Sviluppo Risorse Ambientali SRL

General Data Protection Regulation

Trattamento e protezione dei dati personali

Sicurezza informatica

Rev. 1 del 01/06/2018

A.1 *Sommario*

A.1 Sommario 2
A.2 Azienda 4
A.3 Allegati al G.D.P.R. 4
A.4 Documenti esterni 4
1. Premessa 5
1.1. Scopo del presente documento 5
1.2. Riferimenti normativi 5
1.3. Ambito di applicazione materiale 5
1.4. Ambito di applicazione territoriale 6
1.5. Definizioni 6
1.6. Principi applicabili al trattamento dei dati personali (art. 5) 9
1.7. Condizioni per il consenso (art. 7) 9
1.8. Trattamento di categorie particolari di dati personali (art. 9) 10
1.9. Diritto di accesso dell'interessato (art. 15) 10
1.10. Diritto di rettifica (art. 16) 11
1.11. Diritto alla cancellazione (diritto all'oblio) (art. 17) 11
1.12. Diritto alla portabilità dei dati (art. 20) 12
1.13. Responsabilità del titolare del trattamento (art. 24) 12
1.14. Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita (art. 25) 13
1.15. Responsabile del trattamento (art. 28) 13
1.16. Registri delle attività di trattamento 14
1.17. Notifica di una violazione dei dati personali all'autorità di controllo (art. 33) 15
1.18. Comunicazione di una violazione dei dati personali all'interessato (art. 34) 16
1.19. Valutazione d'impatto sulla protezione dei dati (art. 35) 17
2. Elenco dei trattamenti di dati personali 18
2.1. Le tipologie di dati trattati 18
2.1.1. Dati Comuni 18
2.1.2. Dati Sensibili 18
2.1.3. Dati Giudiziari 18
2.2. Le tipologie dei trattamenti 19
3. Il modello organizzativo interno 23
3.1. Organigramma del trattamento e tutela dei dati 23
3.2. Titolare del trattamento dei dati 24
3.3. Responsabile della Protezione dei Dati (Data Protection Officer) 24
3.4. Responsabile del trattamento dei dati 25
3.5. Incaricato del trattamento dei dati 30
3.5.1. Le modalità e il contenuto della formazione degli Incaricati 35
3.5.2. Servizio pulizie 36
3.6. Registro delle attività dei trattamenti 36
4. I diritti dell'interessato 36
5. I luoghi fisici 37
6. Gli strumenti elettronici 40
7. Le modalità di trattamento, l'analisi dei rischi e le procedure di sicurezza 43

7.1. Il trattamento dei dati senza l'ausilio di strumenti elettronici 43
7.1.1. Ambito del comportamento: istruzioni agli incaricati e formazione continua 44
7.1.2. Ambito delle attrezzature: predisposizione di armadi \ classificatori \ cassettiere e sale archivio dotate di serratura 45
7.1.3. Ambito della struttura: organizzazione degli spazi e programmazione della manutenzione 46
7.2. Il trattamento dei dati con l'ausilio di strumenti elettronici 46
7.2.1. Istruzioni agli incaricati della gestione e manutenzione degli strumenti elettronici 49
7.2.2. Istruzioni agli incaricati e formazione continua 50
7.2.3. Il sistema hardware 51
7.2.4. Il sistema software 52
7.2.4.1. Il monitoraggio degli accessi degli amministratori di sistema al sistema informatico . 52
7.2.5. Sistema di autenticazione informatica 52
7.2.5.1. Istruzioni per la scelta della password e la sua protezione 53
7.2.6. Il backup e il ripristino dei dati 54
7.2.6.1. Istruzioni di copia 54
7.2.7. Istruzioni di ripristino 55
7.3. Indicazioni generali di comportamento per gli incaricati 55
7.3.1. Comunicazioni in presenza di più persone 55
7.3.2. Locali aperti al pubblico 55
7.3.3. Tono di voce 55
8. Sistema di videosorveglianza 56
8.1. Motivazioni e finalità dell'installazione dell'impianto 56
8.2. Caratteristiche dell'impianto 56
8.3. Modalità di trattamento dei dati 57
9. Piano di miglioramento 58

A.2 *Azienda*

Ragione sociale	**SRA SRL**
Sede legale	**Via Zona Industriale lotto 70-72-74-76 Polla (SA)**
Sede operativa	**Via Zona Industriale lotto 70-72-74-76 Polla (SA)**
P. IVA	**04067290652**
C.F.	**04067290652**
Legale Rappresentante	**Antonio Cancro**
Tipologia di attività **ATECO 38.11**	**Raccolta di rifiuti solidi non pericolosi**

A.3 *Allegati al G.D.P.R.*

- Guida pratica per l'Incaricato del Trattamento dei Dati, rev. 0 del 23/05/2018
- Informative per gli interessati
  - lavoratori dipendenti
  - clienti e fornitori

- Modello delle lettere di nomina delle seguenti figure
  - Responsabile del trattamento dei dati
  - Incaricato del trattamento dei dati

- Modello di lettere per i fornitori esterni di servizi

A.4 *Documenti esterni*

- Piano di Formazione Aziendale
- Piano della Manutenzione
- Procedure e moduli richiamati dal GDPR

1. Premessa

1.1. Scopo del presente documento

Il presente documento è redatto in conformità ai requisiti posti dal Regolamento UE 2016/679 che stabilisce norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché norme relative alla libera circolazione di tali dati. Il Regolamento protegge i diritti e le libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali. Esso, inoltre, detta che la libera circolazione dei dati personali nell'Unione non può essere limitata né vietata per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati personali.
Il Regolamento promuove la responsabilizzazione (***accountability***) dei titolari del trattamento e l'adozione di approcci e politiche che tengano conto costantemente del rischio che un determinato trattamento di dati personali può comportare per i diritti e le libertà degli interessati.
Il principio-chiave è «***privacy by design***», ossia garantire la protezione dei dati fin dalla fase di ideazione e progettazione di un trattamento o di un sistema, e adottare comportamenti che consentano di prevenire possibili problematiche. Ad esempio, è previsto l'obbligo di effettuare valutazioni di impatto prima di procedere ad un trattamento di dati che presenti rischi elevati per i diritti delle persone, consultando l'Autorità di protezione dei dati in caso di dubbi. Viene inoltre introdotta la figura del «***Responsabile della protezione dei dati***» (***Data Protection Officer*** o ***DPO***), incaricato di assicurare una gestione corretta dei dati personali nelle imprese e negli enti.

1.2. Riferimenti normativi

La normativa di riferimento in materia di trattamento dei dati personali è il Regolamento UE 2016/679. Il "Codice in materia di protezione dei dati personali" emanato con D. Lgs n. 196 del 30 giugno 2003 non è abrogato dal regolamento.

1.3. Ambito di applicazione materiale

Il Regolamento si applica al trattamento interamente o parzialmente automatizzato di dati personali delle persone fisiche e al trattamento non automatizzato di dati personali delle persone fisiche contenuti in un archivio o destinati a figurarvi.
Il Regolamento non si applica ai trattamenti di dati personali delle persone fisiche:
a) effettuati per attività che non rientrano nell'ambito di applicazione del diritto dell'Unione;
b) effettuati dagli Stati membri nell'esercizio di attività che rientrano nell'ambito di applicazione del titolo V, capo 2, TUE;
c) effettuati da una persona fisica per l'esercizio di attività a carattere esclusivamente personale o domestico;
d) effettuati dalle autorità competenti a fini di prevenzione, indagine, accertamento o perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro minacce alla sicurezza pubblica e la prevenzione delle stesse.

1.4. Ambito di applicazione territoriale

Il Regolamento si applica al trattamento dei dati personali delle persone fisiche effettuato nell'ambito delle attività di uno stabilimento da parte di un titolare del trattamento o di un responsabile del trattamento nell'Unione, indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione.
Inoltre, il Regolamento si applica al trattamento dei dati personali di interessati che si trovano nell'Unione, effettuato da un titolare del trattamento o da un responsabile del trattamento che non è stabilito nell'Unione, quando le attività di trattamento riguardano:
a) l'offerta di beni o la prestazione di servizi ai suddetti interessati nell'Unione, indipendentemente dall'obbligatorietà di un pagamento dell'interessato; oppure
b) il monitoraggio del loro comportamento nella misura in cui tale comportamento ha luogo all'interno dell'Unione.
Infine, il Regolamento si applica al trattamento dei dati personali effettuato da un titolare del trattamento che non è stabilito nell'Unione, ma in un luogo soggetto al diritto di uno Stato membro in virtù del diritto internazionale pubblico.

1.5. Definizioni

Di seguito si riportano alcune definizioni di termini ricorrenti nel prosieguo del documento desunte sia dall'art. 4 del Regolamento UE 2016/679 che da definizioni di natura tecnica:

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.

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

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.

Pseudomizzazione

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

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

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

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.

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.

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.

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.

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.

Dati genetici

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

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

Dati 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.

Comunicazione elettronica
Ogni informazione scambiata o trasmessa tra un numero finito di soggetti tramite un servizio di comunicazione elettronica accessibile al pubblico. Sono escluse le informazioni trasmesse al pubblico tramite una rete di comunicazione elettronica, come parte di un servizio di radiodiffusione, salvo che le stesse informazioni siano collegate ad un abbonato o utente ricevente, identificato o identificabile.

Misure minime
Il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti nell'articolo 31.

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

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

Credenziali di autenticazione
I dati ed i dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l'autenticazione informatica.

Parola chiave
Componente di una credenziale di autenticazione associata ad una persona e solo a questa nota, costituita da una sequenza di caratteri o altri dati in forma elettronica.

Profilo di autorizzazione
L'insieme delle informazioni, univocamente associate ad una persona, che consente di individuare a quali dati essa può accedere, nonché i trattamenti ad essa consentiti.

Sistema di autorizzazione
L'insieme degli strumenti e delle procedure che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione del richiedente.

1.6. Principi applicabili al trattamento dei dati personali (art. 5)

I dati personali sono:
a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato (***liceità, correttezza e trasparenza***);
b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali (***limitazione della finalità***);
c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati (***minimizzazione dei dati***);
d) esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati (***esattezza***);
e) conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal Regolamento a tutela dei diritti e delle libertà dell'interessato (***limitazione della conservazione***);
f) trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali (***integrità e riservatezza***).
Il titolare del trattamento è competente per il rispetto dei principi su esposti ed in grado di comprovarlo da quanto contenuto nel presente documento (***responsabilizzazione***).

1.7. Condizioni per il consenso (art. 7)

Qualora il trattamento sia basato sul consenso, il titolare del trattamento deve essere in grado di dimostrare che l'interessato ha prestato il proprio consenso al trattamento dei propri dati personali.
Se il consenso dell'interessato è prestato nel contesto di una dichiarazione scritta che riguarda anche altre questioni, la richiesta di consenso è presentata in modo chiaramente distinguibile dalle altre materie, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro. Nessuna parte di una tale dichiarazione che costituisca una violazione del Regolamento è vincolante.
3.L'interessato ha il diritto di revocare il proprio consenso in qualsiasi momento. La revoca del consenso non pregiudica la liceità del trattamento basata sul consenso prima della revoca. Prima di esprimere il proprio consenso, l'interessato è informato di ciò. Il consenso è revocato con la stessa facilità con cui è accordato.
Nel valutare se il consenso sia stato liberamente prestato, si tiene nella massima considerazione l'eventualità, tra le altre, che l'esecuzione di un contratto, compresa la prestazione di un servizio, sia condizionata alla prestazione del consenso al trattamento di dati personali non necessario all'esecuzione di tale contratto.

1.8. Trattamento di categorie particolari di dati personali (art. 9)

È vietato trattare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.
Il paragrafo che precede non si applica se si verifica uno dei seguenti casi:
a) l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche, salvo nei casi in cui il diritto dell'Unione o degli Stati membri dispone che l'interessato non possa revocare il divieto di cui al paragrafo 1;
b) il trattamento è necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale, nella misura in cui sia autorizzato dal diritto dell'Unione o degli Stati membri o da un contratto collettivo ai sensi del diritto degli Stati membri, in presenza di garanzie appropriate per i diritti fondamentali e gli interessi dell'interessato;
c)il trattamento è necessario per tutelare un interesse vitale dell'interessato o di un'altra persona fisica qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso;
e) il trattamento riguarda dati personali resi manifestamente pubblici dall'interessato;
f) il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali;
h) il trattamento è necessario per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali sulla base del diritto dell'Unione o degli Stati membri o conformemente al contratto con un professionista della sanità;
i) il trattamento è necessario per motivi di interesse pubblico nel settore della sanità pubblica, quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici, sulla base del diritto dell'Unione o degli Stati membri che prevede misure appropriate e specifiche per tutelare i diritti e le libertà dell'interessato, in particolare il segreto professionale;
j) il trattamento è necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici in conformità dell'articolo 89, paragrafo 1 del Regolamento, sulla base del diritto dell'Unione o nazionale, che è proporzionato alla finalità perseguita, rispetta l'essenza del diritto alla protezione dei dati e prevede misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato.
Gli Stati membri possono mantenere o introdurre ulteriori condizioni, comprese limitazioni, con riguardo al trattamento di dati genetici, dati biometrici o dati relativi alla salute.

1.9. Diritto di accesso dell'interessato (art. 15)

L'interessato ha il diritto di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e in tal caso, di ottenere l'accesso ai dati personali e alle seguenti informazioni:
a) le finalità del trattamento;
b) le categorie di dati personali in questione;
c) 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;

d) quando possibile, il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
e) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento la rettifica o la cancellazione dei dati personali o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento;
f) il diritto di proporre reclamo a un'autorità di controllo;
g) qualora i dati non siano raccolti presso l'interessato, tutte le informazioni disponibili sulla loro origine;
h) l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22 del Regolamento, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.
Qualora i dati personali siano trasferiti a un paese terzo o a un'organizzazione internazionale, l'interessato ha il diritto di essere informato dell'esistenza di garanzie adeguate ai sensi dell'articolo 46 del Regolamento relative al trasferimento.
Il titolare del trattamento fornisce una copia dei dati personali oggetto di trattamento. In caso di ulteriori copie richieste dall'interessato, il titolare del trattamento può addebitare un contributo spese ragionevole basato sui costi amministrativi. Se l'interessato presenta la richiesta mediante mezzi elettronici, e salvo indicazione diversa dell'interessato, le informazioni sono fornite in un formato elettronico di uso comune.
Il diritto di ottenere una copia di cui al paragrafo precedente non deve ledere i diritti e le libertà altrui.

1.10. Diritto di rettifica (art. 16)

L'interessato ha il diritto di ottenere dal titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo. Tenuto conto delle finalità del trattamento, l'interessato ha il diritto di ottenere l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa.

1.11. Diritto alla cancellazione (diritto all'oblio) (art. 17)

L'interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo e il titolare del trattamento ha l'obbligo di cancellare senza ingiustificato ritardo i dati personali, se sussiste uno dei motivi seguenti:
a) i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati;
b) l'interessato revoca il consenso su cui si basa il trattamento conformemente all'articolo 6, paragrafo 1, lettera a), o all'articolo 9, paragrafo 2, lettera a) del Regolamento, e se non sussiste altro fondamento giuridico per il trattamento;
c) l'interessato si oppone al trattamento ai sensi dell'articolo 21, paragrafo 1 del Regolamento, e non sussiste alcun motivo legittimo prevalente per procedere al trattamento, oppure si oppone al trattamento ai sensi dell'articolo 21, paragrafo 2 del Regolamento;
d) i dati personali sono stati trattati illecitamente;
e) 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;
f) i dati personali sono stati raccolti relativamente all'offerta di servizi della società dell'informazione di cui all'articolo 8, paragrafo 1 del Regolamento.

