

☐ Dati che rivelino l'appartenenza sindacale

☐ Dati relativi alla vita sessuale o all'orientamento sessuale

☐ Dati relativi alla salute

☐ Dati genetici

☐ Dati biometrici

☐ Categorie non ancora determinate

☐ Altro

9. Indicare il volume (anche approssimativo) dei dati personali oggetto di violazione[13]

◯ N.

◯ Circa N.

◯ Un numero (ancora) non definito di dati

10. Categorie di interessati coinvolti nella violazione

☐ Dipendenti/Consulenti

☐ Utenti/Contraenti/Abbonati/Clienti (attuali o potenziali)

☐ Associati, soci, aderenti, simpatizzanti, sostenitori

☐ Soggetti che ricoprono cariche sociali

☐ Beneficiari o assistiti

☐ Pazienti

☐ Minori

☐ Persone vulnerabili (es. vittime di violenze o abusi, rifugiati, richiedenti asilo)

13 Ad esempio numero di referti, numero di record di un database, numero di transazioni registrate.

☐ Categorie ancora non determinate

☐ Altro (specificare)

☐ Ulteriori dettagli circa le categorie di interessati

11. Numero (anche approssimativo) di interessati coinvolti nella violazione

- ◯ N. interessati
- ◯ Circa n. interessati
- ◯ Un numero (ancora) sconosciuto di interessati

Sez. D - Informazioni di dettaglio sulla violazione

1. Descrizione dell'incidente di sicurezza alla base della violazione[14]

2. Descrizione delle categorie di dati personali oggetto della violazione[15]

14 Segue punto 5, 6 e 7 della sez. C

15 Segue punto 8 della sez. C

3. Descrizione dei sistemi e delle infrastrutture IT coinvolti nell'incidente, con indicazione della loro ubicazione

4. Misure di sicurezza tecniche e organizzative adottate per garantire la sicurezza dei dati, dei sistemi e delle infrastrutture IT coinvolti[16]

Sez. E - Informazioni di sintesi sulla violazione

1. Possibili conseguenze della violazione sugli interessati

a) In caso di perdita di confidenzialità:17

☐ I dati sono stati divulgati al di fuori di quanto previsto dall'informativa ovvero dalla disciplina di riferimento

☐ I dati possono essere correlati, senza sforzo irragionevole, ad altre informazioni relative agli interessati

☐ I dati possono essere utilizzati per finalità diverse da quelle previste oppure in modo non lecito

☐ Altro (specificare)

16 Indicare le misure in essere al momento della violazione

17 Da compilare solo nel caso in cui è stata selezionata l'opzione a) del punto 6, Sez. C

b) In caso di perdita di integrità:18

☐ I dati sono stati modificati e resi incosistenti

☐ I dati sono stati modificati mantenendo la consistenza

☐ Altro (specificare)

c) In caso di perdita di disponibilità:19

☐ Mancato accesso a servizi

☐ Malfunzionamento e difficoltà nell'utilizzo di servizi

☐ Altro (specificare)

Ulteriori considerazioni sulle possibili conseguenze

2. Potenziali effetti negativi per gli interessati

☐ Perdita del controllo dei dati personali

☐ Limitazione dei diritti

☐ Discriminazione

☐ Furto o usurpazione d'identità

☐ Frodi

☐ Perdite finanziarie

18 Da compilare solo nel caso in cui è stata selezionata l'opzione b) del punto 6, Sez. C

19 Da compilare solo nel caso in cui è stata selezionata l'opzione c) del punto 6, Sez. C

☐ Decifratura non autorizzata della pseudonimizzazione

☐ Pregiduzio alla reputazione

☐ Perdita di riservatezza dei dati personali protetti da segreto professionale

☐ Conoscenza da parte di terzi non autorizzati

Qualsiasi altro danno economico o sociale significativo (specificare)

3. Stima della gravità della violazione

◯ Trascurabile

◯ Basso

◯

Medio

Alto

Indicare le motivazioni

Sez. F - Misure adottate a seguito della violazione

1. Misure tecniche e organizzative adottate (o di cui si propone l'adozione[20]) per porre rimedio alla violazione e ridurne gli effetti negativi per gli interessati

