GDPR - EU General Data Protection Regulation
Regolamento Europeo 2016/679
in materia di protezione dei dati personali

GDPR

Registro dei Trattamenti

Ai sensi dell'Art. 30 del R.E. 2016/679

Titolare del trattamento

KENT SERVICE S.R.L.
VIA A. MORO 109
SAN DONATO MIL.SE

Sommario

1. SCOPO (ART. 30)

Il presente Registro dei Trattamenti (di seguito “Registro”) è adottato ai sensi dell’Art. 30 del Regolamento Europeo 2016/679 (di seguito “Regolamento”), per tracciare tutte le categorie di attività di trattamento, svolte per conto di un titolare di trattamento, in materia di dati personali, i criteri organizzativi adottati e le misure per la protezione dei dati personali.

In particolare il Registro dei Trattamenti contiene idonee informazioni riguardo:

- il nome e le generalità del titolare del trattamento e, ove nominato, del contitolare del trattamento, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati;
- le finalità del trattamento;
- una descrizione delle categorie di interessati e delle categorie di dati personali da trattare;
- le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi rispetto all’Europa o le organizzazioni internazionali;
- i trasferimenti di dati personali verso un paese terzo o ad un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adottate;
- ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati, la cui cancellazione viene comunque garantita non appena il trattamento non sia più necessario;
- ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1.

Su richiesta, il titolare del trattamento od il responsabile del trattamento, od i loro rappresentanti mettono il registro a disposizione dell'autorità di controllo.

2. DEFINIZIONI (ART. 4)

Ai fini del presente registro s'intende per:

1) «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, dati relativi all'ubicazione, un codice online o ad uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale, sempre che sia sufficiente a caratterizzarlo in maniera univoca;

2) «trattamento»: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicata a dati personali o insiemi di dati personali, come la loro 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;

3) «limitazione di trattamento»: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;

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

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

6) «archivio»: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale e/o geografico;

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

8) «responsabile del trattamento»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;

9) «destinatario»: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari. Il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento;

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

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

12) «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;

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

14) «dati biometrici»: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali, a titolo meramente esemplificativo, l'immagine facciale o i dati dattiloscopici;

15) «dati relativi alla salute»: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;

16) «stabilimento principale»:

a) per quanto riguarda un titolare del trattamento con stabilimenti in più di uno Stato membro è il luogo della sua amministrazione centrale nell'Unione, salvo che le decisioni sulle finalità e i mezzi del trattamento di dati personali siano adottate in un altro stabilimento del titolare del trattamento nell'ambito dell'Unione e che quest'ultimo stabilimento abbia facoltà di ordinare l'esecuzione di tali decisioni: nel qual caso lo stabilimento che ha adottato siffatte decisioni è considerato essere lo stabilimento principale;

b) con riferimento ad un responsabile del trattamento con stabilimenti in più di uno Stato membro, è il luogo in cui ha sede la sua amministrazione centrale nell'Unione o, se il responsabile del trattamento non ha un'amministrazione centrale nell'Unione, lo stabilimento del responsabile del trattamento nell'Unione in cui sono condotte le principali attività di trattamento;

17) «rappresentante»: la persona fisica o giuridica stabilita nell'Unione che, designata dal titolare del trattamento o dal responsabile del trattamento per iscritto ai sensi dell'articolo 27, li rappresenta per quanto riguarda gli obblighi rispettivi a norma del presente regolamento;

18) «impresa»: la persona fisica o giuridica, indipendentemente dalla forma giuridica rivestita, che eserciti un'attività economica, comprendente le società di persone o le associazioni che esercitano regolarmente un'attività economica;

19) «gruppo imprenditoriale»: un gruppo costituito da un'impresa controllante e dalle imprese da questa controllate;

20) «norme vincolanti d'impresa»: le politiche in materia di protezione dei dati personali applicate da un titolare del trattamento o responsabile del trattamento stabilito nel territorio di uno Stato membro al trasferimento o al complesso di trasferimenti di dati personali a un titolare del trattamento o responsabile del trattamento in uno o più paesi terzi, nell'ambito di un gruppo imprenditoriale o di un gruppo di imprese che svolge un'attività economica comune;

21) «autorità di controllo»: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51;

22) «autorità di controllo interessata»: un'autorità di controllo interessata dal trattamento di dati personali in quanto:

a) Il titolare del trattamento od il responsabile del trattamento è stabilito sul territorio dello Stato membro di tale autorità di controllo;

b)gli interessati che risiedono nello Stato membro dell'autorità di controllo sono o sono probabilmente influenzati in modo sostanziale dal trattamento; oppure

c) un reclamo è stato proposto a tale autorità di controllo;

23) «trattamento transfrontaliero»:

a) trattamento di dati personali che ha luogo nell'ambito delle attività di stabilimenti in più di uno Stato membro di un titolare del trattamento o responsabile del trattamento nell'Unione ove il titolare del trattamento o il responsabile del trattamento siano stabiliti in più di uno Stato membro; oppure

b)trattamento di dati personali che ha luogo nell'ambito delle attività di un unico stabilimento di un titolare del trattamento o responsabile del trattamento nell'Unione, ma che incide o probabilmente incide in modo sostanziale su interessati in più di uno Stato membro;

24) «obiezione pertinente e motivata»: un'obiezione al progetto di decisione sul fatto che vi sia o meno una violazione del presente regolamento, oppure che l'azione prevista in relazione al titolare del trattamento o responsabile del trattamento sia conforme al presente regolamento, la quale obiezione dimostra chiaramente la rilevanza dei rischi posti dal progetto di decisione riguardo ai diritti e alle libertà fondamentali degli interessati e, ove applicabile, alla libera circolazione dei dati personali all'interno dell'Unione;

25) «servizio della società dell'informazione»: il servizio definito all'articolo 1, paragrafo 1, lettera b), della direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio (19);

26) «organizzazione internazionale»: un'organizzazione e gli organismi di diritto internazionale pubblico a essa subordinati o qualsiasi altro organismo istituito da o sulla base di un accordo tra due o più Stati.

3. RIFERIMENTO NORMATIVO

Il Registro è tenuto in osservanza alle seguenti normative:

- Regolamento Europeo 2016/679, Art. 30

4. CAMPO DI APPLICAZIONE

Il Registro ha lo scopo di censire le banche dati in cui vengono memorizzati i dati personali ed i relativi flussi informativi che li coinvolgono, le politiche e gli standard di sicurezza in merito al trattamento dei dati personali.

In particolare, il registro permette di avere un quadro competo delle attività di trattamento svolte in azienda e, quindi, facilita l'opera di controllo delle attività stesse.

Questa attività riguarda tutti i dati personali e ogni banca di dati o archivio è classificato in relazione alle informazioni in esso contenute e in relazione al tipo di trattamento eseguito indicando se si tratta di:

- Dati personali (Definizioni, comma 1)
- Dati personali particolari (Art. 9 comma 1)
- Dati personali relativi alla salute (Art. 9 comma 1)
- Dati personali relativi a condanne penali e reati (Art. 10)
- Dati personali genetici (Definizioni, comma 13)
- Dati personali biometrici (Definizioni, comma 14)

I dati personali sono classificati secondo le seguenti definizioni:

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

Dati personali particolari
Dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale

Dati personali relativi alla salute
Dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona

Dati personali relativi a condanne penali e reati
Dati e notizie relativi a condanne penali e reati

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

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

Dati personali "sensibili" o dati personali "giudiziari".