Il titolare del trattamento, se ha reso pubblici dati personali ed è obbligato, ai sensi del paragrafo precedente, a cancellarli, tenendo conto della tecnologia disponibile e dei costi di attuazione adotta le misure ragionevoli, anche tecniche, per informare i titolari del trattamento che stanno trattando i dati personali della richiesta dell'interessato di cancellare qualsiasi link, copia o riproduzione dei suoi dati personali.
I paragrafi che precedono non si applicano nella misura in cui il trattamento sia necessario:
a) per l'esercizio del diritto alla libertà di espressione e di informazione;
b) per l'adempimento di un obbligo legale che richieda il trattamento previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento o per l'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui è investito il titolare del trattamento;
c) per motivi di interesse pubblico nel settore della sanità pubblica in conformità dell'articolo 9, paragrafo 2, lettere h) e i), e dell'articolo 9, paragrafo 3 del Regolamento;
d) a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici conformemente all'articolo 89, paragrafo 1 del Regolamento, nella misura in cui il diritto di cui al primo paragrafo rischi di rendere impossibile o di pregiudicare gravemente il conseguimento degli obiettivi di tale trattamento; o
e) per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

1.12. Diritto alla portabilità dei dati (art. 20)

L'interessato ha il diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano forniti a un titolare del trattamento e ha il diritto di trasmettere tali dati a un altro titolare del trattamento senza impedimenti da parte del titolare del trattamento cui li ha forniti qualora:
a) il trattamento si basi sul consenso ai sensi dell'articolo 6, paragrafo 1, lettera a), o dell'articolo 9, paragrafo 2, lettera a) del Regolamento, o su un contratto ai sensi dell'articolo 6, paragrafo 1, lettera b) del Regolamento; e
b) il trattamento sia effettuato con mezzi automatizzati.
Nell'esercitare i propri diritti relativamente alla portabilità dei dati a norma del paragrafo precedente, l'interessato ha il diritto di ottenere la trasmissione diretta dei dati personali da un titolare del trattamento all'altro, se tecnicamente fattibile.
L'esercizio del diritto di cui al primo paragrafo del presente punto lascia impregiudicato l'articolo 17 del Regolamento. Tale diritto non si applica al trattamento necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento.
Il diritto di cui al primo paragrafo non deve ledere i diritti e le libertà altrui.

1.13. Responsabilità del titolare del trattamento (art. 24)

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 precedente 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 del Regolamento può essere utilizzata come elemento per dimostrare il rispetto degli obblighi del titolare del trattamento.

1.14. Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita (art. 25)

Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso il titolare del trattamento mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati.
Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica.
Un meccanismo di certificazione approvato ai sensi dell'articolo 42 del Regolamento può essere utilizzato come elemento per dimostrare la conformità ai requisiti di cui ai paragrafi precedenti.

1.15. Responsabile del trattamento (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 del Regolamento;
d) rispetti le condizioni di cui ai paragrafi 2 e 4 per ricorrere a un altro responsabile del trattamento;
e) tenendo conto della natura del trattamento, assista il titolare del trattamento con misure tecniche e 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;
f) assista il titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36 del Regolamento, 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 precedente lettera h), il responsabile del trattamento informa immediatamente il titolare del trattamento qualora, a suo parere, un'istruzione violi il 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 precedente 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 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 del Regolamento può essere utilizzata come elemento per dimostrare le garanzie sufficienti di cui ai paragrafi 1 e 4 del presente paragrafo.

1.16. Registri delle attività di trattamento

Ogni titolare del trattamento e, ove applicabile, il suo rappresentante tengono un registro delle attività di trattamento svolte sotto la propria responsabilità. Tale registro contiene tutte le seguenti informazioni:

a) il nome e i dati di contatto del titolare del trattamento e, ove applicabile, del contitolare del trattamento, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati;
b) le finalità del trattamento;
c) una descrizione delle categorie di interessati e delle categorie di dati personali;
d) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;
e) ove applicabile, i trasferimenti di dati personali verso un paese terzo o 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 adeguate;
f) ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
g) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1 del Regolamento.
Ogni responsabile del trattamento e, ove applicabile, il suo rappresentante tengono un registro di tutte le categorie di attività relative al trattamento svolte per conto di un titolare del trattamento, contenente:
a) il nome e i dati di contatto del responsabile o dei responsabili del trattamento, di ogni titolare del trattamento per conto del quale agisce il responsabile del trattamento, del rappresentante del titolare del trattamento o del responsabile del trattamento e, ove applicabile, del responsabile della protezione dei dati;
b) le categorie dei trattamenti effettuati per conto di ogni titolare del trattamento;
c) ove applicabile, i trasferimenti di dati personali verso un paese terzo o 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 del Regolamento, la documentazione delle garanzie adeguate;
d) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1 del Regolamento.
I registri di cui ai paragrafi precedenti sono tenuti in forma scritta, anche in formato elettronico.
Su richiesta, il titolare del trattamento o il responsabile del trattamento e, ove applicabile, il rappresentante del titolare del trattamento o del responsabile del trattamento mettono il registro a disposizione dell'autorità di controllo.
Gli obblighi di cui ai paragrafi precedenti non si applicano alle imprese o organizzazioni con meno di 250 dipendenti, a meno che il trattamento che esse effettuano possa presentare un rischio per i diritti e le libertà dell'interessato, il trattamento non sia occasionale o includa il trattamento di categorie particolari di dati di cui all'articolo 9, paragrafo 1, o i dati personali relativi a condanne penali e a reati di cui all'articolo 10 del Regolamento.

1.17. Notifica di una violazione dei dati personali all'autorità di controllo (art. 33)

In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'articolo 55 del Regolamento senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo.

Il responsabile del trattamento informa il titolare del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione.
La notifica di cui al paragrafo 1 deve almeno:
a) descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
b) comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
c) descrivere le probabili conseguenze della violazione dei dati personali;
d) descrivere le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.
Qualora e nella misura in cui non sia possibile fornire le informazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo.
Il titolare del trattamento documenta qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio. Tale documentazione consente all'autorità di controllo di verificare il rispetto dell'art. 33 del Regolamento.

1.18. Comunicazione di una violazione dei dati personali all'interessato (art. 34)

Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo.
La comunicazione all'interessato di cui al paragrafo precedente descrive con un linguaggio semplice e chiaro la natura della violazione dei dati personali e contiene almeno le informazioni e le misure di cui all'articolo 33, paragrafo 3, lettere b), c) e d) del Regolamento.
Non è richiesta la comunicazione all'interessato di cui al paragrafo 1 se è soddisfatta una delle seguenti condizioni:
a) 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 della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;
b) 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 di cui al paragrafo 1;
c) detta comunicazione richiederebbe sforzi sproporzionati.
In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.
Nel caso in cui il titolare del trattamento non abbia ancora comunicato all'interessato la violazione dei dati personali, l'autorità di controllo può richiedere, dopo aver valutato la probabilità che la violazione dei dati personali presenti un rischio elevato, che vi provveda o può decidere che una delle condizioni di cui al paragrafo 3 è soddisfatta.

1.19. Valutazione d'impatto sulla protezione dei dati (art. 35)

Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali. Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi.
Il titolare del trattamento, allorquando svolge una valutazione d'impatto sulla protezione dei dati, si consulta con il responsabile della protezione dei dati, qualora ne sia designato uno.
La valutazione d'impatto sulla protezione dei dati di cui al paragrafo 1 è richiesta in particolare nei casi seguenti:
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 del Regolamento, o di dati relativi a condanne penali e a reati di cui all'articolo 10; o
c) la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.
L'autorità di controllo redige e rende pubblico un elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi del paragrafo 1. L'autorità di controllo comunica tali elenchi al comitato di cui all'articolo 68 del Regolamento.
L'autorità di controllo può inoltre redigere e rendere pubblico un elenco delle tipologie di trattamenti per le quali non è richiesta una valutazione d'impatto sulla protezione dei dati. L'autorità di controllo comunica tali elenchi al comitato.
Prima di adottare gli elenchi di cui ai paragrafi 4 e 5, l'autorità di controllo competente applica il meccanismo di coerenza di cui all'articolo 63 del Regolamento se tali elenchi comprendono attività di trattamento finalizzate all'offerta di beni o servizi a interessati o al monitoraggio del loro comportamento in più Stati membri, o attività di trattamento che possono incidere significativamente sulla libera circolazione dei dati personali all'interno dell'Unione.
La valutazione contiene almeno:
a) una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;
b) una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;
c) una valutazione dei rischi per i diritti e le libertà degli interessati di cui al paragrafo 1; e
d) le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.
Nel valutare l'impatto del trattamento effettuato dai relativi titolari o responsabili è tenuto in debito conto il rispetto da parte di questi ultimi dei codici di condotta approvati di cui all'articolo 40 del Regolamento, in particolare ai fini di una valutazione d'impatto sulla protezione dei dati.
Se del caso, il titolare del trattamento raccoglie le opinioni degli interessati o dei loro rappresentanti sul trattamento previsto, fatta salva la tutela degli interessi commerciali o pubblici o la sicurezza dei trattamenti.
Qualora il trattamento effettuato ai sensi dell'articolo 6, paragrafo 1, lettere c) o e) del Regolamento, trovi nel diritto dell'Unione o nel diritto dello Stato membro cui il titolare del trattamento è soggetto una base giuridica, tale diritto disciplini il trattamento specifico o l'insieme di trattamenti in questione, e sia già stata effettuata una valutazione ''impatto sulla protezione dei

dati nell'ambito di una valutazione d'impatto generale nel contesto dell'adozione di tale base giuridica, i paragrafi da 1 a 7 non si applicano, salvo che gli Stati membri ritengano necessario effettuare tale valutazione prima di procedere alle attività di trattamento.
Se necessario, il titolare del trattamento procede a un riesame per valutare se il trattamento dei dati personali sia effettuato conformemente alla valutazione d'impatto sulla protezione dei dati almeno quando insorgono variazioni del rischio rappresentato dalle attività relative al trattamento.

2. Elenco dei trattamenti di dati personali

2.1. Le tipologie di dati trattati

La ***SRA SRL*** effettua il trattamento delle tipologie di dati specificate di seguito:

2.1.1. Dati Comuni

"Dato personale comune" è da intendersi qualunque informazione relativa alla persona fisica, persona giuridica, ente o associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale.
Nello svolgimento delle attività, sono trattati i seguenti dati comuni:

1) dei **Fornitori** e dei **Clienti**: relativi all'adempimento degli oneri fiscali connessi con l'approvvigionamento di servizi e beni strumentali dell'***Organizzazione***, relativi alla loro reperibilità e destinati alla corrispondenza con gli stessi;
2) del **Personale**: relativi all'adempimento degli oneri fiscali, tributari, previdenziali e assistenziali, relativi alla sicurezza sui luoghi di lavoro, relativi alla loro reperibilità e destinati alla corrispondenza con gli stessi; sono inclusi i dati dei **Familiari dei lavoratori dipendenti**, relativamente al godimento di alcuni diritti (ad esempio, Assegni Nucleo Familiare, permessi ex L.104 per assistere familiari in condizioni di grave disabilità, ecc.).

2.1.2. Dati Sensibili

"Dato sensibile" è qualsiasi dato personale idoneo a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché idoneo a rivelare lo stato di salute e la vita sessuale.
Più specificatamente, L'Organizzazione tratta i seguenti dati sensibili:

1) del **Personale Dipendente**: inerenti i rapporti con gli enti previdenziali e assistenziali, idonei a rivelare l'adesione a organizzazioni sindacali o idonei a rivelare lo stato di salute; anche in questo caso sono inclusi i dati dei **Familiari dei lavoratori dipendenti**, relativamente al godimento di alcuni diritti.

2.1.3. Dati Giudiziari

"Dato Giudiziario" è qualsiasi dato idoneo a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del D.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale.

Più specificatamente, L'Organizzazione tratta i seguenti dati giudiziari:

1) del **Personale**: idonei a rivelare la sussistenza di processi penali in corso, di condanne penali o provvedimenti e, in particolare, di condanne penali o sanzioni interdittive all'esercizio di attività a contatto con minori.

2.2. Le tipologie dei trattamenti

Nelle tabelle di seguito sono descritte, sinteticamente, le tipologie di trattamento effettuate. Esse sono divise in cinque categorie.
Nella prima tabella si illustrano le finalità perseguite e l'attività svolta per ciascuna categoria, si elencano le categorie di interessati, si specifica la natura dei dati, le strutture aziendali di riferimento e quelle che concorrono al trattamento; si indica infine il responsabile degli archivi e si evidenzia se il trattamento avviene con mezzi informatici e\o cartacei.
Nelle due tabelle seguenti, si specifica l'ubicazione fisica degli archivi, le modalità di accesso, si identificano i destinatari e le modalità di comunicazione e diffusione dei dati.
A proposito di quest'ultima fattispecie, si ribadisce quanto evidenziato in tabella e cioè che la ***SRA SRL*** ***non effettua diffusione di alcun dato trattato al suo interno***.

Tabella 2.2.1 *Elenco dei trattamenti: informazioni essenziali*

Descrizione sintetica del trattamento			Natura dei dati trattati (1)			Struttura di riferimento e responsabile degli archivi	Strutture (interne e esterne) che concorrono al trattamento	Descrizione degli strumenti utilizzati	
Codice identifica	Finalità perseguita o Attività svolta	Categorie di Interessati ai quali si riferisce il trattamento	C	S	G			C	E
ID1	Gestione contabile e fiscale aziendale	Clienti e Fornitori di beni e servizi Personale e Professionisti Enti Gestori ambientali	X			**Direzione Amministrativa** Amministratore Unico Antonio Cancro	**Impiegati amministrativi** Rossella Cerullo Carmela Padovani Francesca Mansione Antonio Cancro Benedetto Sica Ciro Donnarumma **Dott. Martino De Stefano Consulente fiscale**	X	X
ID2	Gestione giuridico-economica e della sicurezza sul luogo di lavoro del personale dipendente[3]	Personale dipendente Familiari del personale dipendente	X	X	X	**Direzione Amministrativa** Amministratore Unico e RSPP Antonio Cancro	**Impiegati amministrativi** Gianluca Santimone **Dott. Antonio Cerrato Medico Competente** **Dott. Felice Cece Consulente del lavoro**	X	X
ID3	Gestione del personale di sub appaltatori Inserimento dati su portale COREPLA	Personale dipendente proprio e dei sub appaltatori	X	X		**Direzione Amministrativa** Amministratore Unico Antonio Cancro	**Impiegati amministrativi** Gianluca Santimone Antonio Cancro	X	X

[1] Natura dei dati trattati: la lettera "**C**" indica che si tratta di dati personali comuni, la lettera "**S**" che si tratta di dati sensibili e la lettera "**G**" che si tratta di dati giudiziari.
[2] Descrizione degli strumenti utilizzati: la lettera "**C**" indica l'utilizzo di archivi cartacei (fascicoli) mente la lettera "**E**" indica l'utilizzo di strumenti elettronici.
[3] Inclusi volontari e tirocinanti

Tabella 2.2.2 *Elenco dei trattamenti: ulteriori elementi per descrivere gli strumenti*

ID del trattamento	Archivi informatici e cartacei di riferimento	Ubicazione fisica dei supporti di memorizzazione (informatici\cartacei)	Tipologia dei dispositivi di accesso	Tipologia di interconnessione
ID 1	*SW gestionale:* WinWast Piattaforma SISTRI *Archivi informatici* [4] *Archivi cartacei:* Faldoni della contabilità Faldoni Sistema di Gestione Faldoni autorizzazioni e formulari	Sede sociale[5] Personal Computer che funge da server Direzione Ufficio amministrativo Ufficio logistica	Personal Computer Archivi cartacei	Rete LAN
ID 2	*Archivi informatici* [1] *Archivi cartacei:* Cedolini paga Elaborazione stipendi Documentazione relativa alla sicurezza sul lavoro Fascicoli del personale Archivio delle cartelle sanitarie e di rischio	Sede sociale Personal Computer che funge da server Direzione Ufficio Amministrativo	Personal Computer Archivi cartacei	Rete LAN
ID 3	*Archivi informatici* [1] *Archivi cartacei:* Registro presenze dipendenti sub appaltatori Documenti identità dipendenti sub appaltatori	Sede sociale Personal Computer che funge da server Ufficio logistica	Personal Computer Archivi cartacei	Rete LAN

[4] Gli archivi informatici diversi dal software WinWast sono contenuti nelle cartelle personali degli operatori.
[5] La sede sociale è situata in Polla (SA), Via Zona Industriale lotto 70-72-74-76.