20 Nella descrizione distinguere le misure adottate da quelle in corso di adozione

2. Misure tecniche e organizzative adottate (o di cui si propone l'adozione) per prevenire simili violazioni in futuro

Sez. G - Comucazione agli interessati

1. La violazione è stata comunicata agli interessati?

Si, è stata comunicata il

◯ No, sarà comunicata

il

in una data da definire

◯ No, sono tuttora in corso le dovute valutazioni[21]

◯ No e non sarà comunicata perché:

☐ a) il titolare del trattamento ritiene che la violazione dei dati personali non presenti un rischio elevato per i diritti e le libertà delle persone fisiche;

Spiegare le motivazioni

21 Selezionando questa opzione, il titolare del trattamento si impegna a effettuare una integrazione alla presente notifica

☐ b) il titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto **d**ella violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi;

Descrivere le misure applicate

☐ c) il titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati;

Descrivere le misure adottate

☐ d) detta comunicazione richiederebbe sforzi sproporzionati.

Descrivere la modalità (comunicazione pubblica o misura simile) tramite la quale gli interessati sono stati informati.

2. Numero di interessati a cui è stata comunicata la violazione[22]

N. interessati

22 Da compilare solo nel caso in cui al punto 1 venga scelta una delle prime due opzioni.

3. Contenuto della comunicazione agli interessati

4. Canale utilizzato per la comunicazione agli interessati

☐ SMS

☐ Posta cartacea

☐ Posta elettronica

☐ Altro (specificare)

Sez. H - Altre informazioni

1. **La violazione coinvolge interessati di altri Paesi dello Spazio Economico Europeo?[23]**

- ◯ Si (indicare quali)
- ◯ No

2. **La violazione coinvolge interessati di altri Paesi non appartenenti allo Spazio Economico Europeo?**

- ◯ Si (indicare quali)
- ◯ No

23 Fanno parte dello Spazio Economico Europeo tutti gli Stati membri della Unione Europea, nonchè l'Islanda, il Liechtenstein e la Norvegia

3. La violazione è stata notificata ad altre autorità di controllo?[24]

- ◯ Si (indicare quali)
- ◯ No

4. La violazione è stata notificata ad altri organismi di vigilanza o di controllo in virtù di ulteriori disposizioni normative?[25]

- ◯ Si (indicare quali)
- ◯ No

5. E' stata effettuata una segnalazione all'autorità giudiziaria o di polizia?

- ◯ Si
- ◯ No

24 Autorità di controllo così come definite ex art. 51 del Regolamento (UE) 2016/679

25 Ad esempio: Regolamento (UE) 910/2014 (eIDAS), d.lgs. 65/2018 attuativo della Direttiva (UE) 2016/1148 (NIS)

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

INFORMAZIONI SUL TRATTAMENTO DEI DATI PERSONALI

Ai sensi dell'articolo 13 del Regolamento (UE) 2016/679 si rappresenta che il Garante per la protezione dei dati personali, in qualità di titolare del trattamento (con sede in Piazza Venezia 11, IT-00187, Roma; Email: garante@gpdp.it; PEC: protocollo@pec.gpdp.it; Centralino: +39 06696771), tratterà i dati personali conferiti con il presente modulo, con modalità prevalentemente informatiche e telematiche, per le finalità previste dal Regolamento (UE) 2016/679 e dal Codice in materia di protezione dei dati personali (d.lgs. 30 giugno 2003,
n. 196 e s.m.i.), in particolare per l'esecuzione dei propri compiti di interesse pubblico o comunque connessi all'esercizio dei propri pubblici poteri attribuiti al Garante dalla disciplina vigente.

Il conferimento dei dati, fermo restando quanto previsto dall'art. 33, par. 4, del Regolamento (UE) 2016/679, è obbligatorio e la loro mancata indicazione non consente di ritenere adempiuto il dovere di notificazione della violazione all'autorità di controllo. I dati acquisiti nell'ambito della procedura saranno conservati in conformità alle norme sulla conservazione della documentazione amministrativa.

I dati saranno trattati esclusivamente dal personale e da collaboratori del Garante o delle imprese espressamente designate come responsabili del trattamento. Al di fuori di queste ipotesi, i dati non saranno diffusi, né saranno comunicati a terzi, fatti salvi i casi in cui si renda necessario comunicarli ad altri soggetti coinvolti nell'attività istruttoria e nei casi specificamente previsti dal diritto nazionale o dell'Unione europea.