Non esiste più una specifica definizione di dati personali "sensibili" o di dati personali "giudiziari".

Tuttavia, l'art. 9 individua in generale le "categorie particolari di dati personali" nelle informazioni "che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, i dati genetici, i dati biometrici intesi a identificare in modo univoco una persona fisica, i dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona fisica"; mentre il successivo articolo 10 del Regolamento disciplina il trattamento dei "dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza".

Dati relativi alla salute.

Il Regolamento introduce comunque una nuova definizione limitata ai "*dati relativi alla salute*" intesi quali i «*dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute*».

Il trattamento di dati (ex) sensibili è addirittura vietato come regola generale, derogabile nei casi specifici elencati dall'art. 9.

Gli Stati membri possono comunque mantenere o introdurre ulteriori condizioni, comprese limitazioni, con riguardo al trattamento di dati genetici, dati biometrici o dati relativi alla salute.

Per quanto riguarda il trattamento dei dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza, vale il principio – già noto al Codice della *privacy – per il quale il trattamento dei dati giudiziari deve avvenire soltanto sotto il controllo dell'autorità pubblica o se il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri che preveda garanzie appropriate per i diritti e le libertà degli interessati*.

5. IL TITOLARE DEL TRATTAMENTO

Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento. Dette misure sono riesaminate e aggiornate qualora necessario.

Se ciò è proporzionato rispetto alle attività di trattamento, le misure di cui al paragrafo 1 includono l'attuazione di politiche adeguate in materia di protezione dei dati da parte del titolare del trattamento.

L'adesione ai codici di condotta di cui all'articolo 40 o a un meccanismo di certificazione di cui all'articolo 42 può essere utilizzata come elemento per dimostrare il rispetto degli obblighi del titolare del trattamento.

Il Titolare del trattamento dati che redige il presente Registro è:

Ragione Sociale	KENT S.R.L.
Indirizzo	Via Aldo Moro 109 SAN DONATO MIL.SE
Partita IVA	**……**

Attività del titolare: Vedi visura camerale allegata

6. IL RESPONSABILE DEL TRATTAMENTO (DATA CONTROLLER – ART. 28)

Qualora un trattamento debba essere effettuato per conto del titolare del trattamento, quest'ultimo ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato.

Il responsabile del trattamento non ricorre a un altro responsabile senza previa autorizzazione scritta, specifica o generale, del titolare del trattamento. Nel caso di autorizzazione scritta generale, il responsabile del trattamento informa il titolare del trattamento di eventuali modifiche previste riguardanti l'aggiunta o la sostituzione di altri responsabili del trattamento, dando così al titolare del trattamento l'opportunità di opporsi a tali modifiche.

I trattamenti da parte di un responsabile del trattamento sono disciplinati da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, che vincoli il responsabile del trattamento al titolare del trattamento e che stipuli la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento. Il contratto o altro atto giuridico prevede, in particolare, che il responsabile del trattamento:

a) tratti i dati personali soltanto su istruzione documentata del titolare del trattamento, anche in caso di trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale, salvo che lo richieda il diritto dell'Unione o nazionale cui è soggetto il responsabile del trattamento; in tal caso, il responsabile del trattamento informa il titolare del trattamento circa tale obbligo giuridico prima del trattamento, a meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico;

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

c) adotti tutte le misure richieste ai sensi dell'articolo 32;

d) rispetti le condizioni di cui ai paragrafi 2 e 4 per ricorrere ad un altro responsabile del trattamento;

e) tenendo conto della natura del trattamento, assista il titolare del trattamento con misure tecniche ed organizzative adeguate, nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo del titolare del trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato di cui al capo III;

f) assista il titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36, tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento;

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

h) metta a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al presente articolo e consenta e contribuisca alle attività di revisione, comprese le ispezioni, realizzati dal titolare del trattamento o da un altro soggetto da questi incaricato.

Con riguardo alla lettera h) del primo comma, il responsabile del trattamento informa immediatamente il titolare del trattamento qualora, a suo parere, un'istruzione violi il presente regolamento o altre disposizioni, nazionali o dell'Unione, relative alla protezione dei dati.

Quando un responsabile del trattamento ricorre a un altro responsabile del trattamento per l'esecuzione di specifiche attività di trattamento per conto del titolare del trattamento, su tale altro responsabile del trattamento sono imposti, mediante un contratto o un altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, gli stessi obblighi in materia di protezione dei dati contenuti nel contratto o in altro atto giuridico tra il titolare del trattamento e il responsabile del trattamento di cui al paragrafo 3, prevedendo in particolare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento. Qualora l'altro responsabile del trattamento ometta di adempiere ai propri obblighi in materia di protezione dei dati, il responsabile iniziale conserva nei confronti del titolare del trattamento l'intera responsabilità dell'adempimento degli obblighi dell'altro responsabile.

L'adesione da parte del responsabile del trattamento a un codice di condotta approvato di cui all'**articolo 40** o a un meccanismo di certificazione approvato di cui all'**articolo 42** può essere utilizzata come elemento per dimostrare le garanzie sufficienti di cui ai paragrafi 1 e 4 del presente articolo.

Fatto salvo un contratto individuale tra il titolare del trattamento e il responsabile del trattamento, il contratto o altro atto giuridico di cui ai paragrafi 3 e 4 del presente articolo può basarsi, in tutto o in parte, su clausole contrattuali tipo di cui ai paragrafi 7 e 8 del presente articolo, anche laddove siano parte di una certificazione concessa al titolare del trattamento o al responsabile del trattamento ai sensi degli articoli 42 e 43.

La Commissione può stabilire clausole contrattuali tipo per le materie di cui ai paragrafi 3 e 4 del presente articolo e secondo la procedura d'esame di cui all'**articolo 93**, paragrafo 2.

Un'autorità di controllo può adottare clausole contrattuali tipo per le materie di cui ai paragrafi 3 e 4 del presente articolo in conformità del meccanismo di coerenza di cui all'**articolo 63**.