Tabella 2.2.3 *Comunicazione e diffusione[1] dei dati*

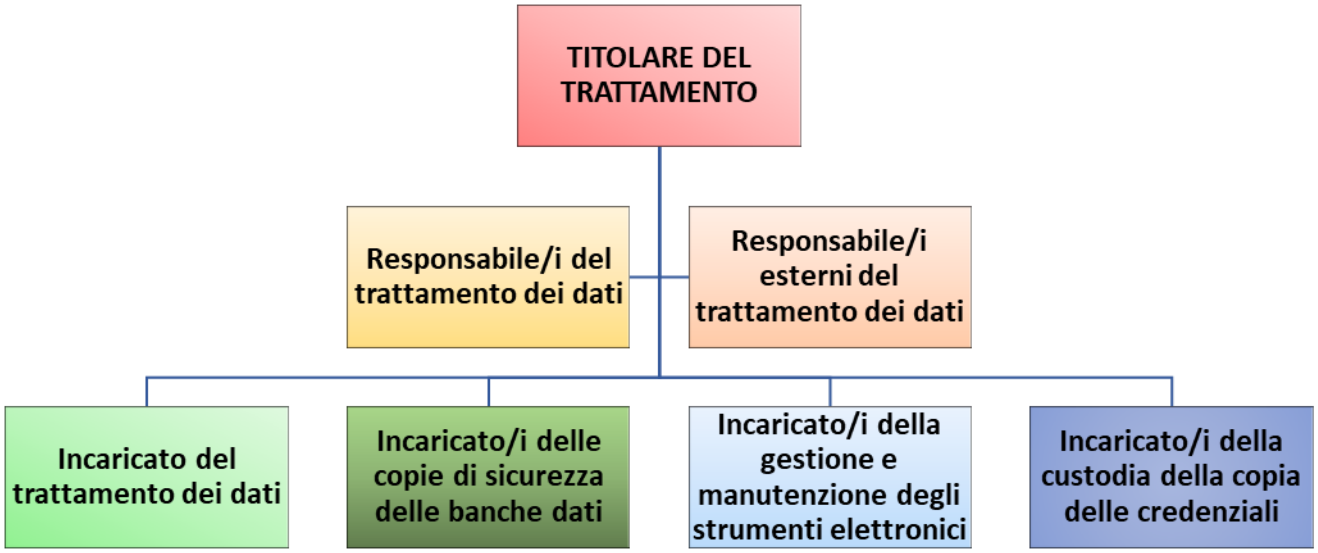
ID del trattamento	Destinatari della comunicazione\diffusione	Modalità di comunicazione\diffusione	Responsabili della comunicazione\diffusione
ID 1	Pubblica Amministrazione Clienti Fornitori Lavoratori dipendenti Trasportatori Operatori ambientali Ministero dell'Ambiente	Contabilità mensile e documenti allegati Comunicazioni di tipo amministrativo MUD Fogli firma mensili Fatture Buste paga Fatture vendita Fatture acquisti Deleghe per il pagamento dei tributi Certificazioni dei compensi Estratti conto	Amministrazione Direzione Amministrativa
ID 2	Pubblica Amministrazione Lavoratori dipendenti	Buste paga Situazioni di famiglia Certificazione Unica Modelli 770 Documentazione prevista dal D. Lgs. 81/2008 Documentazione relativa alla medicina del lavoro	Direzione Amministrativa
ID 3	Fornitori	Registro presenze dipendenti sub appaltatori	Amministrazione

[1] La **SRA SRL** non effettua alcuna attività di diffusione di dati

3. Il modello organizzativo interno

All'interno della struttura sono stati definiti alcuni ruoli al fine di attribuire compiti e responsabilità in accordo con le previsioni del G.D.P.R. e le disposizioni normative. Si realizza pertanto un vero e proprio organigramma per il trattamento e la tutela dei dati che si può riassumere schematicamente nel diagramma riportato nel paragrafo successivo e che viene illustrato nel dettaglio nei paragrafi e nelle tabelle seguenti:

3.1. Organigramma del trattamento e tutela dei dati



3.2. Titolare del trattamento dei dati

È la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri.
Egli è investito del potere di pianificare ed attuare le linee strategiche e organizzative; a questo ampio potere di direzione corrisponde una serie articolata di responsabilità e di adempimenti nei confronti dell'**Interessato** e del Garante.
Il **Titolare del trattamento dei dati** ha il compito di garantire che i dati siano:

a. trattati in modo lecito e secondo correttezza, adottando le misure di sicurezza previste dalla normativa vigente e tese a ridurre al minimo i rischi incombenti (distruzione, accesso non autorizzato, trattamento non consentito);
b. raccolti e registrati per scopi determinati, espliciti e legittimi;
c. esatti e, in caso di necessità, aggiornati;
d. pertinenti, completi e non eccedenti le finalità della raccolta e del trattamento;
e. conservati per un tempo congruo con le finalità del trattamento.

La titolarità del trattamento dei dati non è disponibile: non si può nominare un altro soggetto Titolare. Essa è uno "stato di fatto".
Il Titolare del trattamento dei dati è la SRL SRA *nella persona del/dei suo/suoi rappresentante/i legale/i pro-tempore*

3.3. Responsabile della Protezione dei Dati (Data Protection Officer)

È la persona fisica che ha la responsabilità principale di osservare, valutare e organizzare la gestione del trattamento di dati personali (e dunque la loro protezione) all'interno di un'azienda (sia essa pubblica che privata), affinché questi siano trattati nel rispetto delle normative privacy europee e nazionali.
Questo soggetto è già conosciuto nel mondo anglosassone con il termine di Chief Privacy Officer (CPO); Privacy Officer, Data Protection Officer o Data Security Officer.
Il Regolamento disciplina l'istituzione della figura del Data Protection Officer (in italiano Responsabile della Protezione dei Dati) nei seguenti casi:
a) il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali;
b) le attività principali del Titolare del trattamento o del Responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala; oppure
c) le attività principali del Titolare del trattamento o del Responsabile del trattamento consistono nel trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9 (dati particolari | sensibili) o di dati relativi a condanne penali e a reati di cui all'articolo 10.
L'articolo 9 del Regolamento al comma 1 definisce quelli che sono le categorie particolari di dati personali (ex dati sensibili) ed in particolare i dati personali che: "rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona".
L'art. 39 del Regolamento europeo sulla protezione dei dati personali elenca i principali compiti del DPO (Responsabile della protezione dei dati):

1. Il responsabile della protezione dei dati è incaricato almeno dei seguenti compiti:
a) informare e fornire consulenza al Titolare del trattamento o al Responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal presente regolamento nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;
b) sorvegliare l'osservanza del presente regolamento, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del Titolare del trattamento o del Responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;
c) fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35;
d) cooperare con l'autorità di controllo; e
e) fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.
2. Nell'eseguire i propri compiti il responsabile della protezione dei dati considera debitamente i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo.
Tenendo conto di quanto sopra riportato e dei chiarimenti pubblicati dal Garante per la protezione dei dati personali nelle "Nuove Faq sul Responsabile della Protezione dei Dati (RPD) in ambito privato (in aggiunta a quelle adottate dal Gruppo Art. 29 in Allegato alle Linee guida sul RPD)", **nel caso della SRA SRL non sussistono i presupposti per la nomina del DPO**.

3.4. Responsabile del trattamento dei dati

È la persona fisica o giuridica, appartenente o non alla **SRA SRL,** che assume un ruolo che comporta il coordinamento delle attività inerenti il trattamento di dati personali.
La nomina viene effettuata dal **Titolare del trattamento dei dati** tramite contratto o altro atto giuridico a norma del diritto dell'Unione o degli Stati membri ai sensi dell'art. 28 del Regolamento UE 2016/679.
Tale nomina ha delle caratteristiche peculiari: il disposto del Regolamento UE 2016/679 indica che l'atto di nomina specifichi "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". Quindi, a poter assegnare la gestione del trattamento dei dati di propria pertinenza (in tutto o in parte), è il **Titolare** (e solo lui) e nella sua disponibilità rimane il potere di direzione (cioè le decisioni riguardanti i fini, i mezzi e le modalità del trattamento stesso).
La designazione del **Responsabile** è facoltativa; va effettuata "qualora un trattamento debba essere effettuato per conto del titolare del trattamento". Per l'ordinamento vigente, trattare dati personali costituisce, di per sé, attività pericolosa; per questo motivo, grava sul **Titolare** l'onere di dimostrare di aver fatto tutto il possibile per evitare il danno (inversione dell'onere della prova) essendo sufficiente, per il danneggiato, provare solamente il semplice danno e non il nesso di causalità con la condotta del presunto danneggiante.
Il quadro normativo di riferimento richiede che l'attenzione sia mantenuta altissima, soprattutto in contesti che, per dimensioni strutturali oppure per mole o delicatezza dei trattamenti effettuati, richiedono capacità pratiche ed operative e\o tempi di applicazione che travalicano quelli disponibili da parte del **Titolare**; la predisposizione di una organizzazione consapevole e

proporzionata, anche attraverso la designazione di uno o più **Responsabili**, testimonia l'effettiva precauzionale attivazione del **Titolare** in relazione ai rischi gravanti sull'attività.
La nomina può essere a tempo determinato ed a tempo indeterminato; nel secondo caso decade per dimissioni oppure per revoca; quest'ultima può essere disposta dal **Titolare del trattamento dei dati** senza alcun preavviso.
Riguardo ai requisiti che deve possedere il nominando **Responsabile**, la normativa specifica che essi debbano presentare "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". Essi sono da ricercare alla luce dell'idoneità, della predisposizione e dell'inclinazione del soggetto a coadiuvare il **Titolare** e a svilupparne le strategie.
Pertanto, più che valutare la specifica competenza in materia di legislazione sul trattamento e tutela dei dati, il **Titolare** è chiamato a ricercare il potenziale del nominando, anche in riferimento a quanto espresso nel passato rispetto ad incarichi similari, che cioè comportassero mansioni organizzative con incombenze normative.
Il **Titolare** ha precisi obblighi non solo *in eligendo* ma anche *in vigilando* rispetto all'attività del **Responsabile** ed è quindi tenuto a verificare costantemente l'idoneità della propria scelta, essendo tenuto a rispondere del fatto antigiuridico del **Responsabile** nel caso non presenti obiettivamente i requisiti richiesti.
È infine possibile nominare più **Responsabili** laddove lo richiedano il numero di addetti, le tipologie di dati trattati, la suddivisine interna delle attività aziendali, la dislocazione territoriale degli uffici\filiali\divisioni, ecc.
In ogni caso, è opportuno dare visibilità alla nomina del **Responsabile**, attraverso il proprio sito internet oppure attraverso le informative affisse o consegnate agli **Interessati**: ciò sia al fine di veicolare alla persona giusta le richieste che potrebbero provenire dagli **Interessati** sia per dimostrare, durante un eventuale controllo, che il **Titolare** ha inteso migliorare, attraverso tale nomina, la qualità del proprio ambiente di trattamento dei dati e facilitare la promozione di eventuali istanze attraverso la massima trasparenza.

Nell'atto di nomina, il **Titolare** deve indicare analiticamente i compiti (e quindi le responsabilità) del **Responsabile**.
Di seguito, un maggiore dettaglio dei compiti e delle responsabilità di questa figura:

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 del Regolamento;

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

e) tenendo conto della natura del trattamento, assista il titolare del trattamento con misure tecniche e 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;

f) assista il titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36 del Regolamento, 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.

L'Azienda, vista la natura e l'esiguità dei dati personali trattati in Azienda, non ha provveduto a nominare un Responsabile del trattamento dei dati interno; ha individuato e nominato tutti i professionisti od aziende esterne che vengano in contatto, utilizzino e custodiscano dati dell'***Organizzazione***.

Questi ultimi sono di seguito riportati.

Tabella 3.3.1 – *Elenco dei Responsabili esterni del trattamento dei dati*

1	**Professionista\Azienda**	**Consulenza del lavoro Dott. Felice Cece**
	Indirizzo e P.IVA	Via M. De Sena, 234 80035 Nola (NA) tel. 0818238101; cell. 3339659484 C.F. CCEFLC79S06F839Y P.IVA
	Responsabile del trattamento	Dott. Felice Cece
	Incaricati del trattamento	
	Finalità del trattamento	Consulenza in materia di lavoro
	Riferimento alle tipologie di trattamento aziendali	ID2, ID3
	Specifica dei dati comuni ai quali accede o che sono trasmessi	Anagrafiche dei lavoratori dipendenti Attestazioni di residenza Attestazioni di stato di famiglia Modelli per richiesta di ANF Rilevazione delle presenze Attestazioni di malattia Domande di ferie e permessi (retribuiti e non) Documentazione riguardante astensione dal lavoro Contratti di cessione del V dello stipendio Fatture fornitori e consulenti Modelli delega F24 Comunicazione Unica dei compensi
	Specifica dei dati sensibili ai quali accede o che sono trasmessi	***Deleghe e permessi sindacali*** ***SINP (Sistema informativo nazionale per la prevenzione nei luoghi di lavoro)*** ***Dichiarazioni di stato di gravidanza***
	Modalità di accesso o trasmissione dei dati	I documenti sono trasmessi in formato cartaceo, con consegna a mano, e in formato digitale

1	**Professionista\Azienda**	**Consulenza del lavoro Dott. Felice Cece**
	Trattamenti che sono effettuati in relazione alla finalità da perseguire	Registrazione per elaborazione cedolini paga Registrazione per elaborazione deleghe F24 Registrazione per elaborazione trattenute sindacali Elaborazione documenti contabili Trasmissione dei dati agli enti previdenziali e assicurativi Elaborazione di prospetti sulla cessione del V dello stipendio Elaborazione modelli CUD Elaborazione modelli F24 Elaborazione bilancio annuale Comunicazione agli enti istituzionali e previdenziali Elaborazione Comunicazione Unica dei Compensi Elaborazione dichiarazione sostituto d'imposta

2	**Professionista\Azienda**	**Consulenza fiscale Dott. Martino De Stefano**
	Indirizzo e P.IVA	Via Udine 6, 84091 Battipaglia (SA) P.IVA 04907620654 CF DSTMTN78T13F839R
	Responsabile del trattamento	Dott. Martino De Stefano
	Incaricati del trattamento	Dott.ssa Martina Marolda
	Finalità del trattamento	Consulenza in materia contabile e fiscale
	Riferimento alle tipologie di trattamento aziendali	ID2
	Specifica dei dati comuni ai quali accede o che sono trasmessi	Anagrafiche Clienti Anagrafiche Fornitori
	Specifica dei dati sensibili ai quali accede o che sono trasmessi	N.A.
	Modalità di accesso o trasmissione dei dati	I documenti sono trasmessi in formato cartaceo, con consegna a mano, e in formato digitale
	Trattamenti che sono effettuati in relazione alla finalità da perseguire	Compilazione registro Iva acquisti Compilazione registro Iva vendite Predisposizione ed invio elenchi clienti e fornitori Predisposizione ed invio dichiarazioni dei redditi Gestione registrazioni contabili