Gli interessati hanno il diritto di ottenere dal Garante, nei casi previsti, l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento che li riguarda o di opporsi al trattamento (artt. 15 e ss. del Regolamento UE 2016/679). L'apposita istanza è presentata contattando il Responsabile della protezione dei dati presso il Garante (Garante per la protezione dei personali - Responsabile della Protezione dei dati personali, Piazza Venezia 11, 00187, Roma, email: rpd@gpdp.it).

Gli interessati che ritengono che il trattamento dei dati personali a loro riferiti avvenga in violazione di quanto previsto dalla disciplina in materia di protezione dei dati personali hanno il diritto di proporre reclamo al Garante, come previsto dall'art. 77 del Regolamento (UE) 2016/679, o di adire le opportune sedi giudiziarie ai sensi dell'art. art. 79 del Regolamento citato.

All’attenzione di
(indicare il titolare del trattamento)

ESERCIZIO DI DIRITTI IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

(artt. 15-22 del Regolamento (UE) 2016/679)

Il/La sottoscritto/a…….
nato/a a…….il……, esercita con la presente richiesta i seguenti diritti di cui agli artt. 15-22 del Regolamento (UE) 2016/679:

1. Accesso ai dati personali

(art. 15 del Regolamento (UE) 2016/679)

Il sottoscritto *(barrare solo le caselle che interessano)*:

chiede conferma che sia o meno in corso un trattamento di dati personali che lo riguardano;

in caso di conferma, chiede di ottenere l'accesso a tali dati, una copia degli stessi, e tutte le informazioni previste alle lettere da a) a h) dell’art. 15, paragrafo 1, del Regolamento (UE) 2016/679, e in particolare;

- le finalità del trattamento;
- le categorie di dati personali trattate;
- i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare se destinatari di paesi terzi o organizzazioni internazionali;
- il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
- l’origine dei dati (ovvero il soggetto o la specifica fonte dalla quale essi sono stati acquisiti);
- l'esistenza di un processo decisionale automatizzato, compresa la profilazione, e le informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

2. Richiesta di intervento sui dati

(artt. 16-18 del Regolamento (UE) 2016/679)

Il sottoscritto chiede di effettuare le seguenti operazioni *(barrare solo le caselle che interessano)*:

rettificazione e/o aggiornamento dei dati (art. 16 del Regolamento (UE) 2016/679);

cancellazione dei dati (art. 17, paragrafo 1, del Regolamento (UE) 2016/679), per i seguenti motivi *(specificare quali)*:

a)…;

b)….;

c)…;

nei casi previsti all'art. 17, paragrafo 2, del Regolamento (UE) 2016/679, l'attestazione che il titolare ha informato altri titolari di trattamento della richiesta dell'interessato di cancellare link, copie o riproduzioni dei suoi dati personali;

limitazione del trattamento (art. 18) per i seguenti motivi *(barrare le caselle che interessano)*:

contesta l'esattezza dei dati personali;

il trattamento dei dati è illecito;

i dati sono necessari all'interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria;

l'interessato si è opposto al trattamento dei dati ai sensi dell'art. 21, paragrafo 1, del Regolamento (UE) 2016/679.

La presente richiesta riguarda (indicare i dati personali, le categorie di dati o il trattamento cui si fa riferimento):

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

3.Portabilità dei dati

(art. 20 del Regolamento (UE) 2016/679)

Con riferimento a tutti i dati personali forniti al titolare, il sottoscritto chiede di *(barrare solo le caselle che interessano)*:

ricevere tali dati in un formato strutturato, di uso comune e leggibile da dispositivo automatico;

trasmettere direttamente al seguente diverso titolare del trattamento *(specificare i riferimenti identificativi e di contatto del titolare: ……..):*

tutti i dati personali forniti al titolare;

un sottoinsieme di tali dati.

La presente richiesta riguarda (indicare i dati personali, le categorie di dati o il trattamento cui si fa riferimento):

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

4. Opposizione al trattamento

(art. 21, paragrafo 1 del Regolamento (UE) 2016/679)

Il sottoscritto si oppone al trattamento dei suoi dati personali ai sensi dell'art. 6, paragrafo 1, lettera e) o lettera f), per i seguenti motivi legati alla sua situazione particolare (specificare):

_____
_____
_____
_____
_____
_____
_____

5. Opposizione al trattamento per fini di marketing diretto

(art. 21, paragrafo 2 del Regolamento (UE) 2016/679)

Il sottoscritto si oppone al trattamento dei dati effettuato a fini di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale.