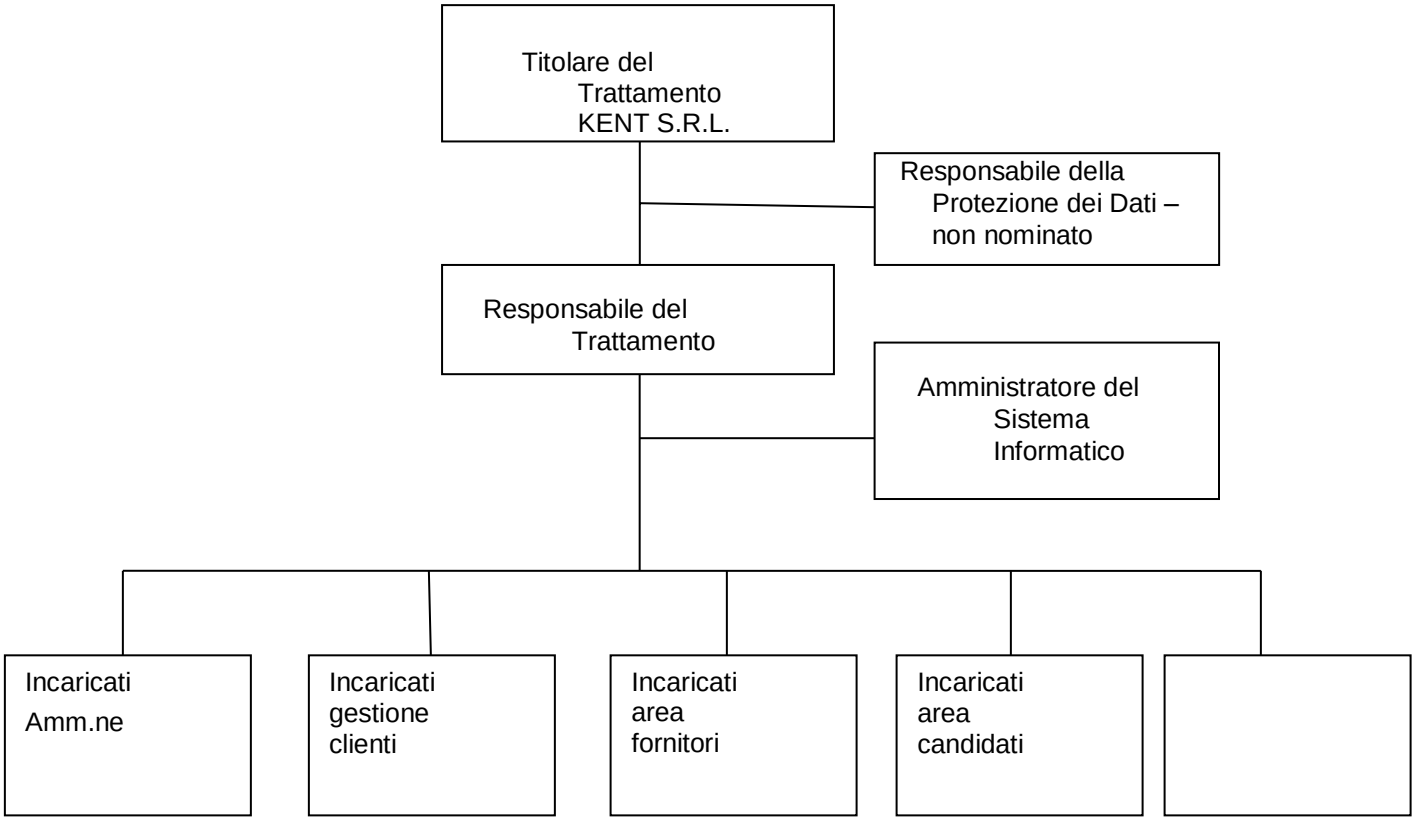
Il contratto o altro atto giuridico di cui ai paragrafi 3 e 4 è stipulato in forma scritta, anche in formato elettronico.

Fatti salvi gli **articoli 82, 83 e 84**, se un responsabile del trattamento viola il presente regolamento, determinando le finalità e i mezzi del trattamento, è considerato un titolare del trattamento in questione.

All'interno della sua organizzazione, il Titolare ha stabilito i seguenti responsabili del trattamento dei dati:

Identificativo	Funzione / Incarico	Tipologia	Modalità

7. L'ORGANIZZAZIONE CHE EFFETTUA I TRATTAMENTI



SEDE CENTRALE E UFFICI

Indirizzo sede operativa/unità locale	Ufficio	Strutture presenti
V. A. MORO 109 SAN DONATO MIL.SE	UNICA SEDE Accesso controllato Antifurto Estintori	Ufficio rapporti con i clienti Ufficio selezione candidature Ufficio relazione con i fornitori

ELENCO DELLE APPARECCHIATURE

Tipo apparecchiatura	Sistema operativo	Archivi	Ubicazione ufficio
n. 1 Server	Italia	Attività operativa, data base, cedolini, anagrafica clienti, fornitori, dipendenti, candidati ma solo dell'anno in corso	S.D.
n. 1 Server	Romania	Posta elettronica	Rom.
n. 2 Personal computer		Anagrafiche clienti e fornitori, dipendenti, messaggi di posta, documenti vari	S.D.
n. 1 Smartphone		Messaggi di posta	S.D.
Sito internet			

INCARICATI DEL TRATTAMENTO

Nome Cognome	Sigla ufficio	struttura
	AMM	Ufficio gestione clienti
	FOR	Gestione fornitori
	SELEZ	Gestione candidature e selezione
	AMM	Amministrazione

CATEGORIE DI UTENTI

Struttura	Trattamenti operati dalla struttura	Compiti della struttura
Ufficio Amministrazione	Trattamento dei dati relativi a clienti, fornitori, dipendenti, consulenti	Gestione delle pratiche del personale, contratti, fatturazione.
Ufficio Acquisti/fornitori	Trattamento dei dati relativi a fornitori	Redazione di ordini di acquisto, utenze e locazione sede operativa
Ufficio Commerciale/clienti	Trattamento dei dati relativi a clienti	Servizio di selezione e reclutamento, servizi di consulenza alla clientela, procacciamento di nuovi clienti.

All'interno di queste strutture organizzative operano incaricati al trattamento secondo quanto previsto dal Regolamento.

Gli Incaricati del trattamento ricevono idonee ed analitiche istruzioni sulle mansioni loro affidate e sugli adempimenti cui sono tenuti.

8. CATEGORIE DI INTERESSATI E DI DATI PERSONALI TRATTATI

L'elenco delle categorie di interessati e dei relativi dati personali trattati è da tenersi aggiornato continuamente ad ogni variazione dell'elenco delle tipologie di trattamenti effettuati e delle relative banche dati. Le categorie di interessati e di dati personali oggetto del trattamento da parte del titolare sono:

Trattamento	Finalità del trattamento	Descrizione del trattamento	Categorie di interessati	Categorie di dati personali	Categorie di destinatari	Trasferimentia paesiterzio organizzazioni internazionali	Termini di cancellazione dei dati	Misure di sicurezza tecniche e organizzative specifiche
Busta paga dipendenti	Pagamento degli stipendi	Copie delle buste paga e altri eventuali documenti sono conservati all'interno di armadi con serratura.	Dipendenti	dati identificativi dati retribuzione dati sulla salute (P)	STUDIO PAGHE (esterno)	no	Termini di legge	Misure di sicurezza generali
Fascicolo dipendenti /clienti	Permettere la gestione degli oneri fiscali e previdenziali e i pagamenti	I fascicoli correnti sono conservati in armadio protetto in ufficio personale e gestiti solo dagli addetti autorizzati I dati sono trattati per obblighi contabili e fiscali al fine dell'erogazione dei servizi e prodotti offerti dal titolare, nonché per la gestione dei pagamenti	Dipendenti/clienti	dati identificativi dati carriera dati sulla salute	Commercialista Banche Ist. credito Enti pubblici Preposti ex lege	no	Termini di legge	Misure di sicurezza generali