3	**Professionista\Azienda**	**CEDIM Consulting Srls**
	Indirizzo e P.IVA	Via IV Novembre Snc 81030 Carinola (CE) P.IVA 04177250612

	Responsabile del trattamento	Dott. Antonio Cerrato
	Incaricati del trattamento	
	Finalità del trattamento	Adempimenti in materia di sicurezza sui luoghi di lavoro da parte del Medico Competente
	Riferimento alle tipologie di trattamento aziendali	ID2
	Specifica dei dati comuni ai quali accede o che sono trasmessi	Anagrafica dei lavoratori dipendenti Mansionario
	Specifica dei dati sensibili ai quali accede o che sono trasmessi	Referti di esami clinici o strumentali Referti di visite specialistiche Dichiarazioni di stato di gravidanza Cartella sanitaria e di rischio Attestato di idoneità alla mansione
	Modalità di accesso o trasmissione dei dati	L'accesso avviene in modalità cartacea
	Trattamenti che sono effettuati in relazione alla finalità da perseguire	Raccolta dei dati anagrafici Raccolta dei dati relativi alle mansioni Compilazione della cartella sanitaria e di rischio Compilazione dell'attestato di idoneità alla mansione

4	**Professionista\Azienda**	**SI WORK SRL**
	Indirizzo e P.IVA	Via S. Pietro, 7 84060 Perdifumo (SA) P.IVA 05080910655
	Responsabile del trattamento	Antonio Ianni
	Incaricati del trattamento	
	Finalità del trattamento	Consulenza in materia di sicurezza sui luoghi di lavoro D. Lgs. 81/2008.
	Riferimento alle tipologie di trattamento aziendali	ID3
	Specifica dei dati comuni ai quali accede o che sono trasmessi	Anagrafica dei lavoratori dipendenti Anagrafica componenti SPP Mansionario
	Specifica dei dati sensibili ai quali accede o che sono trasmessi	NA
	Modalità di accesso o trasmissione dei dati	I documenti sono trasmessi in formato cartaceo, con consegna a mano, e in formato digitale
	Trattamenti che sono effettuati in relazione alla finalità da perseguire	Redazione DVR Registri corsi di formazione Attestati di formazione

3.5. Incaricato del trattamento dei dati

Il Regolamento UE 2016/679 non menziona e disciplina la figura dell'incaricato al trattamento dei dati. Ai fini della definizione, funzionamento e gestione del modello organizzativo aziendale destinato al trattamento ed alla tutela dei dati, l'***Organizzazione*** ha nominato **Incaricato del trattamento dei dati** chiunque, nel corso del proprio lavoro, debba svolgere qualunque operazione o complesso di operazioni, con o senza l'ausilio di mezzi elettronici o comunque automatizzati, concernente la raccolta, la registrazione, l'organizzazione, la conservazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione dei dati.

Il **Titolare del trattamento dei dati** effettua la nomina attraverso una lettera redatta ai sensi dell'art. 30 del D. Lgs. 196/03: in essa specifica i compiti affidati e le responsabilità. La veste di **Incaricato**, pertanto, non si assume in conseguenza di uno stato di fatto – come accade per il **Titolare** - ma solamente a seguito di una designazione espressa.

Perché la nomina sia valida, non è necessaria l'espressione del consenso da parte dell'**Incaricato**: è sufficiente l'avvenuta ricezione oppure la certa presa visione per dare vita all'incarico. È quindi non obbligatorio ma opportuno che l'**Incaricato** firmi la nomina per presa visione in maniera da creare una maggiore consapevolezza nel preposto e da comprovare l'avvenuta ricezione.

Nel caso in cui il nominato rifiuti la nomina, è compito del **Titolare**

- far comprendere come essa sia "assolutamente ineluttabile" per qualsiasi lavoratore che, nello svolgimento delle proprie mansioni, tratti dati personali,
- illustrare come essa non costituisca un aggravio bensì un'integrazione nell'esecuzione della propria attività quotidiana al fine di renderla più corretta e rispettosa dei diritti altrui,
- chiarire che un rifiuto di fatto di ricevere la nomina costringerebbe il **Titolare** alla commissione di un illecito.

La nomina è a tempo indeterminato e decade per revoca oppure per dimissioni o licenziamento. La revoca comporta la disattivazione delle credenziali per accedere agli archivi informatici ed il divieto di accedere a quelli cartacei e ai locali della struttura dove avviene il trattamento. La nomina deve avvenire prima che l'operatore possa, nell'ambito delle sue mansioni, prendere visione anche di un solo dato personale. In caso contrario, si rientrerebbe nella fattispecie della comunicazione del dato a terzo: sicuramente legittima ma decisamente onerosa da sostenere.

Successivamente alla nomina, il **Titolare del trattamento dei dati** (o il Responsabile, se nominato) ha il compito di informare e formare adeguatamente ciascun **Incaricato del trattamento dei dati** sulle responsabilità ed i compiti a lui affidati.

Riguardo al contenuto della formazione, si faccia riferimento al sottoparagrafo 3.5.1.

È ritenuto necessario dalla ***SRA SRL*** erogare formazione di aggiornamento in occasione di cambiamenti di mansioni, o introduzione di nuovi significativi strumenti rilevanti per il trattamento dei dati personali, nel caso di novità di carattere legislativo, giurisprudenziale oppure interpretativo della normativa di riferimento.

Gli Incaricati sono autorizzati ad accedere agli archivi digitali e cartacei al solo fine di eseguire le operazioni di concetto sotto la diretta autorità e la responsabilità del **Titolare** oppure del **Responsabile del Trattamento dei dati**, attenendosi alle istruzioni impartite.

Gli Incaricati accedono agli elaboratori installati nelle stanze di terapia, nelle sale mediche, nella sala riunioni, nelle stanze dedicate all'amministrazione; attraverso la connessione di rete intranet possono accedere ai dati memorizzati nel server centrale, a condizione di possedere le credenziali necessarie. Inoltre, possono accedere, laddove abilitati, ad alcune tipologie di dati dall'esterno della struttura utilizzando la rete internet.

Di seguito, le principali disposizioni che l'***Organizzazione*** ha impartito e che devono osservare dagli incaricati:

a) trattare i dati personali nella misura necessaria e sufficiente alle finalità del trattamento e, comunque, in modo lecito e secondo correttezza;
b) conservare con la massima segretezza le credenziali informatiche e\o i dispositivi di autenticazione ricevuti, destinandoli ad esclusivo uso personale e informando immediatamente il **Responsabile del trattamento dei dati** in caso di smarrimento oppure di sottrazione;
c) utilizzare, come password per l'accesso al sistema informatico, una parola che rispetti le regole stabilite nel prosieguo del documento e che sono state comunicate attraverso la *Guida pratica per l'incaricato del trattamento dei dati personali*;
d) durante una sessione di trattamento di dati personali, non lasciare lo strumento elettronico incustodito senza avere attivato la protezione (sui sistemi Windows basta premere contemporaneamente il tasto Windows e la lettera "L"[1] per bloccare l'account e impedirne l'utilizzo prima che sia inserita la relativa password); parimenti, non utilizzare un computer nel quale sia stato inserito l'account di un altro operatore;
e) controllare e custodire fino alla restituzione i documenti cartacei loro affidati, impedendo che vi possano avere accesso persone non autorizzate e riponendoli in cassetti o armadi chiusi a chiave nel caso sia necessario tenerli a disposizione oltre il termine dell'orario di lavoro giornaliero;
f) non copiare dati personali su supporti informatici personali (penne usb, schede di memoria, telefono cellulare, ecc);
g) adottare le misure di sicurezza e rispettare le disposizioni impartite durante la formazione iniziale, periodica o straordinaria e attraverso la *Guida Pratica per l'incaricato del trattamento dei dati personali,* soprattutto riguardo agli archivi ai quali è consentito l'accesso, alla tipologia dei dati che è possibile trattare, alle finalità del trattamento, ecc.
h) non diffondere verbalmente, in modo inopinato, dati personali o sensibili acquisiti durante l'attività lavorativa, rispetto ai quali è obbligatorio mantenere un assoluto riserbo; tale divieto riguarda sia l'ambito interno all'azienda che l'ambito esterno e qualsiasi tipologia di dato, anche riguardante la quotidianità della vita aziendale;
i) rispettare sempre, nella comunicazione verbale, le indicazioni inserite nella *Guida Pratica per l'incaricato del trattamento dei dati personali* e presenti nelle procedure aziendali (distanza di cortesia, locali nei quali effettuare la comunicazione, ecc);
j) informare immediatamente il **Titolare** in caso di situazioni anomale o di emergenze.

Rispetto all'ultimo punto, gli **Incaricati** possono essere oggetto del cosiddetto "social engineering" cioè di tecniche psicologiche usate per indurre un soggetto ai propri scopi presentandosi personalmente o contattando dall'esterno a mezzo telefono o posta elettronica. Gli obiettivi possono andare dalla raccolta di informazioni apparentemente innocue riguardanti l'azienda o la sua organizzazione e il personale che vi lavora, ma possono arrivare a raggiungere dati anche molto riservati come quelli sugli Utenti.
Con l'ausilio di messaggi studiati o abili tecniche di persuasione l'aggressore può anche rendere l'**Incaricato** complice inconsapevole di azioni che andranno a proprio beneficio come, ad esempio, l'acquisizione di informazioni o l'ottenimento della fiducia del personale, l'apertura di allegati infetti o la visita di un sito che contiene virus, malware o altro materiale pericoloso.

[1] "L" sta per "lock" che significa chiudere, chiusura. Il tasto "Windows" si trova in basso a sinistra, tra i tasti CTRL e ALT.

È quindi necessario che l'**Incaricato** adotti le seguenti precauzioni:

- non fornire informazioni confidenziali, al telefono o di persona, a interlocutori non conosciuti o non identificati con certezza;
- limitarsi a fornire informazioni a interlocutori noti e operanti in team per disposizione aziendale, nei limiti dei contenuti afferenti all'ambito lavorativo assegnato;
- diffidare di messaggi e-mail provenienti da fonte non conosciuta;
- non aprire messaggi e-mail provenienti da fonte non conosciuta contenenti allegati oppure provenienti da fonte nota ma contenenti allegati sospetti;
- non utilizzare mai link contenuti nel testo del messaggio perché possono essere facilmente falsificati; in questi casi si deve andare direttamente sul sito citato digitandone da capo il nome;
- non trasmettere mai alcuna informazione in risposta ad una richiesta proveniente da fonte sconosciuta;
- non trasmettere mai alcuna informazione in risposta ad una richiesta proveniente da fonti istituzionali o apparentemente conosciute (ad esempio banche) in quanto tali strutture non richiedono mai dati utilizzando questa modalità;
- in caso di dubbio è sempre preferibile verificare l'attendibilità delle richieste con il **Responsabile** o il **Titolare**.

È il caso di precisare che l'***Organizzazione*** ha stabilito che la nomina ad **Incaricato** deve essere formalizzata sia per i lavoratori dipendenti che per i lavoratori consulenti ma anche per eventuali lavoratori che non percepiscano alcun compenso (tirocinanti, stagisti, ecc.): la discriminante riguarda unicamente la possibilità, nell'espletamento delle proprie mansioni, di venire a contatto con dati personali, anche con la semplice visione di essi.
L'organizzazione aziendale, per la particolare attività svolta dall'***Organizzazione***, è basata sulla divisione dei compiti e delle responsabilità in base alla mansione ricoperta (che spesso corrisponde anche alla qualifica del lavoratore). Tale principio è valido anche a proposito del trattamento dei dati personali da parte degli **Incaricati**.
Essi sono suddivisi in gruppi omogenei per mansione e ciascun gruppo ha accesso ad alcuni trattamenti con specifici permessi. Nell'ambito di ciascun trattamento, l'incaricato compie le operazioni necessarie e sufficienti all'adempimento dei propri compiti.
Nella tabella 3.4.1 sono riportati i raggruppamenti di operatori individuati in azienda e coincidenti con le mansioni assegnate, i nominativi degli incaricati che appartengono a ciascun gruppo, le tipologie di trattamenti alle quali ciascun gruppo può accedere, il dettaglio delle operazioni che compiono, i permessi riconosciuti. In una colonna è indicata la revoca della nomina ad **Incaricato**. Sono inoltre presenti alcune note per ciascuna mansione.

Attraverso tali informazioni, viene soddisfatta l'esigenza di formalizzare la portata dell'autorizzazione al trattamento per ciascun **Incaricato** e, contemporaneamente, di responsabilizzarlo attraverso una informazione puntuale sulle attività che può compiere sui dati e sulle finalità di esse; le tabelle rappresentano un vero e proprio mansionario del trattamento e della tutela dei dati per le figure coinvolte e costituiscono una integrazione al mansionario generale.
In accordo con esse, viene stabilito il profilo di autorizzazione cioè quali aree del sistema informatico possano essere utilizzate per lo svolgimento dell'attività (vedi paragrafo 7.2).
Laddove ad un lavoratore siano assegnate più mansioni, egli dovrà fare riferimento alle diverse tabelle nelle quali è incluso il suo nome; nel caso i permessi assegnati ad una medesima operazione di trattamento siano in conflitto, è ovvio che prevalgano quelli più rilevanti.

Tabella 3.5.1 – *Elenco delle mansioni, degli ambiti di trattamento, dei permessi*

Direzione Amministrativa												
Trattamento	**Operazioni**	**Permessi**					**Archivi**		**Tipologia di operazione**			
		Lettura	**Scrittura**	**Modifica**	**Cancellazione**	**Stampa**	**Cartacei**	**Elettronici**	**Produzione o acquisizione**	**Conservazione**	**Comunicazione o diffusione**
ID1	Anagrafiche Clienti	X	X	X	X	X		X	X	X	X
	Anagrafiche Fornitori	X	X	X	X	X		X	X	X	X
	Anagrafiche Gestori Ambientali	X	X	X	X	X		X	X	X	X
	Rendicontazione mensile delle prestazioni erogate	X	X	X	X	X	X	X	X	X	X
	Formulari										
	Area amministrativa del programma gestionale	X	X	X	X	X		X	X	X	
	Rubrica telefonica	X	X	X	X	X	X	X			
	Fatture fornitori e professionisti	X					X		X	X	X
	Elenchi fornitori	X	X	X	X		X	X	X	X	
	Riepiloghi fatture e pagamenti	X	X	X	X	X		X	X	X	X
	Fatturazione mensile Clienti	X	X	X	X	X	X	X	X	X	X
ID2	Curricula	X					X	X	X	X	
	Anagrafica lavoratori, consulenti e dipendenti	X	X	X	X	X	X	X	X	X	X
	Cedolini paga	X	X	X		X	X	X	X	X	X
	Stato di famiglia	X					X		X	X	X
	Rendiconto delle presenze mensili	X	X	X	X	X		X	X	X	X
	Richieste di ferie e permessi	X					X		X	X	X
ID3	Rendiconto delle presenze mensili	X	X	X	X	X		X	X	X	X
	Copia documenti di riconoscimento	X	X	X	X	X	X	X	X	X	X
Note:												

