STUDIO MANDELLI
SICUREZZA SUL LAVORO IGIENE DEGLI ALIMENTI

DOCUMENTO DI VALUTAZIONE DEL RISCHO TRATTAMENTO DEI DATI PERSONALI REGISTRO TRATTAMENTI DATI

Regolamento Europeo 679/2016
Decreto Legislativo 101/2018

Ragione Sociale

CERGAS SRL

Sede legale

Via della Tecnologia 16

STMGDPR 119/A19

Gennaio 2019

REV 01

Studio Mandelli S.r.l.

Sede Legale
Via XX Settembre, 120 - 20025 Legnano (MI)
+39 0331.59.84.44
+39 0331.18.58.088

Centro Formativo
Via Stelvio, 7 - 20025 Legnano (MI)
www.studiomandelli.net
info@studiomandelli.net

Accreditamenti
Iscritto all'Albo della Regione Lombardia
Operatori Accreditati per la Formazione n. 794 del 17/09/2013
(ai sensi della D.G.R. n. 2412 del 26/10/2011 e d.a.)

C.F./P.I. 07338790962 - REA MI1952145 - Capitale Sociale € 30.000,00 i.v.

INDICE

Azienda	Cergas Srl
Sede legale	Via della Tecnologia 16, 20020 Arconate (MI)
Sede Operativa	Cantieri Temporanei e mobili
Titolare del Trattamento	Cergas Srl
Normativa di Riferimento	Regolamento Europeo 679/2016 e D.lgs 101/2018
Attività lavorativa	Costruzione e manutenzione di acquedotti e metanodotti
Codice Atecori 2007	432201 - 432202
Email di contatto	segreteria@cergassrl.it
PEC	legalmail@pec.cergassrl.com

Data documento	13 settembre 2018

Aggiornamento n.	Motivo aggiornamento	Data
1	Decreto Legislativo 101/2018	13 settembre 2018

Titolare trattamento dei dati		Cergas Srl
Responsabile trattamento Dati		Ciapparelli Lara
Incaricati		Ciapparella Osvaldo
		Chiara Baga
		Bertani Giuliana Margaret
		Luciano Albrizio

1.1. DESCRIZIONE DELL'AZIENDA

La società Cergas Srl si occupa di costruzione e manutenzione di acquedotti e metanodotti. Ha una sede operativa sita nel Comune di Arconate dove sono presenti gli uffici amministrativi e il magazzino deposito mezzi. Il lavoro si svolge esternamente in cantieri temporanei e mobili.

RISCHI	DELIBERATO	ACCIDENTALE	AMBIENTALE	MISURE
Terremoto			X	Struttura che rispetta caratteristiche sismiche (vedi zonizzazione sismica DGR 5001/2016).
Inondazione			X	Posizione documenti cartacei ed informatici rialzati dal pavimento. Evitare archivi in cantine o garage facilmente allagabili.
Fulmine			X	Protezione scariche atmosferiche.
Incendio				D.C impianto elettrico, verifica messa a terra e presenza mezzi spegnimento fuoco sia attivi (estintori) che passivi (materiale REI).
Uso di armi	X			
Danno volontario	X			
Interruzione corrente		X		

RISCHI	DELIBERATO	ACCIDENTALE	AMBIENTALE	MISURE
Furto	X			Chiudere i locali a chiave, autorizzazione degli accessi, utilizzo di sistemi di crittografia per i dati. Archivi cartacei in armadi chiusi a chiave. Password di accesso minimo 8 caratteri cambiata trimestralmente.
Errore umano		X		Prevedere un bakcup storico al fine di poter recuperare i dati in caso di cancellazione o trascrizione (insomma ad una perdita) legata ad un errore umano.
Errore umano		X		Non rispetto delle informazioni del paziente, comunicazione delle medesime a terzi non autorizzati.
Accesso non autorizzato alla rete	X			Proteggere la propria connessione. Firewall
Invio non corretto di messaggi	X			Prestare attenzione all'inoltro di mail contenete dati sensibili. Utilizzare PEC o posta crittografata.

1.2. TRATTAMENTO DEI DATI PERSONALI

Per trattamento intendiamo qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insieme di dati personali, 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 e la distruzione.

I dati trattati dal Titolare sono dati personali (di tipo anagrafico) ed appartenenti a categoria di dati particolari (medici, sanitari, religiosi etc).

Il trattamento avviene:

	In modalità cartacea
	In modalità informatica
X	Mista (cartacea ed informatica)

Se si pone una crocetta sulle ultime due modalità di trattamento (informatica e mista) occorre specificare, nel dettaglio le attrezzature informatiche impiegate al fine di poter successivamente individuare le misure di sicurezze già messe in atto o da implementare in relazione alla tipologia di dato trattato e all'entità del rischio valutato.

1.3. ATTREZZATURE INFORMATICHE

Il Titolare del trattamento dati mantiene un elenco, da aggiornare **con cadenza annuale**, di tutte le attrezzature informatiche che utilizza, dello scopo cui sono destinate, della loro allocazione fisica, delle misure di sicurezza su esse adottate e delle eventuali misure di adeguamento pianificate. Le risorse hardware utilizzate per trattare i dati personali sono analizzate nelle seguenti schede riepilogative:

PC GIULIANA	Modello	OPTIPLEX 990 SFF REFURBISHED
	Marca	DELL
	Sistema operativo	WINDOW 10 PRO
	Responsabile Esterno	IQUAD SRL
	Cambio password	TRIMESTRALE
	In rete	SI
	Antivirus	OFFICE 365 ADVANCED THREAT PRO
PC OSVALDO	Modello	OPTIPLEX 990 SFF REFURBISHED
	Marca	DELL
	Sistema operativo	WINDOW 10 PRO
	Responsabile Esterno	IQUAD SRL
	Cambio password	TRIMESTRALE
	In rete	SI
	Antivirus	OFFICE 365 ADVANCED THREAT PRO
PC CHIARA	Modello	HP PRO 400 P/N D5T78EA
	Marca	HEWLETT- PACKARD COMPANY
	Sistema operativo	WINDOW 10 PRO
	Responsabile Esterno	IQUAD SRL
	Cambio password	TRIMESTRALE
	In rete	SI
	Antivirus	OFFICE 365 ADVANCED THREAT PRO
PC LUCIANO	Modello	HP ELITE 8300 REFURBISHED
	Marca	HEWLETT- PACKARD COMPANY
	Sistema operativo	WINDOW 10 PRO
	Responsabile Esterno	IQUAD SRL
	Cambio password	TRIMESTRALE
	In rete	SI
	Antivirus	OFFICE 365 ADVANCED THREAT PRO
PC LARA	Modello	HP PRO 3120 MICROTOWER PC
	Marca	HEWLETT- PACKARD COMPANY
	Sistema operativo	WINDOW 10 PRO
	Responsabile Esterno	IQUAD SRL
	Cambio password	TRIMESTRALE
	In rete	SI
	Antivirus	OFFICE 365 ADVANCED THREAT PRO