Trattamento	Finalità del trattamento	Descrizione del trattamento	Categorie di interessati	Categorie di dati personali	Categorie di destinatari	Trasferimentia paesiterzio organizzazioni internazionali	Termini di cancellazione dei dati	Misure di sicurezza tecniche e organizzative specifiche
Anagrafiche fornitori	Acquisto di prodotti e servizi	Gestione delle anagrafiche di base e dei dati contabili e bancari del fornitore al fine di acquisire beni e servizi	Fornitori	dati identificativi dati contabili e bancari	Banche Commercialista	NO	Termini di legge	Misure di sicurezza generali
Archiviazione documentale	Archiviazione documenti in digitale	In questa banca dati sono gestite le immagini di documenti contabili, fiscale e commerciali, al fine di facilitare la gestione aziendale	Clienti Fornitori Dipendenti	dati identificativi fatture e documenti commerciali		NO	Termini di legge	Misure di sicurezza generali
Posta elettronica e rubriche	Corrispondenza e contatti con clienti e fornitori, dipendenti	I dati di contatto dei clienti , fornitori, dipendenti e collaboratori sono gestiti nelle anagrafiche del gestionale e del client di posta al fine di mantenere i contatti con gli interessati.	Clienti, Fornitori, Consulenti Dipendenti	dati commerciali dati di contatto		NO	Termini di legge in funzione della categoria dei contatti	Misure di sicurezza generali

10 ANALISI DEI RISCHI - MISURE DI SICUREZZA TECNICHE E ORGANIZZATIVE

Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio

Il titolare ha adottato o è in procinto di adottare una serie di misure tecniche e organizzative atte a proteggere i dati personali e ad evitare che vi siano rischi per i diritti e le libertà delle persone fisiche.

MISURE ORGANIZZATIVE ADOTTATE O ADOTTABILI	STATO MISURA	EVENTUALE DESCRIZIONE MISURA
Termini di conservazione dei dati personali	Attiva	Secondo i termini di legge
Formazione di incaricati e responsabili	Attiva	Lettera di incarico e mansionario
Policy aziendali per l'uso del sistema informatico	Attiva	Lettera di incarico e mansionario
Policy aziendali per l'uso di internet e la posta elettronica	Attiva	Lettera di incarico e mansionario
Policy aziendali per l'uso dei dispositivi mobili (smartphone e tablet)	Attiva	Lettera di incarico e mansionario
Policy aziendali per la prevenzione della violazione dei dati	Attiva	Lettera di incarico e mansionario
Accordi contrattuali con responsabili esterni	Attiva	Nomina a Responsabili esterni del trattamento
Verifica trasferimenti di dati personali al di fuori della UE	Attiva	
Valutazione dei rischi periodica	Attiva	A cura del data processor
Policy per inserimento di nuovo personale	Attiva	A cura del data processor
Regole per l'accesso alla posta elettronica in caso di assenza	Attiva	

MISURE TECNICHE	STATO MISURA	EVENTUALE DESCRIZIONE MISURA
Verifica periodica delle misure di sicurezza adeguate al rischio	Attiva	
Procedure Data Breach	Attiva	Predisposizione della modulistica
Procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento	Attiva	
Salvataggi dei dati personali	Attiva	
Ripristino tempestivo della disponibilità e dell'accesso dei dati personali in caso di incidente fisico o tecnico	Attiva	
Protezione da intrusioni esterne	Attiva	Firewall
Protezione da virus e malware	Attiva	Antivirus
Procedure per la gestione di possibili infezioni da malware	Attiva	Antimalware
Protezione da accessi interni non autorizzati	Attiva	
Protezione delle reti WiFi	Attiva	La rete WiFi è gestita con password, password separata per gli ospiti
Aggiornamenti periodici dei software	Attiva	
Regole per la dismissione dell'hardware	Attiva	Prima di smaltire l'hardware si provvede a rendere illeggibili i dati contenuti nei dischi
Accesso riservato alla sala centro elab. dati	Attiva	Accesso controllato
Protezione da interruzioni di energia elettrica	Non Attivata	E' presente un gruppo di continuità per la protezione da interruzione di energia elettrica
Cifratura dei dati	Non attivata	Non necessaria considerando la tipologia e il tipo di trattamento dei dati
Protezione delle postazioni di lavoro da accessi indesiderati	Attiva	
Protezione da installazioni di software non autorizzato	Attiva	
Sicurezza delle credenziali di accesso	Attiva	
Controllo accessi al sistema informativo	Attiva	
Protezione del sito internet da minacce hacker	Attiva	A cura del provider, prevista dal contratto.
Controllo virus in invio e ricezione posta elettronica	Attiva	

MISURE TECNICHE	STATO MISURA	EVENTUALE DESCRIZIONE MISURA
Adozione di crittografia in trasmissione di dati particolari	Non attiva	Non necessaria considerando la tipologia e il tipo di trattamento dei dati
Protezione dei log di navigazione internet	Attiva	
Cancellazione periodica dei log di navigazione internet	Attiva	
Applicazione di filtri alla navigazione internet	Attiva	

ANALISI DEI RISCHI

L'analisi dei rischi è rilevata per ogni banca dati e relativi trattamenti svolti ed è da aggiornare ad ogni variazione dell'elenco delle tipologie di trattamenti effettuati e delle relative banche dati.

Ogni banca di dati o archivio è classificato in relazione alle informazioni in essa contenute e in relazione al tipo di trattamento eseguito indicando se si tratta di:

- Dati personali comuni
- Dati personali particolari (Art. 9) (P)
- Dati personali relativi a condanne penali e reati (Art. 10) (R)
- Dati personali genetici (Definizioni, comma 13) (G)
- Dati personali biometrici (Definizioni, comma 14) (B)

Il Titolare è tenuto alla rilevazione dei rischi che incombono sui dati, alla loro valutazione e alla attuazione di contromisure idonee.Periodicamente viene effettuata una analisi completa dei rischi che incombono sui dati, sia di natura elettronica dovuti per esempio a malfunzionamenti dei sistemi informatici, sia di natura fisica, dovuti per esempio ad accessi di persone non autorizzate ai locali.

Struttura	Compiti della struttura	Descrizione dei rischi specifici	Valutazione del rischio (alto, medio, basso, nullo)	Misure specifiche
Ufficio Amministrazione	Tenuta della contabilità aziendale, gestione delle pratiche del personale, pagamento degli stipendi, bonifici, fatturazione, gestione della contabilità dei clienti. Gestione dei dati anagrafici, contabili e fiscali degli agenti per la liquidazione delle spettanze. Consuntivazione lavori.	Rischi relativi alla perdita e distruzione dei dati personali di clienti e fornitori, all'accesso indebito di dipendenti non autorizzati ai dati relativi agli stipendi, errori nelle procedure di pagamento degli stipendi, errate comunicazioni di dati personali a terzi	MEDIO	Controllo degli accessi informatici (profili utente) e delle autorizzazioni
Ufficio Commerciale e Marketing	Redazione di preventivi, offerte, contratti di vendita, gestione delle attività di marketing, procacciamento nuovi clienti, Invio, ricezione e smistamento della corrispondenza commerciale, servizi di consulenza di vendita alla clientela.	Rischi relativi alla perdita e distruzione dei dati personali di clienti, trattamenti illeciti di marketing senza o con errato consenso, errate comunicazioni di dati personali a terzi	MEDIO	Revisione di tutta la modulistica aziendale di raccolta dati e formazione
Ufficio Acquisti e Marketing	Redazione di ordini di acquisto, analisi e selezione dei fornitori, verifica dei listini di acquisto. Gestione delle anagrafiche di base e dei dati contabili e bancari del fornitore al fine di acquisire beni e servizi.	Rischi relativi alla perdita e distruzione dei dati personali di fornitori	BASSO	Applicazione delle misure generali di protezione dei dati
Magazzino	Gestione dei DDT Fornitori e Clienti	Rischi relativi alla perdita e distruzione dei dati personali di fornitori e clienti.	BASSO	Applicazione delle misure generali di protezione dei dati
Ufficio Personale	Assunzioni, raccolta e verifica delle presenze, gestione pratiche e fascicoli personali dei dipendenti	Rischi relativi alla perdita e distruzione dei dati personali di dipendenti, all'accesso indebito di terzi non autorizzati ai dati dei dipendenti (Sensibili e non), errori nelle procedure di comunicazione a terzi dei dati sensibili, accesso indebito ai fascicoli sanitari. Rischio di accesso indesiderato ai dati contenuti nella cartella PERSONALE. Rischio di utilizzo del portale paghe non in formato cifrato https.	ALTO	Sistemi di anti-intrusione, Cifratura di dati, acquisto di un armadio per l'archivio, verifica del ciclo delle buste paga, formazione