Il sottoscritto:

Chiede di essere informato, ai sensi dell'art. 12, paragrafo 4 del Regolamento (UE) 2016/679, al più tardi entro un mese dal ricevimento della presente richiesta, degli eventuali motivi che impediscono al titolare di fornire le informazioni o svolgere le operazioni richieste.

Chiede, in particolare, di essere informato della sussistenza di eventuali condizioni che impediscono al titolare di identificarlo come interessato, ai sensi dell'art. 11, paragrafo 2, del Regolamento (UE) 2016/679.

Recapito per la risposta:

Via/Piazza

Comune Provincia Codice postale

oppure

e-mail/PEC:

Eventuali precisazioni

Il sottoscritto precisa (fornire eventuali spiegazioni utili o indicare eventuali documenti allegati):

(Luogo e data)

(Firma)

INFORMATIVA CLIENTI AL TRATTAMENTO DEI DATI PERSONALI

I dati personali dell'utente sono utilizzati da Studio Legale Associato Felicetti Frascarelli Menghini Studio Associato, che ne è titolare per il trattamento, nel rispetto dei principi di protezione dei dati personali stabiliti dal Regolamento GDPR 2016/679 e della normativa nazionale in vigore.

MODALITÀ E FINALITÀ DEL TRATTAMENTO DATI

1. La informiamo che i dati verranno trattati con il supporto dei seguenti mezzi:
   - Mista - elettronica e cartacea

   con le seguenti finalità:
   - Acquisizione di prove
   - Adempimento di obblighi fiscali o contabili
   - Amministrazione della giustizia (procedimenti giudiziari civili, penali, amministrativi e tributari)
   - Attività di consulenza
   - Compilazione schede di notificazione
   - Contratto di assunzione
   - Difesa del suolo, tutela dell'ambiente e della sicurezza della popolazione
   - Documentazione di beni e patrimoni (tenuta di beni mobili e immobiliari, archivi catastali)
   - Elaborazione, stampa, imbustamento e spedizione delle fatture
   - Erogazione del servizio fornito
   - Gestione del contenzioso (contratti, ordini, arrivi, fatture)
   - Gestione del patrimonio mobiliare e immobiliare
   - Gestione del personale per conto dei clienti
   - Gestione della clientela (contratti, ordini, spedizioni e fatture)
   - Informazione scientifica e giuridica
   - Protezione della proprietà
   - Protezione e incolumità degli individui
   - Relazioni con il pubblico
   - Servizi a tutela di consumatori e utenti

In particolare, per le finalità specificate di seguito i dati dell'utente saranno trattati SOLO su specifica accettazione del consenso:

- Consenso al trattamento di dati particolari:

  ☐ accetta ☐ non accetta

- Consenso al trattamento di dati di minori (almeno 14 anni):

  ☐ accetta ☐ non accetta

BASE GIURIDICA

2. La base giuridica su cui si fonda il trattamento per i dati comuni, secondo l'Art.6 del Regolamento GDPR, è:
   - Contratto;

La base giuridica su cui si fonda il trattamento per categorie particolari di dati personali, secondo l'Art.9 del Regolamento GDPR, è:

- Consenso;

La società tratta i dati facoltativi degli utenti in base al consenso, ossia mediante l'approvazione esplicita della presente policy privacy e in relazione alle modalità e finalità di seguito descritte.