Cellulari Aziendali	Nominativo persone	Finalità
	Lara Ciapparella	Reperibilità durante il lavoro
	Osvaldo Ciapparella	
	Luciano Albrizio	
	Giuseppe Bienati	
	Fabio Mansi	
	Carlo Scordamaglia	
	Giuliana Bertani	
	Alessio Scordamaglia	
	Mauro Gatti	
Tablet Aziendali	Marca o modello	Finalità
	Hauwei	Attività lavorative, di controllo
	Apple Ipad	

Locale	X	Chiuso a chiave
	X	Vdeosorvegliato
	X	Presenza di allarme
		Personale
		Condiviso con altri Titolari
	X	Dichiarazione conformità impianto elettrico
	X	Controllo Messa a terra
	X	Mezzi spegnimento attivi del fuoco
Armadi	X	Chiusi a chiave
		Personali
	X	Condivisi con più incaricati
		REI
Carta	X	Presenza di distruggi documenti
		Società di smaltimento con certificazione
		Non vengono distrutti documenti
	X	I fogli vengono sminuzzati finemente da renderli illeggibili

2.0 LE FIGURE DELLA PRIVACY

2.1 Responsabile del Trattamento Dati

L'articolo 4 del Regolamento 679/2016 definisce il "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. L'articolo 28 del Regolamento esplicita che i trattamenti da parte di un Responsabile del trattamento devono essere disciplinati da un contratto o da un altro atto giuridico che vincoli il Responsabile al Titolare del trattamento.

In particolare, il citato contratto, prevede che il Responsabile del trattamento:

- ✓ Tratti i dati personali soltanto su istruzioni documentata del titolare del trattamento
- ✓ Garantisca che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;
- ✓ Adotti tutte le misure di sicurezza e gli adempimenti in materia di privacy previsti dall'articolo 32 del Regolamento;
- ✓ Rispetti le condizioni previste dall'articolo 28 paragrafi 2 e 4 nel caso di ricorso ad un altro Responsabile;
- ✓ Assista il Titolare del Trattamento con misure tecniche organizzative adeguate al fine di soddisfare l'obbligo del Titolare di dare seguito alle richieste per l'esercizio dei diritti dell'interessato.
- ✓ Su scelta del Titolare cancelli o gli restituisca tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento e cancelli le copie esistenti;
- ✓ Metta a disposizione del titolare tutte le informazioni necessarie per dimostrare il rispetto degli obblighi in materia di Privacy e consenta e contribuisca alle attività di revisione, comprese le ispezioni organizzate da parte del Titolare.

2.2.Incaricato – Persona Autorizzata al trattamento dei dati

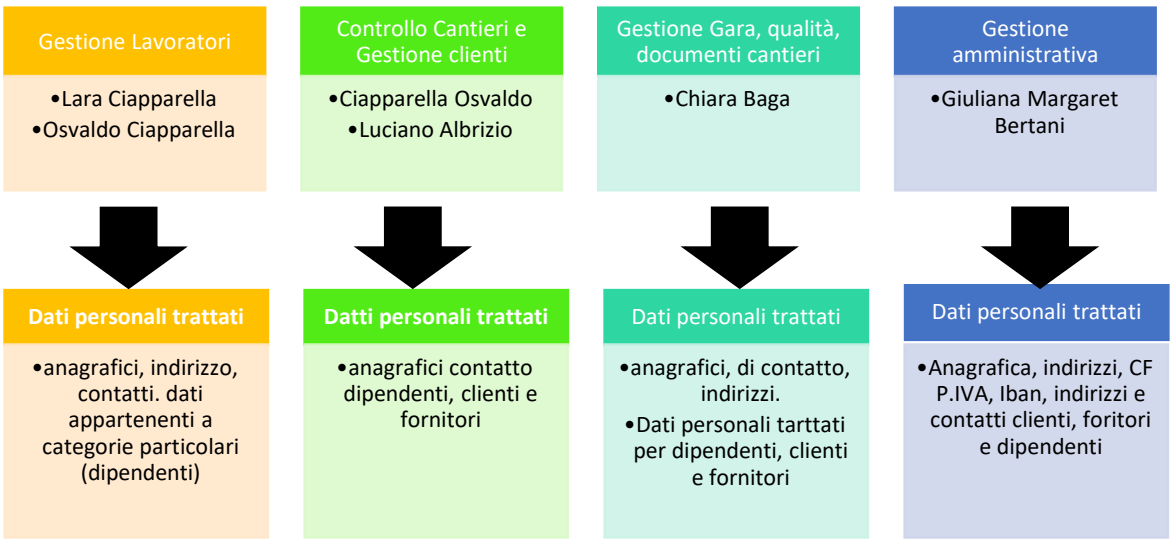
Nel Regolamento 679/2016 la figura dell'incaricato al trattamento viene definito in differenti modalità ovvero come:

- ✓ persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare (art. 4 e 28)
- ✓ personale che esegue i trattamenti (art 39)
- ✓ personale che ha accesso permanente o regolare ai dati personali (art. 47)

In sostanza gli incaricati sono coloro i quali effettuano materialmente le operazioni connesse al trattamento dati personali, ovviamente pur non rispondendo direttamente alle violazioni, anche per tali figure VIGE l'obbligo di rispetto di tutte le norme della privacy.

Qualora il medico dovesse avere personale addetto al trattamento dei dati deve seguire nomina ed istruzioni operative.

Ogni incaricato ha la propria Area e gestisce determinati dati personali che sono pertinenti alla propria attività lavorativa



2.2 Interessato e i suoi Diritti

Il soggetto interessato è il cliente ossia una persona fisica privata che ha determinati diritti:

DIRITTI DELL'INTERESSATO		TITOLARE	INTERESSATO
Diritto di Accesso	Diritto di ottenere dal Titolare la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e di ottenere l'accesso ai dati personali e ad una serie di informazioni che lo riguardano: le finalità del trattamento Le categorie dei dati personali in questione I destinatari o le categorie di destinatari i cui dati sono o saranno comunicati	Diritto di accesso presente nell'informativa Delega per consegne Consenso per invio telematico dati	Modello richiesta esercizio diritto di Accesso o semplice lettera, email, fax
Diritto di Rettifica	Diritto di ottenere dal Titolare la rettifica dei dati personali che lo riguardano, l'integrazione dei dati personali incompleti	Diritto di rettifica presente nell'informativa Corregge o completa le informazioni durante la visita	Fornisce un'integrazione tramite colloquio in visita Modello di rettifica (ALL.5) o semplice lettera, email, fax
Diritto alla Cancellazione	Diritto alla cancellazione dei propri dati personali se sussiste uno degli specifici motivi indicati: a) i dati personali non sono più necessari rispetto alle finalità di raccolta b) l'interessato revoca il consenso o si oppone al trattamento c)	Conservazione dati 10 anni. Risposta obbligatoria con motivazione	Modello di richiesta cancellazione o semplice lettera, email, fax
Diritto alla limitazione del trattamento	Diritto ad ottenere la limitazione del trattamento quando si verifica una delle ipotesi della normativa: a) contestazione dell'esattezza dei dati personali b) l'interessato chiede espressamente la limitazione del trattamento revocando il consenso dato (ad esempio ai familiari)	Diritto di limitazione presente nell'informativa. Risposta entro 30 giorni e presa in carico della limitazione al trattamento.	Modello di richiesta limitazione al trattamento o semplice lettera, email, fax
Diritto di non essere sottoposto a processi automatizzati	Non sviluppato in quanto non applicabile ai Medici		
Diritto di opposizione	Diritto di opporsi per motivi connessi alla sua situazione al trattamento dei dati personali.	Diritto di opposizione presente nell'informativa. Risposta entro 30 giorni	Modello di richiesta limitazione al trattamento o semplice lettera, email, fax

3.0 ALGORITMO VALUTAZIONE

Il seguente documento è stato stilato dal Datore di lavoro con la consulenza della Dottoressa Mandelli (Studio Mandelli Srl) e dell'esperto informatico Matteo Cartabia (IWS di Matteo Cartabia).

1° STEP: identificazione dei trattamenti

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

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

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

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

LR = P X C

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

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

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

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

CONSEGUENZE	
1	**Trascurabili**
2	**Marginali**
3	**Limitate**
4	**Gravi**
5	**Gravissime**

MATRICE DEI RISCHI

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

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

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

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

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

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

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

3 STEP: DPIA – valutazione del rischio normalizzato

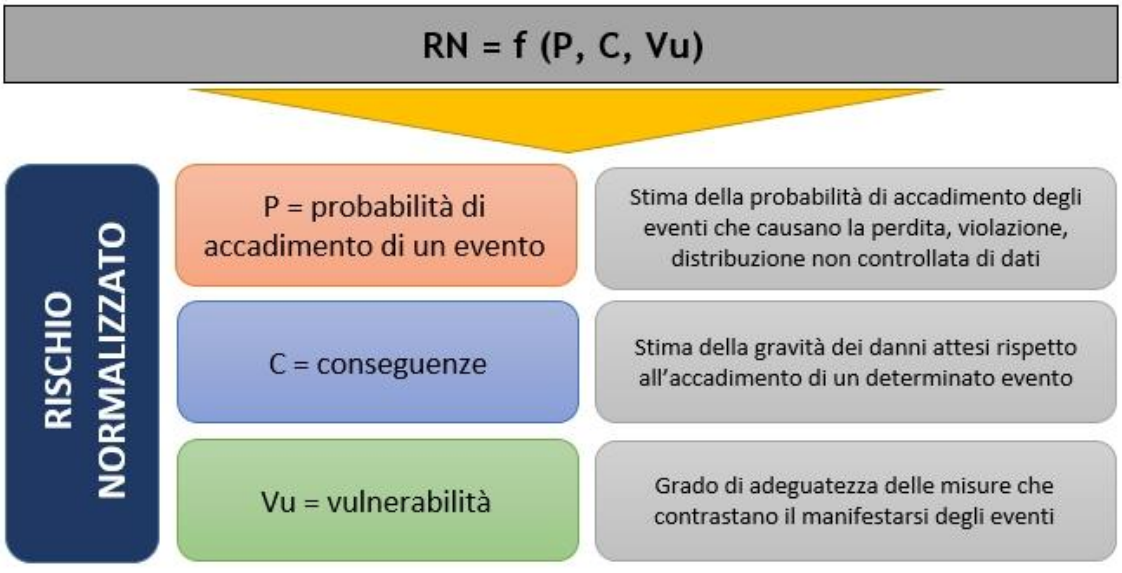
Ai sensi dell'art. 35 del GDPR, vengono individuate tutte le attività di trattamento che in prima analisi presentano un livello di rischio alto e/o prevendono due o più criteri di obbligo DPIA.
Nel caso in cui, quindi, l'indice di rischio si colloca nel range 15 ÷ 25, l'attività necessita di una valutazione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

Il rischio viene calcolato in funzione dei 3 fattori seguenti:

RN = f (P, C, Vu)

Dove:

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



In prima battuta viene ricavato il rischio intrinseco Ri come prodotto della probabilità P e delle conseguenze C, in base agli indici numerici assegnati ad entrambi i fattori.
Alla **probabilità P** è associato un indice numerico rappresentato nella seguente tabella:

Probabilità	
1	**Improbabile**
2	**Poco probabile**
3	**Probabile**
4	**Quasi certo**

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

CONSEGUENZE	
1	**Trascurabili**
2	**Marginali**
3	**Limitate**
4	**Gravi**

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

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

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

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

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

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

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

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

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

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

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

Vu		1	$1 < RN \leq 2$	$3 \leq RN \leq 4$	$6 \leq RN \leq 9$	$12 \leq RN \leq 16$
		0,5	$0,5 < RN \leq 1$	$1,5 \leq RN \leq 2$	$3 < RN \leq 5$	$6 \leq RN \leq 8$
		0,25	$0,25 \leq RN \leq 0,5$	$0,75 \leq RN \leq 1$	$1,5 \leq RN < 3$	$3 \leq RN \leq 4$
			$1 \leq Ri \leq 2$	$3 \leq Ri \leq 4$	$6 \leq Ri \leq 9$	$12 \leq Ri \leq 16$
			Ri			