STUDIO_PAGHE (esterno)	Elaborazione delle buste paga	Rischi relativi alla perdita e distruzione dei dati personali di dipendenti, rischi di comunicazione errata o diffusione dei dati relativi alle buste paga.	ALTO	Nomina a Responsabile esterno del trattamento
Commercialista	Elaborazione dati contabili	Rischi relativi alla perdita e distruzione dei dati personali di dipendenti, clienti e fornitori	ALTO	Nomina a Responsabile esterno del trattamento
SERVIZI_CLOUD (esterno)	Fornitura di servizi Cloud	Rischi relativi alla perdita e distruzione dei dati personali affidati al titolare, accessi abusivi al sistema cloud da parte di terzi	MEDIO	Nomina a Responsabile esterno del trattamento

RISCHI GENERALI RILEVATI

Rischio		Impatto sulla sicurezza dei dati		Fattore di rischio rilevato	Rif. Misure
ID Rischio	Descrizione	Gravità Stimata	Probabilità stimata		
Furto di credenziali di autenticazione	I dati possono venire trattati da soggetti non autorizzati, anche per finalità diverse da quelle per cui sono stati raccolti	Alta	Media	Medio	Autenticazione
Carenza di consapevolezza, disattenzione o incuria sulle autorizzazioni ai dati	I dati possono venire trattati da soggetti non autorizzati	Alta	Media	Medio	Autorizzazione Formazione
Componenti sleali o fraudolenti	I dati possono essere rubati o alterati in modo fraudolento	Bassa	Bassa	Basso	Autorizzazione
Errore materiale	I dati possono essere errati	Bassa	Bassa	Basso	Autorizzazione Formazione
Comunicazione dei dati a soggetti errati	I dati possono essere comunicati per errore a soggetti non autorizzati	Media	Media	Medio	Formazione
Diffusione errata dei dati	I dati possono essere diffusi per errore	Alta	Bassa	Medio	Formazione
Azione di virus informatici o di codici maligno	I dati possono essere distrutti o resi indisponibili al trattamento o sottratti	Alta	Bassa	Medio	Antivirus
Spamming o altre tecniche di sabotaggio	Le funzionalità degli strumenti elettronici possono essere compromesse rendendo impossibile il trattamento	Bassa	Bassa	Basso	Antispam
Malfunzionamento degli strumenti	I dati possono essere distrutti o resi indisponibili al trattamento	Bassa	Bassa	Basso	Aggiornamenti
Accessi esterni non autorizzati	Soggetti esterni possono accedere ai dati, rubarli e diffonderli indiscriminatamente	Media	Media	Medio	Anti-intrusione Cifratura
Intercettazione di informazioni in rete	Soggetti esterni possono accedere ai dati, rubarli e diffonderli indiscriminatamente	Media	Bassa	Basso	Anti-intrusione Cifratura
Accessi non autorizzati a locali ad accesso ristretto	Soggetti esterni possono accedere ai dati, rubarli e diffonderli indiscriminatamente	Alta	Bassa	Medio	Accessi Cifratura
Asporto e furto di strumenti contenenti dati	Soggetti esterni possono accedere ai dati, rubarli e diffonderli indiscriminatamente	Media	Bassa	Basso	Accessi Cifratura
Cancellazione errata di dati	I dati possono essere cancellati o alterati per errore	Media	Bassa	Basso	Salvataggio
Eventi distruttivi, naturali o artificiali, dolosi, accidentali o dovuti a incuria	I dati possono essere distrutti o resi indisponibili al trattamento	Media	Bassa	Basso	Ripristino

Rischio		Impatto sulla sicurezza dei dati		Fattore di rischio rilevato	Rif. Misure
ID Rischio	Descrizione	Gravità Stimata	Probabilità stimata		
Guasto ai sistemi complementari (Impianto elettrico, climatizzazione)	Le funzionalità degli strumenti elettronici possono essere compromesse rendendo impossibile il trattamento	Bassa	Bassa	Basso	UPS ed impianti complementari
. Trattamenti errati da parte di terze parti	Soggetti esterni possono trattare i dati erroneamente, comunicarli o diffonderli a soggetti non autorizzati	Alta	Media	Medio	Accordi

MISURE GENERALI DI CONTRASTO AL RISCHIO

	SISTEMA DI AUTENTICAZIONE
Stato attuazione	In essere
Elementi descrittivi	Prevedere un corretto sistema di autenticazione degli utenti su tutti i sistemi che trattano dati personali. Consegnare le credenziali di autenticazione in modo riservato. Ogni incaricato deve avere un utente a lui assegnato in via esclusiva e una parola chiave complessa. Vengono eliminati o disattivati gli utenti non utilizzati. Gli incaricati vengono formati sul corretto utilizzo del sistema di autenticazione
	SISTEMA DI AUTORIZZAZIONE
Stato attuazione	In essere
Elementi descrittivi	Prevedere un sistema di autorizzazione su tutti i sistemi informatici che contengono dati personali. Tale sistema individua l'ambito del trattamento consentito abilitando l'accesso alle sole informazioni ad esso riservate. Proteggere i dati dei dipendenti rendendoli accessibili ai soli incaricati autorizzati.
	SISTEMI ANTIVIRUS
Stato attuazione	In essere
Elementi descrittivi	Installare ultima versione del software antivirus (non gratuito) su tutti i sistemi che trattano dati personali. Verificare periodicamente il funzionamento dell'aggiornamento delle definizioni dei virus.
	SISTEMI ANTISPAMMING
Stato attuazione	In essere
Elementi descrittivi	Prevedere un sistema antispam sul server di posta elettronica o sul firewall.
	AGGIORNAMENTO DEI SOFTWARE
Stato attuazione	In essere
Elementi descrittivi	Aggiornare periodicamente tutti i software e i sistemi operativi utilizzati per il trattamento dei dati personali. Valutare l'aggiornamento dei software gestionali, in modo che eventuali errori di programmazione non compromettano l'integrità dei dati trattati.