CATEGORIE DI DESTINATARI

3. Ferme restando le comunicazioni eseguite in adempimento di obblighi di legge e contrattuali, tutti i dati raccolti ed elaborati potranno essere comunicati esclusivamente per le finalità sopra specificate alle seguenti categorie di destinatari:
   - Agenzia delle Entrate;
   - Altre amministrazioni pubbliche;
   - Autorità di vigilanza e controllo;
   - Banche e istituti di credito;
   - Call center per assistenza clienti;
   - Camere di commercio, industria, artigianato ed agricoltura;
   - Centrali dei rischi;
   - Consulenti e liberi professionisti anche in forma associata;
   - Enti bilaterali e casse edili;
   - Enti locali;
   - Enti previdenziali ed assistenziali;
   - Enti pubblici economici;
   - Enti pubblici non economici;
   - Familiari dell'interessato;
   - Fondi di assistenza sanitaria integrativa;
   - Fondi di previdenza complementare;
   - Forze armate;
   - Forze di polizia;
   - Imprese di assicurazione;
   - Interessati;
   - Istituti e scuole di ogni ordine e grado e università;
   - Medico competente;
   - Ordini e collegi professionali;
   - Organi costituzionali o di rilievo costituzionale;
   - Organismi paritetici in materia di lavoro ;
   - Organismi per i collegi professionali;
   - Organismi sanitari, personale medico e paramedico;
   - Organizzazioni sindacali e patronati ;
   - Persone autorizzate;
   - Rappresentante dei lavoratori per la sicurezza;
   - Società che effettuano servizi di recapito postale;
   - Società di gestione per il controllo delle frodi;
   - Soggetti che svolgono attività di archiviazione della documentazione;
   - Studi legali;
   - Uffici giudiziari;

Nella gestione dei suoi dati, inoltre, possono venire a conoscenza degli stessi le categorie di persone autorizzate e/o responsabili interni ed esterni individuati ed ai quali sono state fornite specifiche istruzioni scritte circa il trattamento dei dati.

PERIODO DI CONSERVAZIONE

4. I dati obbligatori ai fini contrattuali e contabili sono conservati per il tempo necessario allo svolgimento del rapporto commerciale e contabile.
   I dati di chi non acquista o usufruisce di prodotti/servizi, pur avendo avuto un precedente contatto con dei rappresentanti dell'azienda, saranno immediatamente cancellati o trattati in forma anonima, ove la loro conservazione non risulti altrimenti giustificata, salvo che sia stato acquisito validamente il consenso informato degli interessati relativo ad una successiva attività di promozione commerciale o ricerca di mercato.

   Il periodo di conservazione dei dati è: I dati saranno trattati per tutto il tempo necessario allo svolgimento dell'incarico professionale in essere e per i successivi dieci anni dalla data di cessazione dello stesso.

DIRITTI DELL'INTERESSATO

5. Ai sensi del Regolamento europeo 679/2016 (GDPR) e della normativa nazionale in vigore, l'interessato può, secondo le modalità e nei limiti previsti dalla vigente normativa, esercitare i seguenti diritti:

   - richiedere la conferma dell'esistenza di dati personali che lo riguardano (diritto di accesso dell'interessato – art. 15 del Regolamento 679/2016);
   - conoscerne l'origine;
   - riceverne comunicazione intelligibile;
   - avere informazioni circa la logica, le modalità e le finalità del trattamento;
   - richiederne l'aggiornamento, la rettifica, l'integrazione, la cancellazione, la trasformazione in forma anonima, il blocco dei dati trattati in violazione di legge, ivi compresi quelli non più necessari al perseguimento degli scopi per i quali sono stati raccolti (diritto di rettifica e cancellazione – artt. 16 e 17 del Regolamento 679/2016);
   - diritto di limitazione e/o di opposizione al trattamento dei dati che lo riguardano (art. 18 del Regolamento 679/2016);
   - diritto di revoca;
   - diritto alla portabilità dei dati (art. 20 del Regolamento 679/2016);
   - nei casi di trattamento basato su consenso, ricevere i propri dati forniti al titolare, in forma strutturata e leggibile da un elaboratore di dati e in un formato comunemente usato da un dispositivo elettronico;
   - il diritto di presentare un reclamo all'Autorità di controllo (diritto di accesso dell'interessato – art. 15 del Regolamento 679/2016).