Incaricati	Revocati
Antonio Cancro	

Impiegato amministrativo												
Trattamento	**Operazioni**	**Permessi**					**Archivi**		**Tipologia di operazione**		
		Lettura	**Scrittura**	**Modifica**	**Cancellazione**	**Stampa**	**Cartacei**	**Elettronici**	**Produzione o acquisizione**	**Conservazione**	**Comunicazione o diffusione**
ID1	Anagrafiche Clienti	X	X	X	X	X		X	X	X	X
	Anagrafiche Fornitori	X	X	X	X	X		X	X	X	X
	Anagrafiche Gestori Ambientali	X	X	X	X	X		X	X	X	X
	Rendicontazione mensile delle prestazioni erogate	X	X	X	X	X	X	X	X	X	X
	Formulari										
	Area amministrativa del programma gestionale	X	X	X	X	X		X	X	X	
	Rubrica telefonica	X	X	X	X	X	X	X			
	Fatture fornitori e professionisti	X					X		X	X	X
	Elenchi fornitori	X	X	X	X		X	X	X	X	
	Riepiloghi fatture e pagamenti	X	X	X	X	X		X	X	X	X
	Fatturazione mensile Clienti	X	X	X	X	X	X	X	X	X	X
ID2	Curricula	X					X	X	X	X	
	Anagrafica lavoratori, consulenti e dipendenti	X	X	X	X	X	X	X	X	X	X
	Cedolini paga	X	X	X		X	X	X	X	X	X
	Stato di famiglia	X					X		X	X	X
	Rendiconto delle presenze mensili	X	X	X	X	X		X	X	X	X
	Richieste di ferie e permessi	X					X		X	X	X
ID3	Rendiconto delle presenze mensili	X	X	X	X	X		X	X	X	X
	Copia documenti di riconoscimento	X	X	X	X	X	X	X	X	X	X
Note:											

Incaricati	Revocati
Rossella Cerullo	

Carmela Padovani	
Francesca Mansione	
Antonio Cancro	
Benedetto Sica	
Gianluca Santimone	
Ciro Donnarumma	

3.5.1. Le modalità e il contenuto della formazione degli Incaricati

La normativa vigente non specifica le modalità di erogazione della formazione agli **Incaricati**. Le tre opzioni più comuni sono l'intervento cartaceo, quello attraverso un prodotto audio-visivo o informatico e quello di formazione interattiva, in aula.
L'***Organizzazione*** effettua una formazione iniziale durante un incontro individuale tenuto con l'operatore dal **Titolare** o da un delegato qualificato (eventuale **Responsabile** oppure consulente esterno). La formazione periodica è erogata invece durante incontri ai quali partecipano tutti gli **Incaricati**.
La formazione supplementare, laddove intervengano cambiamenti di mansione o siano introdotti nuovi strumenti o programmi informatici, viene erogata individualmente oppure per gruppi omogenei di **Incaricati**.
Alla formazione diretta si associa sempre la consegna di materiale cartaceo rappresentato dalla *Guida pratica per l'Incaricato* e da eventuali circolari o ordini di servizio; in occasione della consegna, si prescrive all'**Incaricato** di prendere atto dei loro contenuti prima di iniziare la propria attività sui dati, di consultare i documenti ricevuti nel caso in cui sopraggiungano dubbi in merito ad una operazione di trattamento o alla sicurezza dei dati e di rivolgersi al **Titolare** o al **Responsabile** nel caso tali dubbi permangano.
Riguardo ai contenuti della formazione iniziale, l'obiettivo preliminare è quello di sensibilizzare gli **Incaricati** circa il diritto al trattamento ed alla protezione dei dati, rendendoli consapevoli di quanto esso sia il diritto di ogni cittadino e quindi riguardi ciascuno di essi, nella vita privata e in quella professionale: tale tipo di coinvolgimento personale è il viatico per promuovere il rispetto del trattamento e protezione dei dati.
È quindi necessario introdurre le principali definizioni dei termini utilizzati, le figure fondamentali, i principi e le regole generali per il trattamento.
L'aspetto della sicurezza dei dati deve essere affrontato elencando i rischi incombenti ed esponendo le misure e le procedure messe in atto dalla struttura per prevenire gli eventi dannosi, sottolineando l'importanza di un comportamento idoneo nel rapporto con l'**Interessato** e verso i terzi.
Devono essere fornite regole e istruzioni precise per la tenuta dei dati contenuti su supporto cartaceo, per il corretto utilizzo degli strumenti elettronici e per il comportamento da tenere nei rapporti con soggetti terzi: tali istruzioni devono permettere di implementare non solo misure minime di protezione ma misure idonee e confacenti alla realtà aziendale.
La scaletta dell'intervento formativo sopra delineata è ovviamente solo una traccia, da adattare alle esigenze di formazione del singolo **Incaricato**, e rispetta la struttura della *Guida Pratica per l'Incaricato*.

È importante sollecitare tutti gli incaricati di partecipare attivamente e proattivamente al miglioramento delle procedure, dei documenti e del "sistema G.D.P.R." al fine di abbassare il livello di rischio incombente sui dati personali trattati dall'azienda.
I contenuti della formazione successiva sono determinati caso per caso e sono registrati utilizzando le schede di addestramento predisposte nell'ambito del S.G.Q.; esse contengono anche l'elenco dei soggetti formati e l'attestazione dell'avvenuta formazione. Nel caso di formazione periodica, essa è pianificata all'interno del Piano di Formazione Aziendale annuale e registrata con le medesime modalità.

L'***Organizzazione*** ha esternalizzato i servizi di pulizia dei locali; anche nello svolgimento di questi servizi sono state valutate ed adottare delle precauzioni riguardanti la protezione dei dati personali, come specificato nei due paragrafi seguenti:

3.5.2. Servizio pulizie

Gli operatori dell'impresa di pulizie accedono ai locali ad accesso controllato oppure limitato per compiere le ordinarie operazioni di pulizia.
Gli operatori sono informati sui divieti e sulle cautele da adottare attraverso un documento che ricevono e sottoscrivono.

3.6. Registro delle attività dei trattamenti

L'art. 30, comma 1, del Regolamento prevede che ogni titolare del trattamento e, ove applicabile, il suo rappresentante, tengono un registro delle attività di trattamento svolte sotto la propria responsabilità.
Inoltre, al comma 2, è indicato che ogni responsabile del trattamento e, ove applicabile, il suo rappresentante, tengono un registro di tutte le categorie di attività relative al trattamento svolte per conto di un titolare del trattamento
Al comma 5 è riportato che gli obblighi di cui ai commi 1 e 2 non si applicano alle imprese o organizzazioni con meno di 250 dipendenti, a meno che il trattamento che esse effettuano possa presentare un rischio per i diritti e le libertà dell'interessato, il trattamento non sia occasionale o includa il trattamento di categorie particolari di dati di cui all'articolo 9, paragrafo 1, o i dati personali relativi a condanne penali e a reati di cui all'articolo 10.
Non rilevandosi nel caso della ***SRA SRL*** la sussistenza dei requisiti riportati al comma 5, l'Organizzazione non provvede alla redazione del Registro delle attività dei trattamenti.

4. I diritti dell'interessato

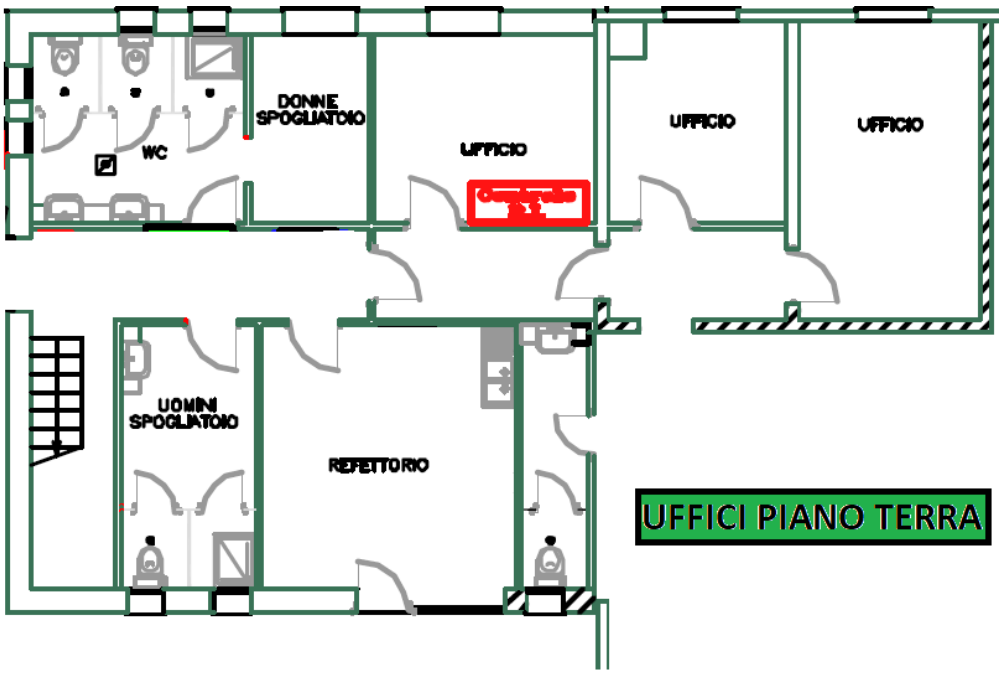
Per quanto riguarda la conoscenza, gestione e trattamento dei diritti dell'interessato, sintetizzabili nei seguenti punti:

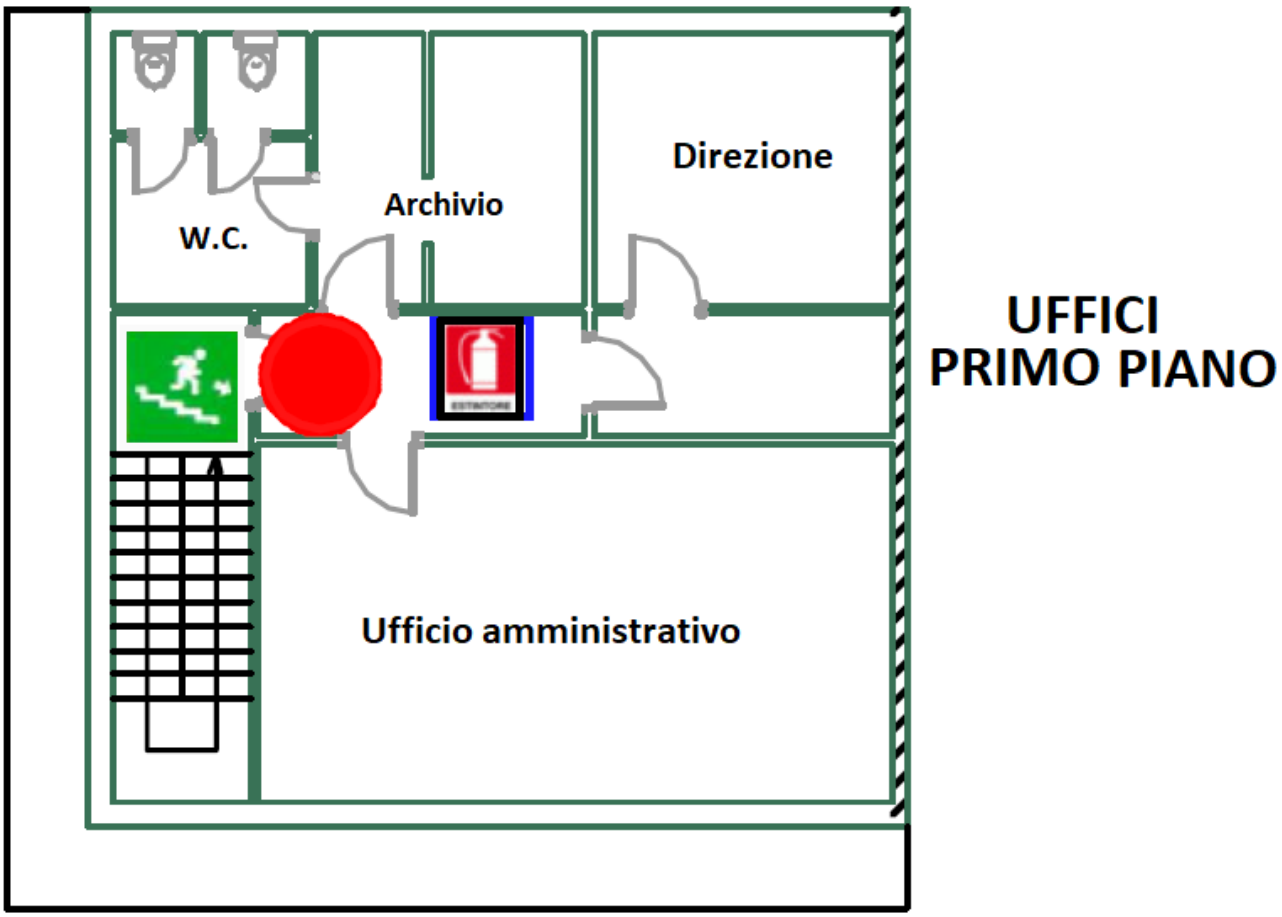
- Trasparenza e modalità di trattamento
- Informazione ed accesso ai dati personali
- Rettifica e cancellazione
- Diritto di opposizione e processo decisionale automatizzato relativo alle persone fisiche
- Limitazioni

si richiama integralmente il Capo III del Regolamento UE 2016/679, dall'art. 12 all'art. 23.

5. I luoghi fisici

Per l'esatta redazione del presente documento sono stati analizzati i luoghi ove si svolge materialmente il trattamento dei dati personali, ove sono conservati i dati stessi, e, infine, ove si trovano i sistemi di elaborazione.
Nelle tabelle che seguono sono riportate le planimetrie dei luoghi fisici dove vengono effettuate le attività oggetto del presente documento:





Nella tabella 5.1 è fornito l'elenco di tali luoghi; per ciascuno:

- si indica se al suo interno si effettuino operazioni di trattamento dei dati, se vi si conservino dati e se vi si trovino sistemi di elaborazione (computer o server);
- si specifica a quale banca dati facciano riferimento gli archivi oppure il trattamento;
- si riporta se si tratti di un locale aperto al pubblico (ma comunque presidiato da un operatore nelle ore di apertura della struttura) al quale cioè l'utente accede autonomamente, se si tratti di un locale al quale l'utente può accedere solamente quando accompagnato da un operatore oppure se si tratti di un locale con accesso riservato agli incaricati autorizzati;
- nelle note si elencano (in grassetto) i contenitori nei quali è possibile conservare documenti contenenti dati; fa eccezione il locale archivio che è esso stesso un contenitore.

Tabella 5.1 *Luoghi fisici nei quali avviene il trattamento*

Sede dove si effettuano i trattamenti:	**SRA Srl**
Indirizzo:	**Via Zona Industriale lotto 70-72-74-76**
Città:	**Polla (SA)**

Descrizione del locale	Si effettua trattamento	Si conservano i dati	Vi si trovano sistemi di elaborazione	ID1	ID2	ID3	ID4	Aperto al pubblico \ presidiato	Accesso consentito al pubblico solo accompagnato	Accesso riservato agli incaricati	Note
Ufficio Amministratore	X	X	X	X	X	X	X			X	Vi si trovano un **armadio con chiusura a chiave**, una **cassettiera** dotata di serratura, un pc. Il locale è accessibile solo all'amministratore. Chiuso in sua assenza.[1].

Descrizione del locale	Si effettua trattamento	Si conservano i dati	Vi si trovano sistemi di elaborazione	ID1	ID2	ID3	ID4	Aperto al pubblico \ presidiato	Accesso consentito al pubblico solo accompagnato	Accesso riservato agli incaricati	Note
Ufficio Amministrativo	X	X	X	X	X					X	Vi si trovano due **armadi con serratura**, due **cassettiere** dotate di serratura, quattro pc. Il locale è sempre presidiato durante le ore di lavoro[2].

Descrizione del locale	Si effettua trattamento	Si conservano i dati	Vi si trovano sistemi di elaborazione	ID1	ID2	ID3	ID4	Aperto al pubblico \ presidiato	Accesso consentito al pubblico solo accompagnato	Accesso riservato agli incaricati	Note
Ufficio Logistica									X		Vi si trovano due **armadi con serratura**, due **cassettiere** dotate di serratura, sei pc di cui uno funge da server. Il locale è sempre presidiato durante le ore di lavoro[3].