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

RISULTATI

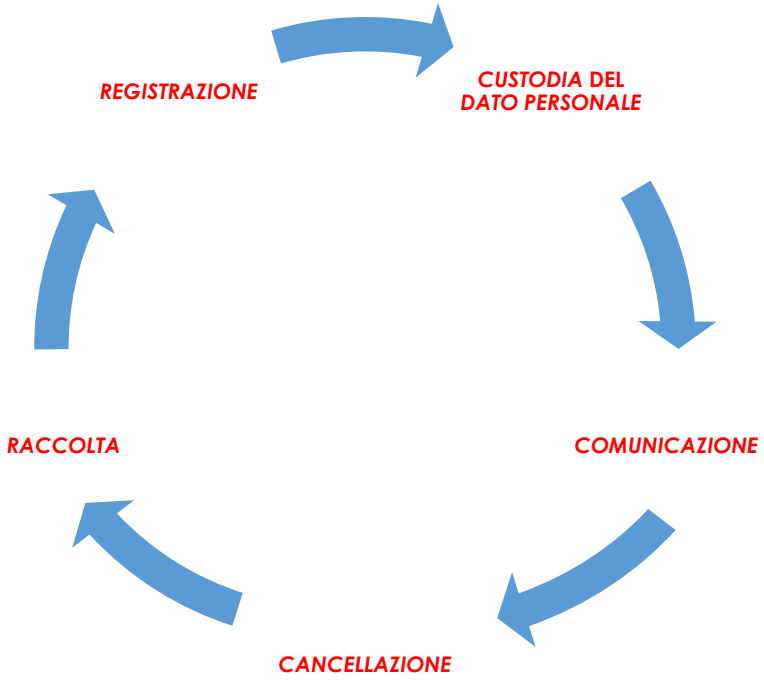
Dai risultati emersi dalla valutazione è emerso che NESSUNA ATTIVITA' PRESENTE necessita di essere sottoposta a DPIA. Viene allegato al presente Documento il Registro del trattamento dei dati (flussi) e la valutazione.

AZIONI DA IMPLEMENTARE

L'azienda segnala che verrà implementato il gestionale in quanto da gennaio 2019 dovrà poter usufruire dell'emissione della fattura elettronica. Si predisporrà un backup settimanale.

4.0 FASE DEL CICLO DI VITA DEL DATO PERSONALE4.1

RISULTATI



RISULTATI LEGISLATIVI

- ✓ Art. 33 e 34 del Nuovo regolamento europeo 2016/679 sulle modalità di comunicazione delle informazioni
- ✓ Provvedimento in materia di attuazione della disciplina sulla comunicazione delle violazioni di dati personali (c.d. data breach) del 4 aprile 2013

RISCHI SPECIFICI

La presente istruzione consente di gestire i seguenti rischi:

Superamento dei termini di legge per la gestione delle violazioni;

- ✓ Gestione non trasparente del processo di gestione della violazione;
- ✓ Danno irreparabile sulle banche dati;
- ✓ Danno alla reputazione dell'interessato;

Mancanza di evidenze storiche necessarie all'Autorità di controllo per verificare l'osservanza o meno del regolamento da parte dell'organizzazione attaccata.

4.1 PROCEDURA DI DATA BREACH

BANCA DATI	PROCEDURA
Archivio informatico o Archivio cartaceo	Nel caso di perdita o violazione dati viene avvisato il Titolare del Trattamento che attiva la procedura che consiste nel comunicare la violazione all'Autorità di controllo entro le 72 ore dal momento in cui si è venuti a conoscenza. La modalità e i relativi moduli sono disponibili sul sito del Garante della Privacy e vengono costantemente aggiornati, di seguito ne riportiamo un modello.

DESTINATARI

- ✓ Addetti al trattamento di Dati personali
- ✓ Responsabile del Trattamento

COME RICONOSCERE UNA VIOLAZIONE

- ✓ La violazione è l'effetto di un evento o di un'azione colposa o fraudolenta compiuta da un soggetto, che può compromettere o ha compromesso i diritti e le libertà delle persone fisiche interessate al trattamento.
- ✓ La violazione può essere determinata da:
- ✓ Lettura del dato da parte di uno o più soggetti non autorizzati
- ✓ Copia del dato da parte di uno o più soggetti non autorizzati
- ✓ Alterazione del dato da parte di uno o più soggetti non autorizzati
- ✓ Cancellazione del dato da parte di uno o più soggetti non autorizzati
- ✓ Furto del dato da parte di uno o più soggetti non autorizzati

COME GESTIRE E SEGNALARE UNA VIOLAZIONE

L' incaricato al trattamento che identifica una fra le violazioni citate, segnala con tempestività via mail ed entro 12 ore l'evento al Responsabile del Trattamento il quale ne valuta il danno e decidere se comunicarlo al Garante attraverso apposita modulistica. Tuttavia si considera che i dati personali trattati sono quelli riferiti al dipendente.

MODELLO DI REGISTRAZIONE DELLE VIOLAZIONI E NOTIFICA AL GARANTE

DATI SOCIETARI

Società titolare del trattamento

…….

Denominazione o ragione sociale

…….

Provincia, Comune, Cap, Indirizzo

…….

Nome e Cognome Titolare del Trattamento

…….

Nome e Cognome persona fisica addetta alla comunicazione …….
Funzione rivestita

…….

Indirizzo PEC e/o EMAIL per eventuali comunicazioni …….
Recapito telefonico per eventuali comunicazioni

…….

Eventuali Contatti (altre informazioni)

…….

DENOMINAZIONE DELLA/E BANCA/BANCHE DATI OGGETTO DI DATA BREACH E BREVE DESCRIZIONE DELLA VIOLAZIONE DEI DATI PERSONALI IVI TRATTATI

……

……

……

QUANDO SI È VERIFICATA LA VIOLAZIONE DEI DATI PERSONALI TRATTATI NELL'AMBITO DELLA BANCA DATI?

- ☐ Il ……..
- ☐ Tra il e il ……..
- ☐ In un tempo non ancora determinato
- ☐ E' possibile che sia ancora in corso

DOVE È AVVENUTA LA VIOLAZIONE DEI DATI? (SPECIFICARE SE SIA AVVENUTA A SEGUITO DI SMARRIMENTO DI DISPOSITIVI O DI SUPPORTI PORTATILI)

……

……

……

MODALITÀ DI ESPOSIZIONE AL RISCHIO

……

……

……

TIPO DI VIOLAZIONE

- ☐ Lettura (presumibilmente i dati non sono stati copiati)
- ☐ Copia (i dati sono ancora presenti sui sistemi del titolare)
- ☐ Alterazione (i dati sono presenti sui sistemi ma sono stati alterati)
- ☐ Cancellazione (i dati non sono più sui sistemi del titolare e non li ha neppure l'autore della violazione)
- ☐ Furto (i dati non sono più sui sistemi del titolare e li ha l'autore della violazione)
- ☐ Altro:……

DISPOSITIVO OGGETTO DELLA VIOLAZIONE

- ☐ Computer
- ☐ Rete
- ☐ Dispositivo mobile
- ☐ File o parte di un file
- ☐ Strumento di backup
- ☐ Documento cartaceo
- ☐ Altro:……

SINTETICA DESCRIZIONE DEI SISTEMI DI ELABORAZIONE O DI MEMORIZZAZIONE DEI DATI COINVOLTI, CON INDICAZIONE DELLA LORO UBICAZIONE:

……

……

QUANTE PERSONE SONO STATE COLPITE DALLA VIOLAZIONE DEI DATI PERSONALI TRATTATI NELL'AMBITO DELLA BANCA DATI?