	SISTEMI ANTI-INTRUSIONE
Stato attuazione	In essere
Elementi descrittivi	Installare un firewall di rete per evitare le intrusioni dall'esterno di soggetti non autorizzati al trattamento. Verificare periodicamente gli accessi VPN presenti sul firewall ed eliminare quelli non più utilizzati. Modificare periodicamente le password di accesso VPN al sistema aziendale. Adottare politiche di controllo per evitare che soggetti esterni possano collegarsi al sistema informatico dall'interno dei locali dell'organizzazione. Proteggere la rete wireless con chiave criptata. Configurare la rete wireless in modo che gli utenti "guest" non possano accedere ai computer aziendali.
Misura	**CONTROLLO DEGLI ACCESSI**
Stato attuazione	In essere
Elementi descrittivi	Controllare l'accesso ai siti in cui sono custoditi i dati particolari tramite chiusura a chiave di locali o armadi. Controllare l'accesso ai locali in cui sono custoditi i sistemi informatici e le copie di sicurezza dei dati.
Misura	**SALVATAGGIO DEI DATI**
Stato attuazione	In essere
Elementi descrittivi	Effettuare il salvataggio dei dati personali con cadenza giornaliera. Il salvataggio dei dati deve essere effettuato in modo che consenta di ripristinare dati eventualmente cancellati per errore. Una copia dei dati deve risiedere su un supporto scollegato dalla rete aziendale o inaccessibile da essa.
	PIANO DI RIPRISTINO DELLA DISPONIBILITA' DEI DATI
Stato attuazione	In essere
Elementi descrittivi	Studiare un piano per il ripristino dei sistemi e dei dati personali in caso di distruzione e perdita dei sistemi o dei dati.
	SISTEMI DI ALIMENTAZIONE ELETTRICA AUTONOMA E IMPIANTI COMPLEMENTARI
Stato attuazione	Non in essere
Elementi descrittivi	Prevedere l'utilizzo di un sistema di alimentazione elettrica autonoma che entri in funzione in caso di guasto alla rete elettrica. Controllare periodicamente il funzionamento del sistema di alimentazione e degli impianti tecnici (es. condizionatore) operanti all'interno dei locali in cui sono tenuti i sistemi informatici
	ACCORDI CONTRATTUALI
Stato attuazione	In essere
Elementi descrittivi	Per ogni soggetto esterno che tratta dati personali per conto del titolare stipulare nuovi accordi contrattuali che prevedano la responsabilità congiunta come previsto dal Regolamento UE
	FORMAZIONE INCARICATI
Stato attuazione	In essere
Elementi descrittivi	Prevedere la formazione degli incaricati al trattamento sia al primo ingresso nell'organizzazione che successivamente in caso di cambio mansione o novità normative rilevanti
	PSEUDONIMIZZAZIONE DEI DATI
Stato attuazione	Non richiesta
Elementi descrittivi	Effettuare la pseudonimizzazione dei dati in modo da rendere i dati personali non riconducibili agli interessati.
	CIFRATURA DEI DATI
Stato attuazione	Non richiesta
Elementi descrittivi	Eseguire la cifratura delle cartelle contenenti dati personali particolari. La cifratura deve essere prevista durante tutto il ciclo del trattamento, quindi sia in archiviazione che nella trasmissione dei dati.

10.1 AMMINISTRATORI DI SISTEMA

Il titolare, in ottemperanza al provvedimento del Garante della Privacy del 27 novembre 2008 *("Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema")* ha provveduto alla individuazione ed alla nomina della figura di "Amministratore di sistema".

Elenco Amministratore di Sistema

L'amministratore di sistema è il soggetto che sovrintende alle gestione delle infrastrutture informatiche aziendali, ivi comprese le banche dati oggetto del trattamento dei dati personali.

E' compito di questo soggetto:

- Attivare le credenziali di autenticazione agli incaricati del trattamento
- Prendere tutti i provvedimenti necessari ad evitare la perdita o la distruzione dei dati e provvedere al ricovero periodico degli stessi con copie di back-up;
- Assicurarsi della qualità delle copie di back-up dei dati e della loro conservazione in luogo adatto e sicuro;
- Fare in modo che sia prevista la disattivazione dei Codici identificativi personali (USER-ID), in caso di perdita della qualità che consentiva all'utente o incaricato l'accesso all'elaboratore, oppure nel caso di mancato utilizzo dei Codici identificativi personali (USER-ID) per oltre 6 mesi;
- Proteggere gli elaboratori dal rischio di intrusione (violazione del sistema da parte di "hackers") e dal rischio di virus mediante idonei programmi.

Il Titolare del trattamento dei dati può nominare ulteriori Amministratori di sistema, specificando gli elaboratori o le banche dati che sono chiamati a sovrintendere, informandoli delle responsabilità che gli sono state affidate in relazione a quanto disposto dalle normative in vigore.

10.2 ADDETTI AL TRATTAMENTO DEI DATI (DATA PROCESSOR)

Ogni persona che all'interno dell'organizzazione tratta dati personali si qualifica come addetto al trattamento dei dati.

Gli addetti al trattamento ricevono idonee ed analitiche istruzioni, anche per gruppi omogenei di lavoro, sulle mansioni loro affidate e sugli adempimenti cui sono tenuti; essi sono dotati di specifica competenza circa le modalità di trattamento dei dati personali, quali che fossero "alter ego" dei titolari e ha buone conoscenze sia son riguardo alle misure tecniche che son riguardo a quelle organizzative e procedurali.

In caso di trattamento automatizzato di dati, per ogni addetto al trattamento viene indicato lo USER-ID assegnato.

Il tipo di trattamento effettuato da ogni singolo addetto al trattamento può essere differenziato. In particolare ad ogni addetto al trattamento può essere data dal Responsabile del trattamento la possibilità di:

- Inserire nuove informazioni nella banca di dati personali
- Accedere alle informazioni in visualizzazione e stampa
- Modificare le informazioni esistenti nella banca di dati personali
- Cancellare le informazioni esistenti nella banca di dati personali

Ad ogni addetto sono state comunicate le credenziali per l'autenticazione per l'accesso al sistema e le relative istruzioni di sicurezza (segretezza delle credenziali, blocco del computer in propria assenza temporanea durante una sessione di trattamento), conforme al principio need to know.

All'amministratore di sistema è affidato il compito di verificare ogni sei mesi le autorizzazioni di accesso ai dati oggetto del trattamento e di aggiornare l'elenco degli utenti autorizzati.

Lo stesso ha sottoscritto un impegno alla riservatezza che vale anche dopo aver abbandonato il ruolo assegnatogli; ha seguito un percorso di sensibilizzazione ed è stato appositamente istruito; inoltre ha ricevuto istruzioni scritte differenziate in funzione del profilo di trattamento assegnato ed è soggetto a valutazione in fase di verifica dell'attività svolta.

Il responsabile del trattamento può ricorrere ed appoggiarsi ad altri responsabili del trattamento ove i compiti affidati non spossano essere assolti da un solo individuo ma necessiterà, per questo, dell'autorizzazione scritta, generica o specifica, del titolare.

10.3 ASSEGNAZIONE E GESTIONE DELLE CREDENZIALI DI ACCESSO AI SISTEMI INFORMATICI

Nel caso in cui il trattamento di dati personali è effettuato con strumenti elettronici, l'amministratore di sistema deve assicurarsi che il trattamento sia consentito solamente agli incaricati dotati di credenziali di autenticazione che consentano il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti.