[1] Qualora l'operatore che deve presidiare il locale sia assente, il locale viene tenuto chiuso a chiave
[2] Qualora l'operatore che deve presidiare il locale sia assente, il locale viene tenuto chiuso a chiave
[3] Qualora l'operatore che deve presidiare il locale sia assente, il locale viene tenuto chiuso a chiave

Descrizione del locale	Si effettua trattamento	Si conservano i dati	Vi si trovano sistemi di elaborazione	ID1	ID2	ID3	ID4	Aperto al pubblico \ presidiato	Accesso consentito al pubblico solo accompagnato	Accesso riservato agli incaricati	Note
Archivio									X		Vi si trovano **armadi con serratura ed armadi aperti**. Il locale non è accessibile a personale diverso da quello autorizzato (cartello "Vietato l'ingresso").

6. Gli strumenti elettronici

Per strumenti elettronici si intendono gli elaboratori, i programmi per elaboratori o qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento o che concorre alla sicurezza dei dati.
L'elenco dei computer e dei server fisici è fornito di seguito nella tabella 6.1.1.
L'elenco degli altri strumenti elettronici è fornito nella tabella 6.1.2.
L'elenco dei software è fornito nella tabella 6.1.3.

Tabella 6.1.1 *Inventario dei computer e dei server fisici*

Ubicazione (locale)	Dominio	Nome computer	Indirizzo IP	Marca e modello	Sistema Operativo	Impiego (Terminale o Server)	Accesso alla rete interna	Accesso alla rete internet[1] (SI, NO, Controllato)	Sistema di protezione all'accesso[2]	Antivirus installato	Dispositivi di memorizzazione	Dispositivi di collegamento		Dispositivi di backup[3]	UPS
												Scheda LAN	Scheda WiFi[4]		
Uff logistica	X	PC02	5.158.71.165	HP Pro 3520	Windows 10 Home	Terminale	Si	Si	No	Windows defender	Nas Rete - Atlantis	Si	No	Si	No
Uff logistica	X	PC01	5.158.71.165	Lenovo	Windows 8.1	Terminale	Si	Si	No	Windows defender	Nas Rete - Atlantis	Si	No	Si	No
Uff logistica	X	PC05	5.158.71.165	MSI	Windows 10 home	Terminale	Si	Si	No	Windows defender	Nas Rete- Atlantis	Si	No	Si	No
Direzione	X	Desktop – 12DUBEU	5.158.71.165	MSI	Windows 10 pro	Terminale	Si	Si	No	Windows defender	Nas Rete - Atlantis	Si	No	Si	No
Uff amministrativo	X	PC03	5.158.71.165	Lenovo	Windows 8	Terminale	Si	Si	No	Windows defender	Nas Rete - Atlantis	Si	No	Si	Si
Uff amministrativo	X	PC04	5.158.71.165	Lenovo	Windows 8.1	Terminale	Si	Si	No	Windows defender	Nas Rete - Atlantis	Si	No	Si	Si
Uff logistica	X	Serversra	5.158.71.165	Fujitsu Primergy	Windows server 2012 TX 10053	Server	Si	No	Si	Windows defender	Nas Rete - Atlantis	Si	No	No	Si
Uff amministrativo	X	Desktop – p92kjel	5.158.71.165	MSI	Windows 10	Terminale	Si	Si	No	Windows defender	Nas Rete - Atlantis	Si	No	Si	No
Uff amministrativo	X	Desktop – u8pum1r	5.158.71.165	Lenovo	Windows 10	Terminale	Si	Si	No	Windows defender	Nas Rete - Atlantis	Si	No	Si	No

[1] I computer connessi costantemente alla rete internet sono contrassegnati con il "SI"; quelli dai quali è possibile accedere alla rete internet attraverso un processo di autenticazione attraverso il firewall –riservato solo ad alcuni utenti- sono contrassegnati con il "C" (controllato)

[2] Le password di autenticazione al dominio aziendale sono definite autonomamente dagli operatori che però devono rispettare i requisiti di complessità esplicitati di seguito nel documento; per i computer o i server non connessi al dominio, sono state definite delle password in possesso del solo amministratore di rete

[3] I dispositivi di backup locale elencati sono utilizzati solo da un apparato (HPNL401); il backup viene gestito centralmente

[4] Le schede WiFi presenti sono al momento disattivate su tutti i client

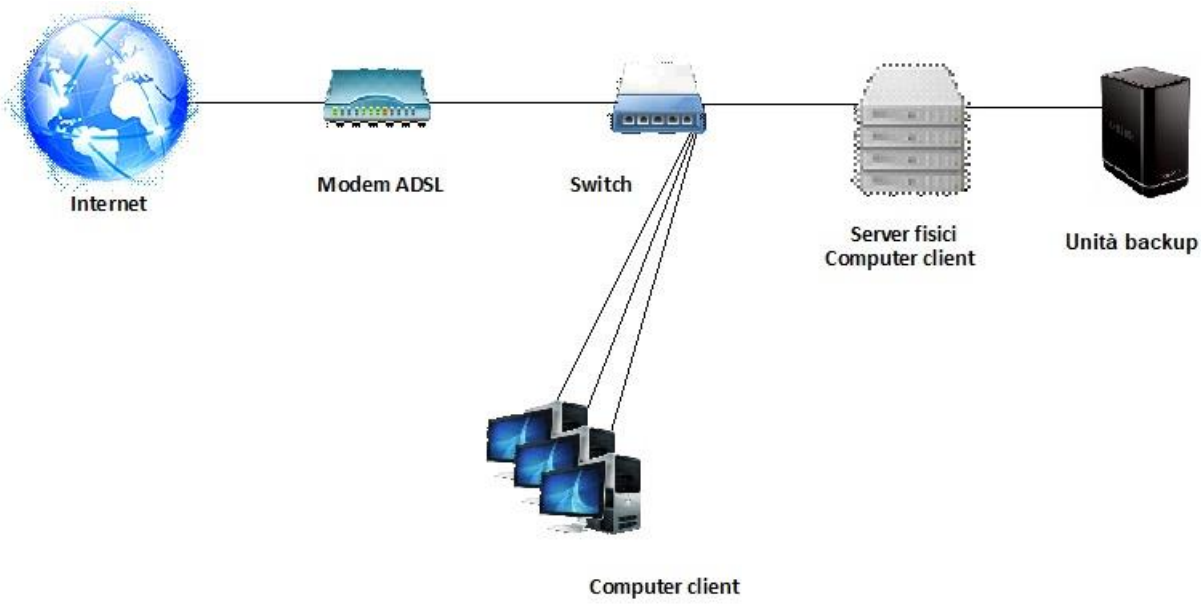
Tabella 6.1.2 *Inventario dei dispositivi elettronici*

Descrizione, marca, modello	Ubicazione	Note descrittive
E - Vision	Ufficio logistica	Sistema video sorveglianza
Atlantis - Rete Nas	Ufficio logistica	Server di rete fisico
Reuter board MIKROTIC mod HEX	Ufficio logistica	Consente di usufruire della linea ADSL; è collegato al firewall attraverso il quale transita tutto il traffico da e verso l'esterno
Firewall ZTE Home Gateway	Ufficio logistica	Firewall

Tabella 6.1.3 *Inventario del software*

Descrizione	Nr. licenze	Periodicità aggiornamento	Tipo di aggiornamento
Win Waste	4	Su segnalazione sistema	On line
MyCDR -Microambiente	1		

Tabella 6.1.4 *Schema della rete interna*



7. Le modalità di trattamento, l'analisi dei rischi e le procedure di sicurezza

I dati sono contenuti all'interno di documenti cartacei oppure all'interno di file, database o e-mail.
Ne consegue che il loro trattamento avviene sia fisicamente sia virtualmente con l'utilizzo di strumenti elettronici.
Nel prosieguo del capitolo si analizzerà ciascuna modalità di trattamento dei dati per individuare i rischi incombenti su di essi e le iniziative attuate per annullarli o ridurli.

7.1. Il trattamento dei dati senza l'ausilio di strumenti elettronici

Il trattamento dei dati senza l'ausilio di strumenti elettronici avviene quando le informazioni sono contenute in documenti cartacei che sono ricevuti dall'esterno oppure sono prodotti durante l'attività lavorativa.
Sui dati trattati in maniera cartacea incombono dei rischi:

- distruzione
- diffusione incontrollata (includente anche la fattispecie dell'errata comunicazione)
- accesso non autorizzato

Tali rischi sono classificabili in funzione dell'evento che li determina:

- comportamento degli operatori
- eventi relativi alle attrezzature
- eventi relativi al contesto

Ogni rischio ha un diverso impatto sulla sicurezza dei dati nel caso si realizzi:

- bassissimo
- basso
- medio
- alto

Nella tabella seguente son analizzati i rischi in relazione ai parametri presentati:

Tabella 7.1.1 *Analisi dei rischi nel trattamento dei dati senza strumenti elettronici*

Rischio	Fattori determinanti			Impatto sulla sicurezza				Esito		
	Comportamento dell'operatore	Evento relativo alle attrezzature	Eventi relativi al contesto	Bassissimo	Basso	Medio	Alto	Distruzione	Diffusione incontrollata	Accesso non autorizzato
Errore materiale	**X**				**X**			**X**	**X**	**X**

Rischio	Fattori determinanti			Impatto sulla sicurezza				Esito		
	Comportamento dell'operatore	Evento relativo alle attrezzature	Eventi relativi al contesto	Bassissimo	Basso	Medio	Alto	Distruzione	Diffusione incontrollata	Accesso non autorizzato
Comportamenti sleali e fraudolenti	X					X		X	X	
Carenza di consapevolezza, disattenzione e incuria	X				X			X	X	
Malfunzionamento, indisponibilità o degrado degli strumenti		X				X		X		X
Errori umani nella gestione della sicurezza fisica	X		X		X				X	X
Ingressi non autorizzati a locali/aree ad accesso ristretto			X			X			X	X
Guasti a sistemi complementari (impianto elettrico, impianto idraulico, climatizzazione, ecc)			X		X			X		
Eventi distruttivi, naturali o artificiali (incendi, allagamenti, scariche atmosferiche) dovuti a dolo, a incuria oppure accidentali			X		X			X		

Per contenere e contrastare i fattori di rischio incombenti sui dati trattati senza l'ausilio di strumenti informatici, l'***Organizzazione*** ha posto in essere delle azioni, descritte nei paragrafi che seguono.

7.1.1. Ambito del comportamento: istruzioni agli incaricati e formazione continua

Gli **Incaricati del trattamento dei dati** vengono formati, durante appositi eventi, sui corretti comportamenti da tenere per ridurre i rischi.

Sono fornite indicazioni di carattere generale sui rischi incombenti sui dati quando essi sono trattati con strumenti cartacei e sulle misure per contrastarli.
In particolare, viene richiamata l'attenzione a proposito della tenuta della postazione di lavoro: ciascun incaricato, che tratti documenti contenti dati personali o sensibili, deve conservarli sotto la propria responsabilità e, terminate le operazioni, riporli o archiviarli nei contenitori muniti di serratura opportunamente approntati o negli armadi e cassetti presenti nelle stanze presidiate, evitando di lasciarli incustoditi. Ad esempio, nel caso in cui si debbano distribuire a più persone dei documenti contenenti dati (si pensi alle buste paga), è inopportuno lasciarle a disposizione su una scrivania affinché ciascuno prelevi la propria perché i destinatari potrebbero venire a conoscenza di dati non di loro pertinenza. Lo stesso può accadere alla rubrica telefonica che, dopo l'uso, deve essere chiusa e non lasciata aperta. Maggiore attenzione a questa tipologia di comportamenti va posta negli ambienti della struttura aperti al pubblico (uffici 1, 2 e 4). Gli incaricati che operano in queste stanze devono tenere i documenti contenenti dati personali sul piano di lavoro per il tempo necessario ad operare, curando di riporli non appena terminato il compito oppure nel caso in cui acceda alla stanza l'utenza.
È fatto divieto a chiunque di:

- effettuare copie fotostatiche di stampe, elenchi, tabulati, rubriche o ogni altro documento che contenga dati oggetto del trattamento;
- trascrivere e diffondere dati contenuti in documenti;
- cancellare dati oppure distruggere documenti;
- consegnare documenti a persone non autorizzate oppure diffonderli in maniera inconsulta o incontrollata;
- portare documenti al di fuori della struttura;
- comunicare verbalmente a soggetti non autorizzati il contenuto di documenti prodotti o acquisiti.

Le azioni elencate sopra possono essere autorizzate dal **Responsabile del trattamento dei dati** in caso di comprovata necessità.
Qualora sia necessario eliminare un documento contenente dati (ad esempio in seguito ad una stampa errata), esso va cestinato. In nessun caso va riutilizzato oppure conservato in luogo non sicuro per essere poi riutilizzato in un secondo momento.
Al fine di assicurare costante attenzione da parte degli incaricati, viene effettuata formazione continua con cadenza annuale (vedi Piano della Formazione Aziendale) oppure in caso di necessità (nomina di nuovo incaricato, cambio di mansioni, modifica delle procedure, reclami o segnalazioni, ecc.).
I contenuti di questi eventi formativi sono riversati nella *Guida pratica per l'Incaricato del trattamento dei dati personali*: essa è allegata al presente documento, viene costantemente aggiornata e viene diffusa agli incaricati in forma cartacea oppure attraverso il sito interno.

7.1.2. Ambito delle attrezzature: predisposizione di armadi \ classificatori \ cassettiere e sale archivio dotate di serratura

Al fine di attuare gli interventi previsti nel precedente paragrafo, sono stati approntati nella struttura degli idonei contenitori (armadi, classificatori, cassettiere) e dei locali archivio nei quali conservare i documenti contenenti dati personali: l'elenco di tali archivi è disponibile al capitolo 4 ed essi sono gli unici contenitori nei quali è possibile conservare documenti contenenti dati personali.
Durante le ore di apertura, nelle quali gli uffici 1, 2 e 4 sono presidiate dagli operatori, gli armadi ed i classificatori restano aperti per consentire una agevole operatività. Durante le ore di chiusura

oppure quando le stanze non sono presidiate, essi restano chiusi. Le stesse stanze vengono mantenute chiuse quando gli assegnatari sono assenti.
Tutte le chiavi degli armadi e dei classificatori nonché dei locali archivi sono riposte all'interno di due cassette portachiavi a sua volta protette da serratura. Le chiavi di esse sono in possesso dei seguenti operatori:

- Antonio Cancro
- Rossella Cerullo
- Carmela Padovani
- Francesca Mansione
- Ciro Donnarumma
- Benedetto Sica
- Gianluca Santimoni

Al termine dell'orario di lavoro, ciascun operatore deve riporre i documenti contenenti dati personali negli appositi vani dotati di serratura, chiuderli a chiave e riporre la chiave nella cassetta portachiavi oppure portarla con sé (ove previsto). In nessun caso documenti contenenti dati personali devono essere lasciati sulle scrivanie oppure in vani non chiusi a chiave in assenza dell'**Incaricato** che ne è responsabile.

7.1.3. Ambito della struttura: organizzazione degli spazi e programmazione della manutenzione

La struttura è dotata di porte interne che separano chiaramente le aree aperte al pubblico da quelle alle quali gli Ospiti possono accedere solamente accompagnati da un dipendente.
È presente un cartello che avvisa gli Ospiti di questa limitazione, sulla porta che divide la sala di attesa dal corridoio.
La struttura è dotata di un piano di emergenza che comprende la presenza di estintori che vengono manutenuti periodicamente a norma di legge.
Inoltre, l'impianto elettrico è dotato di misure salvavita (qualità dei materiali impiegati, quadri elettrici dotati di interruttori differenziali, adeguata sezione dei cavi elettrici, ecc.) atte ad evitare cortocircuiti e possibili incendi.
Infine, tutti i documenti cartacei sono conservati in posizione rialzata dal pavimento in modo che un eventuale allagamento non li danneggi. L'impianto idraulico è dotato di chiavi di arresto per affrontare una emergenza dovuta ad un danno delle condutture.
La manutenzione periodica di attrezzature ed impianti viene monitorata attraverso il "Piano della Manutenzione".