- ☐ N. persone ……
- ☐ Circa persone ……
- ☐ Un numero (ancora) sconosciuto di persone

CHE TIPO DI DATI SONO OGGETTO DI VIOLAZIONE?

- ☐ Dati anagrafici/codice fiscale
- ☐ Dati di accesso e di identificazione (user name, password, customer ID, altro)
- ☐ Dati relativi a minori
- ☐ Dati personali idonei 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
- ☐ Dati personali idonei a rivelare lo stato di salute e la vita sessuale
- ☐ Dati giudiziari
- ☐ Copia per immagine su supporto informatico di documenti analogici
- ☐ Ancora sconosciuto
- ☐ Altro:……

LIVELLO DI GRAVITÀ DELLA VIOLAZIONE DEI DATI PERSONALI TRATTATI NELL'AMBITO DELLA BANCA DATI (SECONDO LE VALUTAZIONI DEL TITOLARE)?

- ☐ Basso/trascurabile
- ☐ Medio
- ☐ Alto
- ☐ Molto alto

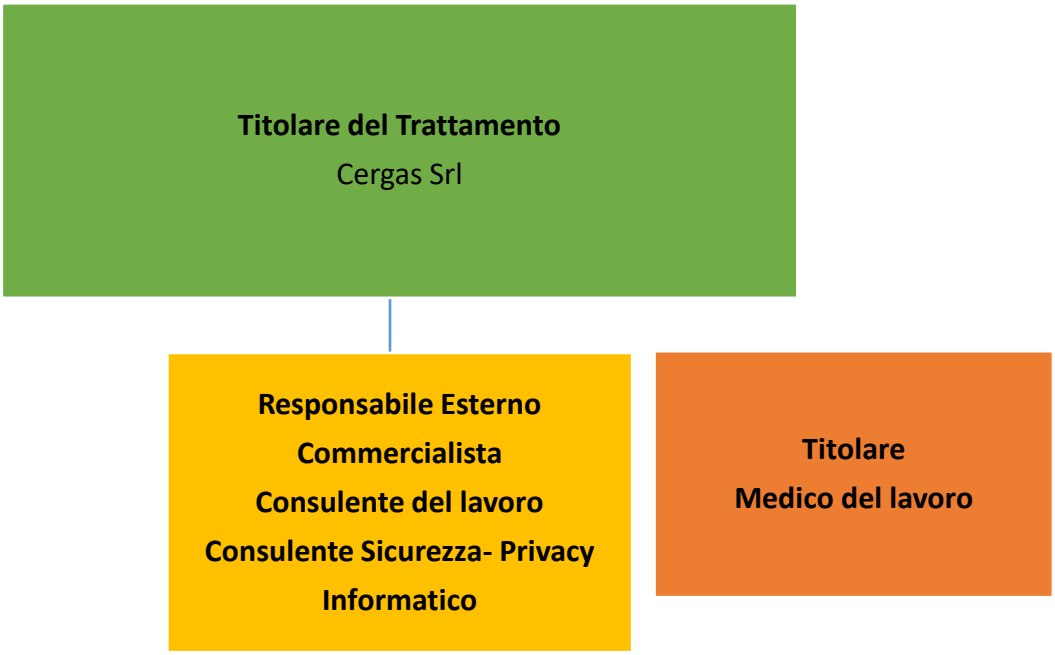
MISURE TECNICHE E ORGANIZZATIVE APPLICATE AI DATI OGGETTO DI VIOLAZIONE

……

……

……

5. ORGANIGRAMMA PRIVACY



Nomine	Nomi o Ragioni Sociali	Dati trattati	Nomina
Responsabile del trattamento Dati	Commercialista	Anagrafici e appartenenti a categorie particolari	SI
Responsabile del trattamento dati	Consulente del lavoro	Anagrafici ed appartenenti a categorie di dati particolari	SI
Responsabile del trattamento dati	Consulente sicurezza e privacy	Anagrafici e contatti	SI
Responsabile del trattamento dati	Consulente informatico	Anagrafici e di contatto	SI
Responsabile del trattamento dati	Consulente certificazione	Anagrafici e di contatto	SI
Titolare trattamento dati	Medico Competente	Anagrafici ed appartenenti a categorie di dati particolari	SI

Si rimanda all'allegato 4 dove l'azienda aggiorna l'elenco dei consulenti esterni – fornitori e quindi le nomine dei Responsabili esterni.

5.1 MISURE DI SICUREZZA ADOTTATE

RISCHIO RILEVATO	*TRATTAMENTO*	*MISURA*	*INTEGRAZIONE*	*ENTRO IL*
Sottrazione di credenziali di autenticazione per comportamenti sleali o fraudolenti	Tutti con conseguenza perdita di dati	Per i dati conservati a portale vi sono le credenziali di autentificazioni che devono essere personali e cambiate ogni 3 mesi. Le proprie credenziali di accesso potranno essere comunicate al Titolare qualora volesse entrare a seguito di una prolungata assenza. In caso di non utilizzo prolungato da almeno 6 mesi vengono disattivate. Se l'incaricato non deve più accedere a quella tipologia di dati occorre disattivargli le credenziali. Ogni incaricato accede ai dati strettamente necessari per svolgere la propria mansione lavorativa. Il Titolare del Trattamento provvederà alla verifica annuale della sussistenza delle condizioni per la conservazione dei profili di autorizzazione.	In essere	
Errori del personale, carenza di consapevolezza	Tutti con conseguenza perdita di dati	Attività formativa	Effettuata	

RISCHIO RILEVATO	*TRATTAMENTO*	*MISURA*	*INTEGRAZIONE*	*ENTRO IL*
Comportamenti sleali	Tutti con conseguenza perdita di dati	Attività formativa	Effettuata	
Accessi esterni non autorizzati	Tutti con conseguenza perdita di dati	Sono state adottate le misure di sicurezza per i dati appartenenti a categorie particolari (cifratura – separazione)		
Azione di virus informatici o di programmi suscettibili di recare danno	Tutti con conseguenza perdita di dati	Il pc è dotato di programma antivirus		
Azione di virus informatici o di programmi suscettibili di recare danno	Tutti con conseguenza perdita di dati	Aggiornamento dei programmi per elaborare. Il sistema operativo e gli applicativi vengono aggiornati utilizzando le procedure di download da Internet rese disponibili dai produttori		
Malfunzionamento, degrado degli strumenti	Tutti con conseguenza perdita di dati	Copie di sicurezza. Sono previste delle procedure che prevedono il backup dei dati		
Malfunzionamento, degrado degli strumenti	Tutti con conseguenza perdita di dati	Ripristino dei dati avviene entro 3 giorni		
Accessi esterni non autorizzati	Tutti	Custodia dello strumento elettronico durante una sessione di trattamento. Non vengono lasciati appunti o meglio schede di registrazione dati personali incustoditi o su banchi e scrivanie. Finita la consultazione vengono riposti nel cassetto chiuso.		