6. Titolare del trattamento dei Suoi dati personali è Studio Legale Associato Felicetti Frascarelli Menghini Studio Associato, p.iva 02287020545, c.f. 02287020545
   - Email: studio.ffm@tin.it
   - PEC: dimitri.frascarelli@avvocatispoleto.legalmail.it
   - Telefono: 0742 780573

   Studio Legale Associato Felicetti Frascarelli Menghini, p.iva 02287020545

7. Contitolari del trattamento dei Suoi dati personali sono:
   - Felicetti Mauro, c.f. FLCMRA53H16D653Y
     - Email: mauro.felicetti@studioffm.it
     - PEC: mauro.felicetti@avvocatispoleto.legalmail.it
     - Telefono: 0742 780573
   - Frascarelli Dimitri, c.f. FRSDTR60M12F492M
     - Email: dimitri.frascarelli@studioffm.it
     - PEC: dimitri.frascarelli@avvocatispoleto.legalmail.it

- Telefono: 0742 780573
- Menghini Alberto, c.f. MNGLRT65D17D653D
  - Email: alberto.menghini@studioffm.it
  - PEC: alberto.menghini@avvocatispoleto.legalmail.it
  - Telefono: 0742 780573

****

Il/I sottoscritto/i in calce identificato/i dichiara di aver ricevuto completa informativa ai sensi dell'art. 13 del Regolamento UE 2016/679 e della normativa nazionale in vigore, ed esprime il consenso al trattamento ed alla comunicazione dei propri dati personali con particolare riguardo a quelli cosiddetti particolari nei limiti, per le finalità e per la durata precisati nell'informativa.

Data Firma

_____ _____

CONSENSO INFORMATO PER GENITORI/TUTORE LEGALE

Io sottoscritta (madre/tutore) _____
nata il ___/___/_____residente a_____ via/piazza _____ Tel._____ domicilio (se diverso dalla residenza) _____

Io sottoscritto (padre/tutore) _____
nato il ___/___/_____residente a_____ via/piazza _____ Tel. _____ domicilio (se diverso dalla residenza) _____

del minore _____ nato il ___/___/_____
residente a_____ via/piazza _____

dichiaro di aver ricevuto completa informativa ai sensi dell'art. 13 del Regolamento UE 2016/679 e della normativa nazionale in vigore, ed esprimo il consenso al trattamento ed alla comunicazione dei dati personali di mio figlio/a, con particolare riguardo a quelli cosiddetti particolari, nei limiti, per le finalità e per la durata precisati nell'informativa fornitami con il presente documento.

_____	___/___/_____	_____
Nome per esteso del genitore/tutore legale	Data	Firma
_____	___/___/_____	_____
Nome per esteso del genitore/tutore legale	Data	Firma

INFORMATIVA FORNITORI AL TRATTAMENTO DEI DATI PERSONALI

I dati personali dell'utente sono utilizzati da Studio Legale Associato Felicetti Frascarelli Menghini Studio Associato, che ne è titolare per il trattamento, nel rispetto dei principi di protezione dei dati personali stabiliti dal Regolamento GDPR 2016/679 e della normativa nazionale in vigore.

MODALITÀ E FINALITÀ DEL TRATTAMENTO DATI

1. La informiamo che i dati verranno trattati con il supporto dei seguenti mezzi:
   - Mista - elettronica e cartacea

   con le seguenti finalità:
   - Adempimento di obblighi di legge connessi a rapporti commerciali
   - Adempimento di obblighi fiscali o contabili
   - Elaborazione, stampa, imbustamento e spedizione delle fatture
   - Erogazione del servizio fornito
   - Gestione dei fornitori (contratti, ordini, arrivi, fatture)
   - Gestione del contenzioso (contratti, ordini, arrivi, fatture)

BASE GIURIDICA

2. La base giuridica su cui si fonda il trattamento per i dati comuni, secondo l'Art.6 del Regolamento GDPR, è:
   - Contratto;

CATEGORIE DI DESTINATARI

3. Ferme restando le comunicazioni eseguite in adempimento di obblighi di legge e contrattuali, tutti i dati raccolti ed elaborati potranno essere comunicati esclusivamente per le finalità sopra specificate alle seguenti categorie di destinatari:
   - Banche e istituti di credito;
   - Consulenti e liberi professionisti anche in forma associata;
   - Società che effettuano il servizio di logistica di magazzino e trasporto;
   - Società che effettuano servizi di recapito postale;

Nella gestione dei suoi dati, inoltre, possono venire a conoscenza degli stessi le categorie di persone autorizzate e/o responsabili interni ed esterni individuati ed ai quali sono state fornite specifiche istruzioni scritte circa il trattamento dei dati.