7.2. Il trattamento dei dati con l'ausilio di strumenti elettronici

Il trattamento dei dati con l'ausilio di strumenti elettronici avviene quando le informazioni sono contenute all'interno di file oppure di database, ospitati all'interno di singoli pc oppure di server, e sono elaborate utilizzando tali strumenti.
Sui dati trattati in maniera informatica incombono dei rischi:

- cancellazione (colposa o dolosa)
- diffusione incontrollata (colposa o dolosa)
- accesso non autorizzato

Tali rischi sono classificabili in funzione dell'evento che li determina:

- comportamento degli operatori (volontari o inconsulti)
- attacchi provenienti dall'esterno
- presenza di virus informatici
- eventi relativi alle attrezzature
- eventi relativi al contesto

Ogni rischio ha un diverso impatto sulla sicurezza:

- bassissimo
- basso
- medio
- alto

Nella tabella seguente son analizzati i rischi in relazione ai parametri presentati:

Tabella 7.2.1 *Analisi dei rischi nel trattamento dei dati con l'utilizzo di strumenti elettronici*

Rischio	Fattori determinanti					Impatto sulla sicurezza				Esito		
	Comportamento dell'operatore	Attacchi provenienti dall'esterno	Presenza di virus informatici	Evento relativo alle attrezzature	Eventi relativi al contesto	Bassissimo	Basso	Medio	Alto	Cancellazione	Diffusione incontrollata	Accesso non autorizzato
Sottrazione di credenziali di autenticazione	X	X	X					X				X
Carenza di consapevolezza, disattenzione e incuria	X						X			X	X	
Comportamenti sleali e fraudolenti	X						X			X	X	X
Errore materiale	X						X			X	X	
Azione di virus informatici o di programmi suscettibili di creare danno	X	X	X					X		X		X
Spamming e tecniche di sabotaggio		X	X			X				X	X	X
Malfunzionamento, indisponibilità o degrado degli strumenti				X			X			X		
Intercettazione di informazioni attraverso la rete		X	X	X			X				X	X
Ingressi non autorizzati a locali/aree ad accesso ristretto					X	X						X

Rischio	Fattori determinanti					Impatto sulla sicurezza				Esito		
	Comportamento dell'operatore	Attacchi provenienti dall'esterno	Presenza di virus informatici	Evento relativo alle attrezzature	Eventi relativi al contesto	Bassissimo	Basso	Medio	Alto	Cancellazione	Diffusione incontrollata	Accesso non autorizzato
Sottrazione di strumenti contenenti dati					**X**		**X**				**X**	**X**
Eventi distruttivi, naturali o artificiali (incendi, allagamenti, scariche atmosferiche) dovuti a dolo o a incuria oppure accidentali					**X**		**X**			**X**		
Errori umani nella gestione della sicurezza fisica					**X**		**X**			**X**	**X**	**X**
Guasti a sistemi complementari (impianto elettrico, climatizzazione, ecc)					**X**		**X**			**X**		

Per contrastare i rischi incombenti sui dati trattati con l'ausilio di strumenti informatici, L'Organizzazione ha predisposto le misure di sicurezza illustrate nei paragrafi seguenti e che spaziano negli ambiti del comportamento degli operatori, nella predisposizione di una infrastruttura informatica hardware\software adeguata, nell'approntamento di opportuni spazi all'interno della struttura.

7.2.1. Istruzioni agli incaricati della gestione e manutenzione degli strumenti elettronici

Il **Responsabile del Trattamento dei dati,** ovvero il **Titolare,** forma gli **Incaricati della gestione e manutenzione degli strumenti elettronici** fissando gli obiettivi di sicurezza da raggiungere.
Gli Incaricati adottano le misure tecniche atte al loro raggiungimento attraverso il confronto costante con il **Responsabile del trattamento dei dati**.
Tutti i server ed i computer messi in esercizio devono essere dotati di una password a protezione dell'accesso alle impostazioni del BIOS. Tale password è conosciuta solo dagli Incaricati.
Riguardo agli altri apparati managed (switch, firewall), viene adottata una password diversa da quella standard, conosciuta solo dall'Incaricato della gestione e manutenzione degli strumenti elettronici.
Prima della messa in esercizio, vengono aggiornati tutti i firmware, i sistemi operativi ed i driver delle periferiche.

Si procede ad installare solamente software originale, dotato di regolare licenza ovvero software di libero utilizzo in ambiente commerciale, prelevandolo da supporti originali oppure dai siti dei produttori. Al termine della prima installazione, si provvede ad aggiornare tutti i software e ad attivare eventuali programmi di aggiornamento automatico periodico.
Il software da installare viene selezionato in accordo con il **Responsabile del trattamento dei dati** e deve essere attinente alle attività e alle esigenze aziendali.
Si procede ad assegnare ad un server le funzioni di Controller di Dominio e a renderne membri tutti i computer client; si creano le utenze per gli **Incaricati del trattamento dei dati** e si definisce il sistema di autorizzazione per ciascun ambito fissando i permessi di accesso, lettura, scrittura, modifica e cancellazione secondo quanto comunicato dal **Responsabile del trattamento dei dati**.
Si determinano le Policy di sicurezza ritenute opportune per salvaguardare la sicurezza e si annotano nel *Documento dell'Incaricato della gestione e manutenzione degli strumenti elettronici*.
Le credenziali di Amministratore locale del server e quelle di Amministratore di Dominio sono conosciute solo dagli **Incaricati della gestione e manutenzione degli strumenti elettronici**.
I client sono configurati settando una password per l'account di amministratore locale, conosciuta solo dagli **Incaricati della gestione e manutenzione degli strumenti elettronici**.
Essi son poi uniti al dominio utilizzando le credenziali di Amministratore di Dominio.
Il firewall viene configurato con policy atte a contrastare tentativi di intrusioni.

7.2.2. Istruzioni agli incaricati e formazione continua

Gli Incaricati dell'***Organizzazione*** vengono formati, durante appositi eventi, sui corretti comportamenti da tenere per ridurre i rischi.
Sono fornite indicazioni di carattere generale sui rischi incombenti sui dati, quando essi sono trattati con strumenti elettronici, e sulle misure da adottare per la loro tutela in particolare a proposito della tenuta della postazione di lavoro, laddove essa comprenda un computer, e delle credenziali informatiche. A seconda dell'esperienza e delle conoscenze dell'incaricato in formazione, si procede ad erogare formazione aggiuntiva.
L'incaricato utilizza, per il trattamento dei dati, i computer messi a disposizione dall'***Organizzazione***; è vietato collegare un computer proveniente dall'esterno alla rete aziendale.
In ogni caso, è impossibile accedere ai file memorizzati nei server se non si è in possesso delle opportune credenziali; senza esse non è neanche possibile fruire dei servizi aggiuntivi della rete interna (ad esempio dell'accesso ad internet, dell'accesso al sito interno oppure del backup dei dati).

L'**Incaricato al trattamento dei dati** è tenuto a non lasciare incustodito il computer durante il suo funzionamento; malgrado sia installata una policy di sicurezza che, trascorsi 10 minuti di inattività, fa entrare in funzione il salvaschermo e attiva la protezione dell'accesso con password, è preferibile che l'Incaricato attivi autonomamente il salvaschermo nel caso debba temporaneamente allontanarsi dalla postazione (questa operazione può essere avviata premendo contemporaneamente il tasto con il simbolo di Windows e la lettera "L"). Qualora la sua assenza debba prolungarsi per un tempo maggiore, egli deve procedere alla disconnessione dell'account dal sistema operativo mentre, al termine dell'orario di lavoro, deve effettuare lo spegnimento del computer. Questa operazione è necessaria anche per completare l'installazione di eventuali patch che sono installate automaticamente.
L'Incaricato è tenuto a non lasciare in alcun caso il controllo del computer, nel quale ha inserito le proprie credenziali, ad alcuno, anche se si tratta di un altro Incaricato. In questa evenienza, è

necessario prima disconnettere l'utente e poi consentire all'altro incaricato di inserire le proprie credenziali.
È fatto divieto agli Incaricati di:

- effettuare copie di dati su supporti rimovibili (CD, DVD, penne USB) oppure trasmissioni di dati non autorizzate;
- effettuare stampe non autorizzate di elenchi, tabulati, rubriche o qualsiasi altro dato e\o consegnarle a persone non autorizzate;
- cancellare dati senza l'autorizzazione del **Responsabile del trattamento dei dati**;
- inserire nel client supporti rimovibili contenenti programmi non originali oppure file potenzialmente dannosi;
- smontare computer o altri apparati elettronici;
- trascrivere da video e poi diffondere dati;
- salvare file in directory diverse da desktop, documenti, unità Y (cartella personale sul server);
- comunicare verbalmente a soggetti non autorizzati il contenuto di documenti elettronici.

Al fine di assicurare costante attenzione da parte degli incaricati, viene effettuata formazione continua con cadenza annuale (vedi il Piano di Formazione Aziendale) oppure in caso di necessità (nomina di nuovo incaricato, cambio di mansioni, modifica delle procedure o del software o dell'hardware, reclami o segnalazioni, ecc).
I contenuti di questi eventi formativi sono riversati nella *Guida pratica per l'incaricato del trattamento dei dati personali*: essa è parte integrante del presente documento, viene aggiornata annualmente e viene diffusa agli incaricati in forma cartacea oppure attraverso il sito interno.

7.2.3. Il sistema hardware

Il sistema informatico è formato da un Personal Computer (posizionato nell'Ufficio 1) che funge anche da server, dagli apparati di rete e dai computer client.
L'unico programma condiviso, del quale vengono fatte le copie di backup, è il WinWast.
Due dei computer client sono posizionati nell'Ufficio 2, ed uno nell'Ufficio 4. Una loro asportazione non produrrebbe danni agli archivi informatici relativi al WinWast in quanto i dati risiedono fisicamente nel server oltre che nei supporti di backup.
L'impianto elettrico è dotato di misure salvavita (qualità dei materiali impiegati, quadri elettrici dotati di interruttori differenziali, adeguata sezione dei cavi elettrici, ecc.) atte ad evitare cortocircuiti che potrebbero mettere a rischio gli apparati.
I server, gli apparati di rete e tutti i pc sono collegati a gruppi di continuità opportunamente dimensionati per proteggere gli apparati da sbalzi di tensione e per supplire ad una interruzione nell'erogazione dell'energia elettrica per un tempo sufficiente ad effettuare uno spegnimento programmato del sistema operativo.
Nel caso in cui si renda necessaria la dismissione del server, di un computer oppure di un singolo hard disk, è necessario assicurare la completa cancellazione del disco rigido per evitare una possibile diffusione incontrollata di dati. Essa può essere ottenuta attraverso l'utilizzo di una utility di libero utilizzo (come ad esempio WipeDisk) che procede a scrivere più volte sui settori del disco zeri oppure numeri casuali e a successive cancellazioni secondo protocolli di sicurezza validati internazionalmente. In alternativa, è necessario procedere alla distruzione dell'hard disk, fisica oppure elettromagnetica.

7.2.4. Il sistema software

L'installazione di software all'interno del server o di un pc client è permessa solamente agli Amministratori di dominio; agli Utenti è negata la possibilità di effettuare installazioni o disinstallazioni e di variare alcuni parametri di funzionamento (ad esempio il salvaschermo, l'accesso con password, le impostazioni di rete) reputati fondamentali per la sicurezza e fissati attraverso le policy centralizzate.
Sul server ed i computer è presente un software antivirus che provvede alla protezione in tempo reale e che è programmato per effettuare scansioni periodiche del sistema e per aggiornare automaticamente le definizioni dei virus scaricandole da internet sul server principale e poi da esso sui computer client. Il sistema antivirus è dotato di una console di gestione centralizzata, installata su un server, e di un agente e di un client installati automaticamente su ciascun computer che viene aggiunto al dominio.
Poiché la quasi totalità dei sistemi operativi e dei software di produttività è prodotta dalla Microsoft, sui pc è installato il servizio di distribuzione automatica degli aggiornamenti. Esso scarica quotidianamente e approva automaticamente gli aggiornamenti critici e che riguardano la protezione e la sicurezza mentre è compito dell'Incaricato della gestione e manutenzione degli strumenti elettronici approvare l'installazione di aggiornamenti che hanno diversa natura (ad esempio, introduzione di nuove funzionalità).

7.2.4.1. Il monitoraggio degli accessi degli amministratori di sistema al sistema informatico

L'amministratore di sistema è la figura che detiene le più alte credenziali per l'accesso agli apparati informatici.
La normativa vigente prevede che il **Titolare del trattamento dei dati** debba avere la possibilità di supervisionare l'operato dell'amministratore di Sistema.
Tale previsione è – comprensibilmente - di difficile attuazione in quanto, spesso, al Titolare mancano le competenze tecniche per verificare l'attività di una figura specializzata; in caso contrario, non avrebbe avuto la necessità di effettuare tale nomina.
Inoltre, per definizione, l'amministratore di sistema, dotato delle credenziali apicali, è in grado di disattivare o eludere qualsiasi sistema di controllo.
Nella ***SRA SRL***, le figure del Titolare e dell'amministratore di sistema coincidono.

7.2.5. Sistema di autenticazione informatica

Gli **Incaricati** possono accedere al trattamento dei dati utilizzando strumenti elettronici unicamente dopo aver superato una procedura di autenticazione attraverso l'utilizzo di idonee credenziali. Le credenziali informatiche sono formate da un nome utente e da una password.
Il primo viene assegnato personalmente al singolo **Incaricato del trattamento dei dati** e non varierà mai; esso è un codice univoco e pertanto non ne esistono due uguali né il codice associato verrà assegnato ad un altro soggetto, anche in caso di revoca della nomina ad Incaricato del proprietario.
La password che viene consegnata assieme al nome utente è temporanea: l'Incaricato deve modificarla al primo accesso e, successivamente, ogni 90 giorni seguendo le prescrizioni del paragrafo 6.2.2.1, comunicate con una lettera di istruzioni.
In caso di dimenticanza o di smarrimento oppure se si ritenga possibile una sottrazione delle credenziali, è necessario rivolgersi immediatamente al Responsabile del Trattamento dei dati personali affinché provveda, attraverso l'Incaricato della manutenzione dei sistemi informatici, ad azzerare la password bloccando, di fatto, un utilizzo fraudolento di quelle credenziali.

Quando la nomina ad incaricato viene revocata, l'account viene disattivato rendendo impossibile l'accesso al sistema informatico. Nel caso in cui all'**Incaricato** siano assegnati compiti diversi che rendano necessario l'accesso ad altri dati, le autorizzazioni associate al suo account sono modificate di conseguenza.
L'incaricato deve adottare tutte le necessarie cautele per assicurare che la parola chiave resti segreta e unicamente conosciuta da egli stesso. È fatto espresso divieto di comunicarla a chiunque altro, anche se egli sia un **Incaricato** oppure un **Responsabile**.