Il Responsabile del trattamento dei dati, in accordo con l'amministratore di sistema, definisce le modalità di assegnazione dei nomi identificativi per consentire a ciascun addetto al trattamento di accedere ai sistemi di trattamento delle banche di dati.

All'addetto viene assegnato un codice per l'identificazione associato a una parola chiave riservata conosciuta solamente dal medesimo, oppure un dispositivo di autenticazione in possesso e uso esclusivo dell'incaricato, eventualmente associato a un codice identificativo o a una parola chiave, oppure una caratteristica biometrica dell'incaricato, eventualmente associata a un codice identificativo o a una parola chiave.

L'amministratore di sistema si assicura che il codice per l'identificazione, laddove utilizzato, non potrà essere assegnato ad altri incaricati, neppure in tempi diversi.

In caso si debba accedere, per motivi di manutenzione tecnica o per lavoro, alla postazione dell'addetto in sua assenza, l'amministratore di sistema provvede a modificare la parola chiave dell'addetto e a comunicare la nuova parola chiave al tecnico informatico o al collega che sostituisce l'addetto.
Al ritorno, l'addetto non potrà accedere al sistema e dovrà farsi dire la nuova parola chiave. Una volta avuto accesso al sistema, dovrà modificarsi la parola chiave in modo da renderla di nuovo riservata.
L'amministratore di sistema si assicura che le credenziali di autenticazione non utilizzate da oltre sei mesi siano disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica. Si assicura che le credenziali siano disattivate anche in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali.

Ad ogni addetto al trattamento possono essere assegnate o associate individualmente una o più credenziali per l'autenticazione.

La parola chiave è composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito. Non deve contenere riferimenti agevolmente riconducibili all'incaricato o al codice di accesso assegnato (user-id). La parola chiave è modificata dall'incaricato del trattamento al primo utilizzo e, successivamente, almeno ogni sei mesi o ogni tre mesi in caso di trattamento di particolari categorie di dati (sensibili).

Glii addetti adottano le necessarie cautele per assicurare la segretezza della parola chiave e custodire diligentemente ogni altro dispositivo che gli è stato affidato per i sistemi di autenticazione informatica (badge magnetici, tessere magnetiche, ecc..). In particolare è fatto divieto comunicare a chiunque altro addetto le proprie credenziali di accesso al sistema informatico.

Gli addetti hanno l'obbligo di non lasciare incustodito il proprio posto di lavoro e di prendere i necessari accorgimenti per evitare che, durante la loro assenza anche breve, altri addetti o persone non autorizzate possano accedere alla postazione di lavoro.

10.4 SALVATAGGIO DEI DATI PERSONALI

Al fine di garantire l'integrità dei dati contro i rischi di distruzione o perdita, il Titolare o Responsabile del trattamento dei dati dove designato stabilisce, con il supporto tecnico dell'amministratore di sistema, la periodicità con cui debbono essere effettuate le copie di sicurezza delle banche di dati trattati, che in ogni caso vanno effettuate almeno con cadenza settimanale

In particolare per ogni Banca di dati sono definite le seguenti specifiche:

- il tipo di supporto da utilizzare per le copie di salvataggio
- il numero di copie di salvataggio effettuate ogni volta
- se i supporti utilizzati per le copie di salvataggio sono riutilizzati e in questo caso con quale periodicità
- se per effettuare le copie di salvataggio si utilizzano procedure automatizzate e programmate
- le modalità di controllo delle copie di salvataggio
- la durata massima stimata di conservazione delle informazioni senza che ci siano cancellazione di dati
- l'incaricato del trattamento a cui è stato assegnato il compito di effettuare le copie di salvataggio
- le istruzioni e i comandi necessari per effettuare le copie di salvataggio

E' compito degli addetti alle copie di sicurezza delle banche dati:

- prendere tutti i provvedimenti necessari ad evitare la perdita o la distruzione dei dati e provvedere al ricovero periodico degli stessi con copie di sicurezza secondo i criteri stabiliti
- assicurarsi della qualità delle copie di sicurezza dei dati e della loro conservazione in luogo adatto e sicuro ad accesso controllato
- provvedere a conservare con la massima cura e custodia i dispositivi utilizzati per le copie di sicurezza, impedendo l'accesso agli stessi dispositivi da parte di personale non autorizzato
- segnalare tempestivamente al Responsabile della gestione e della manutenzione degli strumenti elettronici, ogni eventuale problema dovesse verificarsi nella normale attività di copia delle banche dati

10.5 CRITERI PER GARANTIRE LA SICUREZZA E LA RESILIENZA DEI SISTEMI E DEI DATI

All'amministratore di sistema è affidato il compito di verificare la situazione delle apparecchiature hardware e software installate con cui vengono trattati i dati, delle apparecchiature ed, in particolare dei dispositivi di collegamento con le reti esterne.

La verifica ha lo scopo di controllare l'affidabilità del sistema, per quanto riguarda:

- la sicurezza dei dati trattati
- il rischio di distruzione o di perdita
- il rischio di accesso non autorizzato o non consentito tenendo conto anche dell'evoluzione tecnologica, ed in particolare di:
    - disponibilità di nuove versioni migliorative dei Sistemi operativi utilizzati
    - segnalazioni di Patch, Fix o System-Pack per la aggiornare il sistema e rimuovere errori o malfunzionamenti
    - segnalazioni di Patch, Fix o System-Pack per l'introduzione di maggiori sicurezze contro i rischi di intrusione o di danneggiamento dei dati
    - disponibilità di nuove versioni migliorative delle applicazioni installate che consentano maggiore sicurezza contro i rischi di intrusione o di danneggiamento dei dati.

Nel caso in cui esistano rischi evidenti l'amministratore di sistema deve informarne il Responsabile o il Titolare del trattamento perché siano presi gli opportuni provvedimenti allo scopo di assicurare il corretto trattamento dei dati in conformità alle norme in vigore.

10.6 CRITERI E PROCEDURE PER GARANTIRE LA DISPONIBILITA' E L'INTEGRITA' DEI DATI

Fermo quanto previsto al punto 10.4, il titolare ha realizzato un dettagliato piano di ripristino dei dati per riattivare la disponibilità dei dati sui sistemi di elaborazione in seguito ad un eventuale danneggiamento degli stessi.

La decisione di ripristinare la disponibilità dei dati in seguito a distruzione o danneggiamento è compito esclusivo del Responsabile del trattamento dei dati personali. La decisione di ripristinare la disponibilità dei dati deve essere presa rapidamente e in ogni caso la disponibilità dei dati deve essere ripristinata al massimo entro sette giorni.

10.7 PROTEZIONE DA VIRUS INFORMATICI

Al fine di garantire l'integrità dei dati contro i rischi di distruzione o perdita di dati a causa di virus informatici, il Responsabile del trattamento dei dati stabilisce, con il supporto tecnico dell'amministratore di sistema, quali protezioni software adottare in relazione all'evoluzione tecnologica dei sistemi disponibili sul mercato.

Gli aggiornamenti dei sistemi antivirus utilizzati sono tempestivi ed effettuati più volte al giorno al fine di ottenere un accettabile standard di sicurezza delle banche dati trattati.