PERIODO DI CONSERVAZIONE

4. I dati obbligatori ai fini contrattuali e contabili sono conservati per il tempo necessario allo svolgimento del rapporto commerciale e contabile.
   I dati di chi non acquista o usufruisce di prodotti/servizi, pur avendo avuto un precedente contatto con dei rappresentanti dell'azienda, saranno immediatamente cancellati o trattati in forma anonima, ove la loro conservazione non risulti altrimenti giustificata, salvo che sia stato acquisito validamente il consenso informato degli interessati relativo ad una successiva attività di promozione commerciale o ricerca di mercato.

   Il periodo di conservazione dei dati è: I dati saranno trattati per tutto il tempo necessario allo svolgimento del rapporto commerciale in essere e per i successivi dieci anni dalla data di cessazione dello stesso.

DIRITTI DELL'INTERESSATO

5. Ai sensi del Regolamento europeo 679/2016 (GDPR) e della normativa nazionale in vigore, l'interessato può, secondo le modalità e nei limiti previsti dalla vigente normativa,

esercitare i seguenti diritti:

- richiedere la conferma dell'esistenza di dati personali che lo riguardano (diritto di accesso dell'interessato – art. 15 del Regolamento 679/2016);
- conoscerne l'origine;
- riceverne comunicazione intelligibile;
- avere informazioni circa la logica, le modalità e le finalità del trattamento;
- richiederne l'aggiornamento, la rettifica, l'integrazione, la cancellazione, la trasformazione in forma anonima, il blocco dei dati trattati in violazione di legge, ivi compresi quelli non più necessari al perseguimento degli scopi per i quali sono stati raccolti (diritto di rettifica e cancellazione – artt. 16 e 17 del Regolamento 679/2016);
- diritto di limitazione o di opposizione al trattamento dei dati che lo riguardano (art. 18 del Regolamento 679/2016);
- diritto di revoca;
- diritto alla portabilità dei dati (art. 20 del Regolamento 679/2016);
- nei casi di trattamento basato su consenso, ricevere i propri dati forniti al titolare, in forma strutturata e leggibile da un elaboratore di dati e in un formato comunemente usato da un dispositivo elettronico;
- il diritto di presentare un reclamo all'Autorità di controllo (diritto di accesso dell'interessato – art. 15 del Regolamento 679/2016).

6. Titolare del trattamento dei Suoi dati personali è Studio Legale Associato Felicetti Frascarelli Menghini Studio Associato, p.iva 02287020545, c.f. 02287020545
   - Email: studio.ffm@tin.it
   - PEC: dimitri.frascarelli@avvocatispoleto.legalmail.it
   - Telefono: 0742 780573

   Studio Legale Associato Felicetti Frascarelli Menghini, p.iva 02287020545

7. Contitolari del trattamento dei Suoi dati personali sono:
   - Felicetti Mauro, c.f. FLCMRA53H16D653Y
     - Email: mauro.felicetti@studioffm.it
     - PEC: mauro.felicetti@avvocatispoleto.legalmail.it
     - Telefono: 0742 780573
   - Frascarelli Dimitri, c.f. FRSDTR60M12F492M
     - Email: dimitri.frascarelli@studioffm.it
     - PEC: dimitri.frascarelli@avvocatispoleto.legalmail.it
     - Telefono: 0742 780573
   - Menghini Alberto, c.f. MNGLRT65D17D653D
     - Email: alberto.menghini@studioffm.it
     - PEC: alberto.menghini@avvocatispoleto.legalmail.it
     - Telefono: 0742 780573

MODELLO COMUNICAZIONE AL GARANTE DEI DATI DELL'RPD AI SENSI DELL'ART. 37, PAR. 1, LETT. *A*) E PAR. 7, DEL RGPD

DATI DEL TITOLARE/RESPONSABILE DEL TRATTAMENTO

Denominazione ente: Studio Legale Associato Felicetti Frascarelli Menghini

Codice Fiscale /P.Iva: 02287020545

Via / Piazza: Via Sant' Egidio N. civico: 56

Città: Trevi Cap: 06039 Provincia: PG

Telefono: 0742 780573 Fax ……

Email: studio.ffm@tin.it Pec: dimitri.frascarelli@avvocatispoleto.legalmail.it

Sito istituzionale ……

DATI DEL RESPONSABILE DELLA PROTEZIONE DEI DATI