7.2.5.1. Istruzioni per la scelta della password e la sua protezione

Gli **Incaricati del trattamento dei dati** scelgono la propria parola chiave autonomamente per assicurare che essa sia conosciuta solo ed unicamente da loro.
La password deve però rispettare dei requisiti minimi di complessità: istruzioni in merito sono comunicate agli incaricati dal **Responsabile del trattamento dei dati** mediante la consegna della *Guida pratica per l'incaricato del trattamento dei dati personali* e mediante la formazione periodica.
La scelta della password è una delle operazioni più importanti nel settore della sicurezza informatica. Questo strumento deve difendere e proteggere, in modo inequivocabile i dati personali e sensibili memorizzati negli archivi informatici aziendali.
Forzare una password può essere complicato ma non impossibile. Un malintenzionato esperto ha diversi sistemi a disposizione per individuare una password. In pratica, comunque, i modi per tentare di trovare le parole chiave sono sostanzialmente due: l'attacco "a forza bruta" (brute-force) (mediante software che tentano di risalire ad una password provando tutte le combinazioni possibili) e l'attacco cosiddetto "a dizionario" (mediante un elenco di termini utilizzati più frequentemente).
Si intuisce immediatamente che una password casuale composta da una sequenza di numeri e lettere, meglio se minuscole e maiuscole, è più difficile da intercettare rispetto a parole di senso compiuto.
La lunghezza della password deve essere di almeno 8 caratteri.
Deve contenere caratteri di almeno tre delle quattro categorie seguenti:

- Lettere maiuscole (A–Z)
- Lettere minuscole (a–z)
- Numeri (0-9)
- Caratteri non alfanumerici (ad esempio !, $, #, %)

Non deve contenere, per intero o in parte, il nome dell'account utente o dell'utente stesso.
Uno degli errori che potrebbe minare la sicurezza è quello di impostare una password con la data di nascita, con la targa dell'auto o, peggio ancora, con il numero del cellulare.
Occorre evitare di inserire una serie di numeri o caratteri ripetuti ("1234567890", "1111111111", "ABCDEFGHIL") oppure password composte da lettere poste tra loro vicine sulla tastiera (come "qwertyuiop" o " asdfghjkl").
Per proteggere la password, è opportuno non trascriverla su documenti cartacei. Nel caso sia necessario, questi documenti andrebbero conservati opportunamente. Nel caso venga salvata nella memoria del proprio telefono cellulare, esso andrebbe protetto con un PIN o un altro sistema di blocco. È vietato trascrivere la password su post-it o foglietti da lasciare nei pressi del computer o addirittura incollati ad esso.

7.2.6. Il backup e il ripristino dei dati

Il backup è l'operazione attraverso la quale i dati sono copiati in una locazione diversa e separata da quella originaria.
Tale processo ha la finalità di salvaguardare i dati sia in caso di guasto degli apparati o di loro sottrazione sia in caso di cancellazione (accidentale o non), permettendone il ripristino alla data dell'esecuzione della copia.
Innanzitutto, è necessario individuare i dati da sottoporre a backup e fissare la periodicità dello stesso. Le operazioni devono essere automatizzate in massima parte per evitare dimenticanze, errori o omissioni.
Nel caso si utilizzino dei supporti rimovibili, essi vanno custoditi all'interno di mobili muniti di chiave. È prescritto assoluto divieto agli incaricati di conservare in luogo diverso supporti rimovibili che contengano o abbiano contenuto dati.
Nel caso in cui si adottino dei supporti rimovibili di tipo riscrivibile, è necessario che, prima di ciascun utilizzo, essi siano formattati. Nel caso si renda necessaria la loro dismissione, bisogna procedere, come per gli hard disk, alla loro cancellazione con modalità validate ovvero alla loro distruzione fisica oppure elettromagnetica.
La decisione di ripristinare dei dati è assunta unicamente dal **Responsabile del trattamento dei dati**. Prima di effettuarla, egli deve rimuovere le cause che hanno provocato la cancellazione o il danneggiamento dei dati, avvalendosi della collaborazione tecnica dell'**Incaricato della gestione e manutenzione degli strumenti elettronici**. Ove possibile, deve essere effettuato un ripristino dei soli dati compromessi/cancellati per evitare di sostituire con copie antecedenti dei file che sono stati modificati e che non risultano compromessi in alcun modo.
Successivamente l'**Incaricato della gestione e manutenzione degli strumenti elettronici**, con il supporto dell'**Incaricato delle copie di sicurezza delle banche dati**, procede al ripristino dei dati.
L'**Incaricato delle copie di sicurezza delle banche dati** annualmente procede alla verifica delle procedure di ripristino: simula la perdita dei dati e, seguendo le istruzioni ricevute, si accerta che il ripristino avvenga in maniera completa.

7.2.6.1. Istruzioni di copia

Le istruzioni di copia, nel caso della ***SRA SRL***, non risultano necessarie, in quanto l'**Incaricato delle copie di sicurezza** ben conosce il software WInWast.
I dati sono attualmente salvati con frequenza settimanale su supporto esterno custodito a cura dell'**Incaricato delle copie di sicurezza**.
Di seguito si elencano, nelle apposite tabelle, le operazioni di salvataggio dei dati e le frequenze.

Tabella 7.2.2 – Backup effettuati

Origine	Destinazione	Frequenza
Database WinWast installato sul server (pc Ufficio 1)	E:\backup	Ogni settimana

7.2.7. Istruzioni di ripristino

Le istruzioni di ripristino, nel caso della ***SRA SRL***, non risultano necessarie, in quanto l'**Incaricato delle copie di sicurezza** ben conosce il software WInWast.
Il ripristino dei dati a partire dalle copie conservate sul dispositivo esterno prevede che le directory salvate (oppure i singoli file da ripristinare) siano trasferite nelle directory originarie manualmente, utilizzando l'interfaccia del sistema operativo. Nel caso di file illeggibili o compromessi, è opportuno provare a crearne una copia prima di procedere al ripristino.

7.3. Indicazioni generali di comportamento per gli incaricati

Nei paragrafi precedenti sono state esaminate le tipologie di trattamento con gli strumenti cartacei e quelle con gli strumenti elettronici, analizzando le modalità di trattamento, i rischi incombenti sui dati e le opportune contromisure adottate.
È necessario che gli **Incaricati** siano formati anche sui corretti comportamenti da adottare durante le fasi di comunicazione verbale che coinvolgano dati personali.

7.3.1. Comunicazioni in presenza di più persone

Qualora sia necessario comunicare una notizia ad un Ospite in sala di attesa, in presenza di altre persone è opportuno non utilizzare il nome o il cognome della persona. È invece necessario apostrofarlo chiamandolo "signore" oppure "signora". Una volta ottenuta la sua attenzione, è opportuno invitarlo ad accomodarsi in un locale separato per potergli comunicare quanto necessario.

7.3.2. Locali aperti al pubblico

Nei locali aperti agli Ospiti, con esclusione della sala d'attesa, deve accedere un Ospite alla volta. Se al suo interno sono presenti diversi **Incaricati**, coloro tra essi che non sono interessati dal trattamento devono uscire.
È opportuno, inoltre, chiudere la porta del locale durante la comunicazione.

7.3.3. Tono di voce

Durante una comunicazione di dati personali, di persona o telefonica, l'**Incaricato** deve mantenere un tono di voce adeguato. Un tono di voce troppo alto, difatti, potrebbe vanificare la distanza di cortesia o la chiusura delle porte e divulgare dei dati a chi si trova nei pressi.

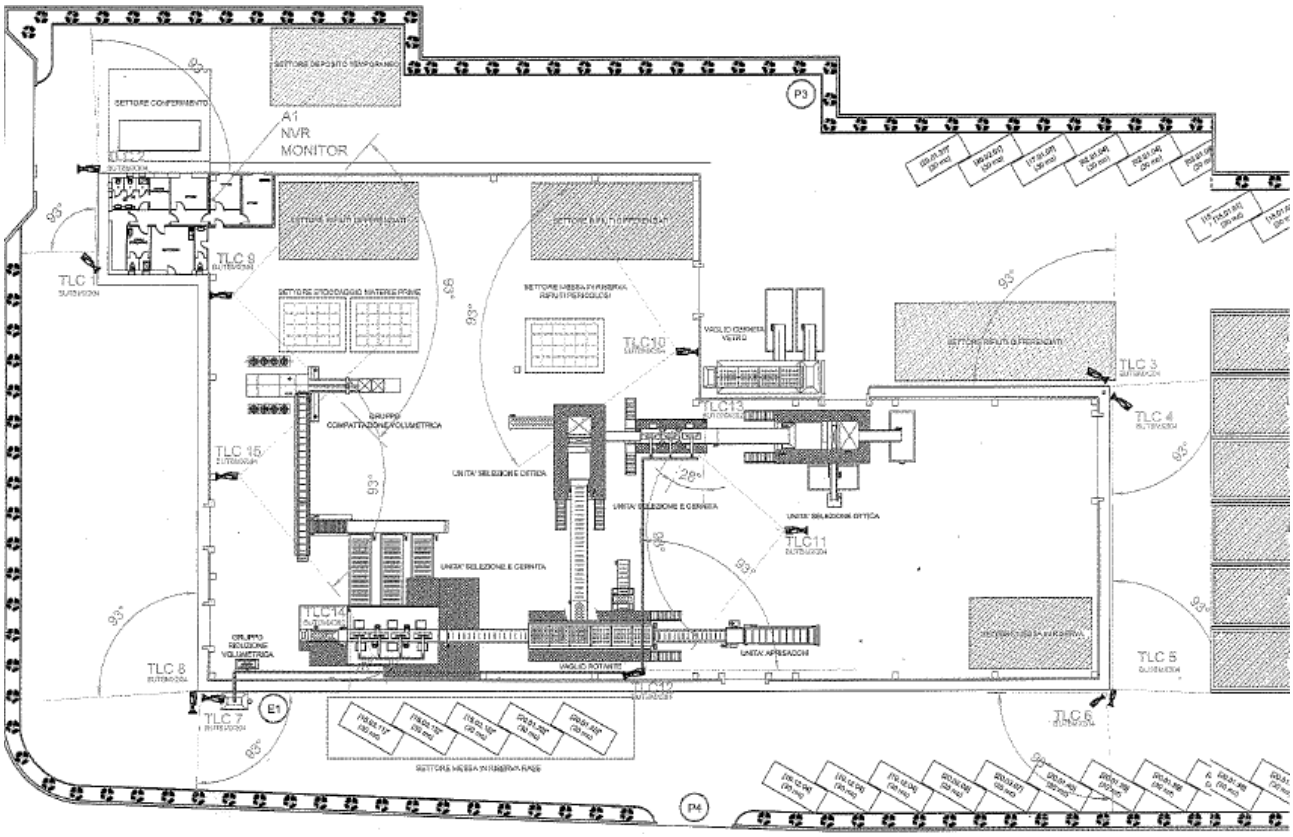
8. Sistema di videosorveglianza

8.1. Motivazioni e finalità dell'installazione dell'impianto

L'impianto di videosorveglianza installato presso la sede sociale ha la finalità di dissuadere e prevenire fenomeni di furto e vandalismo rivolti contro il patrimonio aziendale.
L'impianto produttivo è aperto dalle ore 05:00 alle 23:00 con orari variabili, mentre gli uffici sono aperti dalle 7:00 alle 18:00.
Al di fuori di questi orari, gli ingressi alla struttura sono chiusi e viene attivato l'impianto antifurto interno. Sono inoltre chiusi i due cancelli di accesso ai piazzali prospicienti la struttura.
Il perimetro dell'area è delimitato da una recinzione alta circa 180 cm.
Sono assenti grate alle finestre o alle porte di ingresso.
Queste circostanze, assieme al posizionamento della struttura e all'ampiezza dei piazzali, hanno reso opportuna l'installazione di un impianto di videosorveglianza per le finalità indicate all'inizio del paragrafo. Le immagini raccolte non sono utilizzate per finalità diverse o ulteriori rispetto a queste esigenze e non vengono diffuse o comunicate a terzi.

8.2. Caratteristiche dell'impianto

L'impianto è costituito da nr. 12 videocamere installate all'esterno ed all'interno della struttura, nei punti indicati sulla planimetria riportata di seguito.



È opportuno precisare che nessuna telecamera, come è evidente dalla piantina, è installata all'interno di bagni, spogliatoi, armadietti, stanze di terapia, di visita o di amministrazione; sono invece installate all'interno dei corridoi e della sala di attesa.

Le videocamere sono collegate ad un DVR (Digital Video Recorder, registratore video digitale) installato all'interno del rack che contiene i server aziendali, situato all'interno del locale server al primo piano della struttura e collegato ad un monitor e alla rete intranet.
Il locale è ad accesso limitato.
La presenza delle videocamere è segnalata dagli appositi cartelli affissi all'interno e all'esterno della struttura, nei pressi degli apparati. Sui cartelli sono indicati chi effettua la rilevazione delle immagini e gli scopi per i quali viene effettuata.
All'interno della struttura, in sala di attesa, è invece presente un ulteriore cartello contenente un'informativa per coloro che accedono alla struttura e che riporta:

- le finalità e le modalità del trattamento dei dati registrati;
- soggetti o categorie di soggetti che possono visualizzare i filmati;
- estremi identificativi del titolare e del responsabile del trattamento.

8.3. Modalità di trattamento dei dati

Il sistema di videoregistrazione è programmato per funzionare unicamente nelle ore in cui la struttura non è aperta al pubblico, con la precisa finalità di rispettare le motivazioni che hanno portato all'installazione del suddetto impianto.
Il Provvedimento in materia di videosorveglianza del 8 aprile 2010, emanato dal Garante della Privacy, tratta al punto 3.4 la durata dell'eventuale conservazione ([1]).
La **SRA Srl**, tenendo conto delle finalità della videosorveglianza, e della relativa conservazione, ***dissuadere e prevenire fenomeni di furto e vandalismo rivolti contro il patrimonio aziendale***, al fine di poter rendere disponibili all'Autorità Giudiziaria le immagini registrate dell'evento dannoso, si avvale della possibilità di conservare la registrazione per 72 ore.
Nel caso di chiusura per ferie, la conservazione della registrazione sarà per 144 ore, comunque inferiore alla settimana, indicata da Garante quale tempo limite oltre il quale dover richiedere la Verifica preliminare (si veda punto 3.1 del Provvedimento in materia di videosorveglianza del 8 aprile 2010).
Le immagini sono conservate per 72 ore dopodiché il sistema provvede alla loro sovrascrittura.
Nel caso in cui si rilevino atti vandalici oppure furti, le immagini possono essere visualizzati dalle Forze di Polizia e dall'Autorità giudiziaria.

([1])Nei casi in cui sia stato scelto un sistema che preveda la conservazione delle immagini, in applicazione del principio di proporzionalità (v. art. 11, comma 1, lett. e),del Codice), anche l'eventuale conservazione temporanea dei dati deve essere commisurata al tempo necessario - e predeterminato - a raggiungere la finalità perseguita.
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, sulla scorta anche del tempo massimo legislativamente posto per altri trattamenti, si ritiene non debba comunque superare la settimana.

9. Piano di miglioramento

Il piano di miglioramento delle politiche riguardanti il trattamento e la protezione dei dati è costituito da una serie di azioni che comprendono attività di formazione, acquisti e aggiornamenti delle procedure e del G.D.P.R. stesso al fine di migliorare le misure messe in campo per tutelare il rispetto del trattamento e la protezione dei dati.
Le azioni da implementare sono individuate di seguito e riportate all'interno del Documento del Riesame:

1) Formalizzazione del nuovo Sistema per il trattamento e la tutela dei dati: si procede a convocare una riunione di formazione sul nuovo Sistema; contestualmente si consegnano l'integrazione al mansionario riferita al trattamento e tutela dei dati e la Guida Pratica per l'Incaricato.
2) smaltimento dei documenti cartacei: si procederà ad acquistare un trituratore di documenti per assicurare la distruzione dei documenti cartacei che non si intende conservare; si rinnoverà la formazione degli incaricati sull'utilizzo di tale strumento rimarcando il divieto di distruggere documenti senza autorizzazione.