RISCHIO RILEVATO	*TRATTAMENTO*	*MISURA*	*INTEGRAZIONE*	*ENTRO IL*
Intercettazione di informazioni in rete	Tutti con conseguenza perdita di dati	VPN/HTTPS Sono stati attivati i protocolli per le comunicazioni sicure in rete		30.11.2018
Misure ulteriori	Tutti con conseguenza perdita di dati	Custodia, uso e distruzione dei supporti rimovibili. I supporti rimovibili su cui vengono salvate le copie di sicurezza dei dati vengono conservati in armadi o cassetti chiusi a chiave. I PC una volta obsoleti vengono distrutti oppure, se riutilizzati, possono essere consegnati solo ad utenti autorizzati al trattamento dei dati dopo essere stati formattati.		
Visione di dati personali appartenenti a categorie particolari (sanitari) da parte di terzi non autorizzati	Tutti con conseguenza perdita di dati	Attività formativa		
Accessi esterni non autorizzati, sottrazione documenti contenenti dati	Tutti con conseguenza perdita di dati	Videosorveglianza		

RISCHIO RILEVATO	*TRATTAMENTO*	*MISURA*	*INTEGRAZIONE*	*ENTRO IL*
Errori Umani nella gestione della sicurezza fisica	Tutti con conseguenza perdita di dati	Disposizioni sulla gestione dei documenti. Gli incaricati devono possedere disposizioni affinché i documenti cartacei non siano lasciati incustoditi sulle scrivanie o tavoli di lavoro. I documenti devono essere conservate in armadi o cassetti chiusi e prelevati solo per il tempo necessario al trattamento. Durante il trattamento i documenti dovranno essere custoditi e controllati in modo che non siano visionati, anche temporaneamente, da personale non autorizzato.		
Errori Umani nella gestione della sicurezza fisica	Tutti con conseguenza perdita di dati	Distruzione documenti cartacei. Gli incaricati sono stati istruiti affinché tutti i documenti cartacei destinati allo smaltimento vengono preventivamente distrutti e quindi resi illeggibili.		
Archivio documentale informatizzato				

5.2 PROCEDURE OPERATIVE

RICHIESTA	*BANCA DATI*	*PROCEDURA*	*INCARICATO*
Modifica	Tutte le banchi dati che trattano dati personali dell'interessato	Si procede alla modifica come richiesto dall'interessato il prima possibile, comunque almeno entro le 24 ore. Inoltre si invia comunicazione anche a soggetti terzi (Responsabili del trattamento) anche esterni per le relative procedure di cancellazione. Questo sempre se non risultano impedimenti dettati da obblighi di legge.	
Cancellazione	Tutte le banchi dati che trattano dati personali dell'interessato	Si procede alla modifica come richiesto dall'interessato il prima possibile, comunque almeno entro le 24 ore. Inoltre si invia comunicazione anche a soggetti terzi (Responsabili del trattamento) anche esterni per le relative procedure di limitazione del trattamento. Questo sempre se non risultano impedimenti dettati da obblighi di legge.	
Limitazione al trattamento	Tutte le banchi dati che trattano dati personali dell'interessato	Si procede al blocco dei dati del trattamento come richiesto dall'interessato il prima possibile, comunque almeno entro le 24 ore. Inoltre si invia comunicazione anche a soggetti terzi (Responsabili del trattamento) anche esterni per le relative procedure di limitazione del trattamento. Questo sempre se non risultano impedimenti dettati da obblighi di legge.	

RICHIESTA	*BANCA DATI*	*PROCEDURA*	*INCARICATO*
Portabilità	Tutte le banche dati elettroniche contenenti dati personali dell'interessato	L'incaricato procede all'estrazione dei dati in un formato strutturato di uso comune con la funzione disponibile del centro ottico e consegna al cliente il file protetto da password su memoria USB. La password di accesso al file viene consegnata al cliente in busta chiusa. Al cliente viene richiesta la firma di una ricevuta che attesta la consegna del file in seguito alla richiesta di esercizio del diritto alla portabilità.	

6. CRITERI E MODALITA' DI RIPRISTINO DELLA DISPONIBILITA' DEI DATI

6.1 SALVATAGGIO DATI

BANCA DATI	*PROCEDURA*	*LUOGO DI CUSTODIA BACKUP*	*INCARICATO*
Archivio informatizzato documentale	Il salvataggio dei dati viene effettuato ogni giorno su un disco esterno. Presente anche un salvataggio storico mensile. Il Titolare deve verificare il buon esito del salvataggio.	I salvataggi devono essere chiusi all'interno di un armadio e comunque non accessibili a personale non autorizzato.	

6.2 RIPRISTINO DELLA DISPONIBILITA' DEI DATI

BANCA DATI	*PROCEDURA*	*Prove di ripristino*
Archivio Informatico documentale	Il ripristino dei dati viene effettuato utilizzando i sistemi di backup. Nell'ipotesi in cui i dati o gli strumenti elettronici subiscono dei danni, viene seguita la seguente procedura: • Viene immediatamente avvisato il Titolare del trattamento • Viene contattato un tecnico informatico al fine di sollecitare l'immediato intervento • Se l'hardware non ha subito danni, si procede con sollecitudine alla reinstallazione del sistema operativo e degli applicativi e rispettivamente aggiornamenti • Si procede al ripristino dei dati contenuti nell'ultima copia di sicurezza.	1 volta all'anno

7.0 FORMAZIONE

Il Regolamento Europeo 679/2016 ha istituito il Principio di Accountability che si traduce in italiano con RESPONSABILIZZAZIONE superando il principio espresso nel Codice della Privacy del D.lgs 196/2003. Al fine di poter mettere in atto un sistema di misure di sicurezza documentali - tecniche ed organizzative congrue alla norma occorre essere prima di tutto informati e formati su quanto occorre fare. Solo in questo modo è possibile affrontare una valutazione dei propri rischi sul trattamento dei dati.