Nel caso in cui su uno o più sistemi si dovesse verificare perdita di informazioni o danni a causa di virus informatici l'amministratore di sistema deve provvedere a:

- Isolare il sistema
- Verificare se ci sono altri sistemi infettati con lo stesso virus informatico
- Identificare l'antivirus adatto e bonificare il sistema infetto
- Installare l'antivirus adatto su tutti gli altri sistemi che ne sono sprovvisti.

10.8 PROTEZIONE DEI DATI DA ATTACCHI E INTRUSIONI

Al fine di garantire la sicurezza delle trasmissioni dei dati tra le diverse sedi dislocate nel territorio, attraverso l'utilizzo di apparecchi di trasmissione dati, il Responsabile del trattamento dei dati stabilisce, con il supporto tecnico dell'amministratore di sistema, le misure tecniche da adottare in rapporto al rischio di intercettazione o di intrusione o di hacker.

Inoltre, al fine di tutelare i dati personali contenuti all'interno delle banche dati informatiche occorre installare e configurare un sistema di protezione da eventuali intrusioni da parte di personale non autorizzato. Tale sistema viene mantenuto costantemente aggiornato.

10.9 TRATTAMENTO DEI DATI SENZA STRUMENTI ELETTRONICI

In considerazione di quanto disposto dal Regolamento, è fatto divieto a chiunque di:

- Effettuare copie su supporti magnetici o trasmissioni non autorizzate dal Responsabile del trattamento dei dati di dati oggetto del trattamento.
- Effettuare copie fotostatiche o di qualsiasi altra natura, non autorizzate dal Responsabile del trattamento dei dati, di stampe, tabulati, elenchi, rubriche e di ogni altro materiale riguardante i dati oggetto del trattamento.
- Sottrarre, cancellare, distruggere senza l'autorizzazione del Responsabile del trattamento dei dati stampe, tabulati, elenchi, rubriche e ogni altro materiale riguardante i dati oggetto del trattamento.
- Consegnare a persone non autorizzate dal Responsabile del trattamento dei dati stampe, tabulati, elenchi, rubriche e di ogni altro materiale riguardante i dati oggetto del trattamento.
- Ulteriori disposizioni agli incaricati vengono fornite nelle istruzioni allegate alle lettere di incarico

10.10 PROCEDURE PER CONTROLLARE L'ACCESSO ALLE STRUTTURE IN CUI VENGONO TRATTATI I DATI

Il Responsabile del trattamento dei dati ha definito le modalità di accesso agli uffici in cui sono presenti sistemi o apparecchiature di accesso ai dati trattati in modo che venga controllato l'accesso medesimo da parte di personale non autorizzato.

Per ogni archivio i Responsabili del trattamento dei dati definiscono l'elenco degli addetti autorizzati ad accedervi e impartiscono istruzioni tese a garantire un controllo costante nell'accesso degli archivi.

Gli addetti che trattano atti e documenti contenenti dati personali sono tenuti a conservarli e restituirli al termine delle operazioni.

Qualora i documenti contengano particolari categorie di dati gli addetti sono tenuti a conservarli fino alla restituzione in contenitori muniti di serratura.

L'accesso agli archivi contenenti documenti ove sono presenti particolari categorie di dati è consentito, dopo l'orario di chiusura, previa identificazione e registrazione dei soggetti.

10.11 FORMAZIONE

Al Responsabile del trattamento dei dati è affidato il compito di verificare ogni anno le necessità di formazione del personale addetto al trattamento dei dati con lo scopo di fornire ogni informazione necessaria a migliorare la sicurezza di trattamento dei dati.

In particolare, gli addetti sono edotti dei rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal titolare.

Per ogni addetto o gruppi di addetti il Responsabile del trattamento dei dati definisce, sulla base dell'esperienza e delle sue conoscenze, ed in funzione anche di eventuali variazioni della normativa, le necessità di informazione.

Le relative competenze sono impartite già al momento dell'ingresso in servizio, nonché in occasione di cambiamenti di mansioni, o di introduzione di nuovi significativi strumenti o normative/regolamenti, rilevanti rispetto al trattamento di dati personali.

10.12 TRATTAMENTO DI DATI PERSONALI AFFIDATO ALL'ESTERNO

Il Titolare del trattamento ha deciso di affidare il trattamento dei dati in tutto o in parte a soggetti terzi che sono stati individuati quali responsabili del trattamento in esterno.

Sono quindi stati specificati i soggetti interessati e i luoghi dove fisicamente avviene il trattamento dei dati stessi.

I Responsabili del trattamento in esterno devono intendersi autonomi titolari del trattamento e quindi soggetti ai corrispettivi obblighi, e pertanto rispondono direttamente ed in via esclusiva per le eventuali violazioni alla legge.

Il Titolare mantiene aggiornato l'elenco dei soggetti esterni che effettuano il trattamento dei dati in qualità di Responsabili del trattamento, ed indica per ognuno di essi il tipo di trattamento effettuato.

Per ogni trattamento affidato ad un soggetto esterno, il Titolare del trattamento stipula un accordo contrattuale che preveda al suo interno il rispetto per entrambe le parti di tutte le norme previste dal Regolamento in questi casi. Nell'accordo vengono inoltre specificati i compiti che sono affidati al Responsabile esterno.

…….	Trattamento dei dati relativi a dipendenti	Elaborazione delle buste paga e degli adempimenti del personale
Commercialista	Trattamento dei dati amministrativi	Redazione del bilancio e degli adempimenti fiscali
	Sito internet Trattamento dei dati anagrafici clienti	Commercio elettronico

11.VIDEOSORVEGLIANZA

Non ritenendo attuabili altre soluzioni più efficaci, la scelta della videosorveglianza è stata determinata dalla necessità di meglio proteggere l'area ove viene svolta la nostra attività ed i beni strumentali alla stessa da furti e da atti di violenza e di vandalismo (nei limiti imposti dal principio di proporzionalità) e, quindi, per agevolare l'eventuale esercizio del diritto di difesa del titolare o di terzi.

1. CARATTERISTICHE DEL SISTEMA ADOTTATO

Il sistema adottato permette:

- la semplice visione e la registrazione;
- la registrazione, effettuata su supporti digitali, viene conservata nei limiti consentiti dalla legge e viene cancellata a meno di necessità di conservazione dei filmati per i motivi e gli usi consentiti dalla normativa .

2. INFORMATIVA

All'ingresso dell'area si è provveduto ad esporre un idoneo cartello simile a quello predisposto dal Garante per la protezione dei dati personali, nonché ad esporre idonea informativa ai sensi dell'art. 13 del Codice privacy (D.lgs. n. 196/2003). Tale cartello, avvisa tutti gli interessati che accedono alla zona che la videosorveglianza è attiva in tutta l'area esterna dell'edificio.

3. STATUTO DEI LAVORATORI

Si è provveduto a verificare che l'installazione delle videocamere non vada a ledere i diritti dei lavoratori, precisati dall'Art. 4 dello Statuto dei Lavoratori. Infatti le telecamere non riprendono luoghi di lavoro ma solo le aree esterne dell'edificio in cui non vengono svolte attività lavorative. Per tale motivo non si è provveduto ad inoltrare richiesta di autorizzazione alla competente DPL.

12.AGGIORNAMENTO COSTANTE

Il Registro è da tenersi costantemente aggiornato con le decisioni e le operazione rilevanti svolte dal Titolare in materia di trattamento di dati personali.