Si rende pertanto indispensabile una formazione a più livelli e precisamente:

a) Per gli incaricati – persone autorizzate al trattamento dei dati una formazione generale

FORMAZIONE				
Nomine	**Data Attestato**	**Modalità formazione**		**Nome e Cognome**
		Aula	**E-learning**	
DL		X	X	Ciapparelli Lara
Incaricato			X	Ciapparella Osvaldo
Incaricato			X	Chiara Baga
Incaricato			X	Bertani Giuliana Margaret
Incaricato			X	Luciano Albrizio
Incaricato				

8.0 REGISTRO TRATTAMENTI DATI

GESTIONE PERSONALE

FINALITA'	SOGGETTI INTERESSATI	AMBITI DI TRATTAMENTO	TIPOLOGIA DEI DATI TRATTATI ED INTERESSATI	ARCHIVIAZIONE CARTACEO	ARCHIVIAZIONE ELETTRONICO	PERSONALE AUTORIZZATO INTERNO	PERSONALE AUTORIZZATO ESTERNO
SELEZIONE DEL PERSONALE	CANDIDATO	RACCOLTA CANDIDATURE	DATI PERSONALI DI NATURA COMUNE DEI CANDIDATI (Nome, Cognome, Dati di contatto, CV professionale, Dati Sensibili del candidato solo se appartenente a categorie protette)	NO	NO	CIAPPARELLA LARA	NO
		VALUTAZIONE DEL PROFILO E COLLOQUIO		NO	NO	CIAPPARELLA LARA	NO
		ARCHIVIAZIONE DATI		NO	NO	CIAPPARELLA LARA	NO
GESTIONE DEL PERSONALE	LAVORATORE	FORMULAZIONE CONTRATTO	(Nome, Cognome, Dati di contatto, Coordinate Bancarie, Livello Retributivo, Condizioni Contrattuali, presenze, ferie, iscrizione sindacato, cessione del quinto, pignoramenti, contenzioso, assegni familiari, detrazioni, incentivi, bonus, assicurazioni, TFR, dati familiare a carico, grado di parentela, disabilità (legge 104)	SI	NO	CIAPPARELLA LARA	SI
		GESTIONE PRESENZE		SI	NO	BERTANI GIULIANA LARA CIAPPARELLA	SI
		GESTIONE PAGHE		SI	NO	BERTANI GIULIANA LARA CIAPPARELLA	SI
		FORMAZIONE	Anagrafica, mansione, luogo di lavoro, attestato di valutazione	SI	SI	CIAPPARELLA LARA CHIARA BAGA	SI
		VISITE MEDICHE	Anagrafica, mansione, luogo di lavoro, idoneità	SI	SI	CIAPPARELLA LARA CHIARA BAGA LUCIANO ALBRIZIO	SI

FINALITA'	SOGGETTI INTERESSATI	AMBITI DI TRATTAMENTO	TIPOLOGIA DEI DATI TRATTATI ED INTERESSATI	ARCHIVIAZIONE CARTACEO	ARCHIVIAZIONE ELETTRONICO	PERSONALE AUTORIZZATO INTERNO	PERSONALE AUTORIZZATO ESTERNO
GESTIONE PRATICHE SICUREZZA	DL E LAVORATORI	DOCUMENTI PER NORMTIVA	Dati Anagrafici, Attestati formazione	SI	SI	CIAPPARELLA LARA CHIARA BAGA LUCIANO ALBRIZIO CIAPPARELLA OSVALDO	SI

FINALITA'	SOGGETTI INTERESSATI	AMBITI DI TRATTAMENTO	TIPOLOGIA DEI DATI	ARCHIVIAZIONE CARTACEO	ARCHIVIAZIONE ELETTRONICO	PERSONALE AUTORIZZATO	PERSONALE AUTORIZZATO ESTERNO
GESTIONE CONTABILE	FORNITORI ESTERNI CONSULENTI	PAGAMENTO FATTURE	Dati contabili aziendali Dati fornitori/consulenza (anagrafica) Anagrafica e dati fiscali del professionista, compenso pattuito	SI	SI	BERTANI GIULIANA LARA CIAPPARELLA	SI

FINALITA'	SOGGETTI INTERESSATI	AMBITI DI TRATTAMENTO	TIPOLOGIA DEI DATI TRATTATI ED INTERESSATI	ARCHIVIAZIONE CARTACEO	ARCHIVIAZIONE ELETTRONICO	PERSONALE AUTORIZZATO INTERNO	PERSONALE AUTORIZZATO ESTERNO
ACQUISTO	FORNITORI	MATERIE PRIME, ATTREZZI, MACCHINE	Dati Anagrafici, contat , bancari	SI	SI	**BERTANI GIULIANA LARA CIAPPARELLA**	SI
VISITA MEDICA	**DIPENDENTI**	IDONEITA' ALLA MANSIONE	Idoneità mediche, dati anagrafici	SI	SI	CIAPPARELLA LARA CHIARA BAGA LUCIANO ALBRIZIO CIAPPARELLA OSVALDO	SI

FINALITA'	SOGGETTI INTERESSATI	AMBITI DI TRATTAMENTO	TIPOLOGIA DEI DATI TRATTATI ED INTERESSATI	ARCHIVIAZIONE CARTACEO	ARCHIVIAZIONE ELETTRONICO	PERSONALE AUTORIZZATO INTERNO	PERSONALE AUTORIZZATO ESTERNO
GESTIONE BANCARIA	SOCIETA'	GESTIONE C/C	Dati Anagrafici, Documenti di Riconoscimento	SI	SI	**BERTANI GIULIANA LARA CIAPPARELLA**	SI

FINALITA'	SOGGETTI INTERESSATI	AMBITI DI TRATTAMENTO	TIPOLOGIA DEI DATI TRATTATI ED INTERESSATI	ARCHIVIAZIONE CARTACEO	ARCHIVIAZIONE ELETTRONICO	PERSONALE AUTORIZZATO INTERNO	PERSONALE AUTORIZZATO ESTERNO
GESTIONE DISMISSIONI PC E SUPPORTI INFORMATICI	SOCIETA'	CANCELLAZIONE DATI PERSONALI	Dati Anagrafici, di contatto e appartenenti a categoria di dati particolari	NO	SI	CIAPPARELLA LARA ED OSVALDO	TECNICO INFORMATICO

FINALITA'	SOGGETTI INTERESSATI	AMBITI DI TRATTAMENTO	TIPOLOGIA DEI DATI TRATTATI ED INTERESSATI	ARCHIVIAZIONE CARTACEO	ARCHIVIAZIONE ELETTRONICO	PERSONALE AUTORIZZATO INTERNO	PERSONALE AUTORIZZATO ESTERNO
DIREZIONE CANTIERI GESTIONE CLIENTI COMMITTENTI	CLIENTI, COMMITTENTI	VIGILANZA SULLA CORRETTA ESECUZIONE COMMESSA	Dati Anagrafici, di contatto	si	SI	CIAPPARELLA OSVALDO CHIARA BAGA LUCIANO ALBRIZIO	TECNICO INFORMATICO

FINALITA'	SOGGETTI INTERESSATI	AMBITI DI TRATTAMENTO	TIPOLOGIA DEI DATI TRATTATI ED INTERESSATI	ARCHIVIAZIONE CARTACEO	ARCHIVIAZIONE ELETTRONICO	PERSONALE AUTORIZZATO INTERNO	PERSONALE AUTORIZZATO ESTERNO
PROTEZIONE BENE AZIENDALE	DIPENDENTI, CLIENTI E FORNITORI	CONTROLLO DI POSSIBILI VIOLAZIONI ESTERNE DI PERSONE NON AUTORIZZATE	Immagine	No	SI 24 ore	CIAPPARELLA OSVALDO CHIARA BAGA LUCIANO ALBRIZIO	TECNICO INFORMATICO

9.0 VALUTAZIONE D'IMPATTO

FINALITA'	VIOLAZIONE INTERNA MISURE DI SICUREZZA	VIOLAZIONE ESTERNA MISURE DI SICUREZZA	PROTEZIONE PERDITA DATI	TEMPI DI CUSTODIA	INFORMATIVA	CONSENSO	VALUTAZIONE		
							PROBABILITA	CONSEGUENZE	RISCHIO
GESTIONE BANCARIA	Username e password conservate separatamente dal token in armadi chiusi, corrette procedure comportamentali, chiave d'accesso gestita direttamente dal titolare	Procedure comportamentali, accessi controllati, token posto separatamente e chiuso a chiave Videosorveglianza Firewall	Antivirus, aggiornamento software, non apertura di messaggi da mittenti sconosciuti, non visione di siti non protetti	FINO A REVOCA CONTRATTO CON BANCA	NO	NO	**POCO PROBABILE**	**MARGINALE**	**BASSO**

FINALITA'	VIOLAZIONE INTERNA MISURE DI SICUREZZA	VIOLAZIONE ESTERNA MISURE DI SICUREZZA	PROTEZIONE PERDITA DATI	TEMPI DI CUSTODIA	INFORMATIVA	CONSENSO	VALUTAZIONE		
							PROBABILITA	CONSEGUENZE	RISCHIO
ACQUISTO MATERIE PRIME ATTREZZI	Username e password trimestrali, corrette procedure comportamentali, accessi controllati	Procedure comportamentali, accessi controllati Firewall	Documenti posti in armadi al fine di evitare eventuale perdita da allagamenti.	10 ANNI	SI (verbale)	SI (verbale)	**POCO PROBABILE**	**MARGINALE**	**BASSO**
GESTIONE CANTIERE	Cellulari e tablet con password, non hanno dati personali ma solo informazioni tecniche e rubrica contatti.	Procedure comportamentali,	Non sono conservati dati personali su dispositivi mobili	Fino all'utilizzo della scheda SIM (i dati sono salvati su essa)	SI	MO	**POCO PROBABILE**	**MARGINALE**	**BASSO**
GESTIONE PRATICHE SICUREZZA	Username e password trimestrali, corrette procedure comportamentali, accessi controllati	Procedure comportamentali, accessi controllati. I POS sono sui mezzi da cantiere in una cartella chiusa. Il mezzo viene chiuso a chiave e posto sempre sotto controllo. I mezzi sono dotati di antifurto Firewall	Backup settimanale e storico,	10 ANNI	NO	NO	**POCO PROBABILE**	**MARGINALE**	**BASSO**

FINALITA'	VIOLAZIONE INTERNA MISURE DI SICUREZZA	VIOLAZIONE ESTERNA MISURE DI SICUREZZA	PROTEZIONE PERDITA DATI	TEMPI DI CUSTODIA	INFORMATIVA	CONSENSO	VALUTAZIONE		
							PROBABILITA'	CONSEGUENZE	RISCHIO
GESTIONE DEL PERSONALE	Corrette procedure comportamentali, credenziali di accesso, cedolini ritirati in busto chiusa direttamente a mano e consegnati al dipendente	Videosorveglianza Firewall	Posizionati in armadio chiuso, accesso autorizzato, impianto elettrico conforme e rispettivi controlli di messa a terra, presenza di sistemi spegnimento fuoco	10 ANNI	SI	SI	**POCO PROBABILE**	**MARGINALE**	**BASSO**
PROTEZIONE BENE AZIENDALE	Le registrazioni possono essere viste solo da personale autorizzato in possesso di credenziali di accesso	Evitare a persone non autorizzate di accedere al monitor (le immagini sono protette da password)		24 ORE	SI	Si per i lavoratori	**POCO PROBABILE**	**MARGINALE**	**BASSO**

FINALITA'	VIOLAZIONE INTERNA MISURE DI SICUREZZA	VIOLAZIONE ESTERNA MISURE DI SICUREZZA	PROTEZIONE PERDITA DATI	TEMPI DI CUSTODIA	INFORMATIVA	CONSENSO	VALUTAZIONE		
							PROBABILITA'	CONSEGUENZE	RISCHIO
SELEZIONE DEL PERSONALE	Il trattamento dei dati inerenti il personale (quelli presenti sul CV) non vengono conservati in alcuna modalità (cartacea o informatica). Il candidato spesso arriva a colloquio senza un CV o consegnandolo direttamente all'atto del colloquio.								

FINALITA'	VIOLAZIONE INTERNA MISURE DI SICUREZZA	VIOLAZIONE ESTERNA MISURE DI SICUREZZA	PROTEZIONE PERDITA DATI	TEMPI DI CUSTODIA	INFORMATIVA	CONSENSO	VALUTAZIONE		
							PROBABILITA'	CONSEGUENZE	RISCHIO
INTERAZIONE CON MEDICO DEL LAVORO	Username e password trimestrali, corrette procedure comportamentali, accessi controllati, Crittografia	Procedure comportamentali, accessi controllati, non vengono inoltrati dati contenenti dati personali appartenenti a categorie particolari tramite email. Le idoneità vengono consegnate a mano e archiviate in formato elettronico. Le cartelle sanitarie sono conservate dal Medico del Lavoro	Backup settimanale e storico; armadi chiusi a chiave, mezzi di spegnimento del fuoco, impianto elettrico a norma Videosorveglianza	FINO CESSAZIONE RAPPORTO LAVORATIVO	SI	SI	**POCO PROBABILE**	**MARGINALE**	**BASSO**

FINALITA'	VIOLAZIONE INTERNA MISURE DI SICUREZZA	VIOLAZIONE ESTERNA MISURE DI SICUREZZA	PROTEZIONE PERDITA DATI	TEMPI DI CUSTODIA	INFORMATIVA	CONSENSO	VALUTAZIONE		
							PROBABILITA'	CONSEGUENZE	RISCHIO
GESTIONE DISMISSIONI PC E SUPPORTI INFORMATICI	**Prima di gettare un PC o qualsiasi supporto informatico occorre verificare che non vi siano contenuti dati personali. In tal caso è opportuno rivolgersi direttamente ad un tecnico informatico al fine di poter certificare l'avvenuta cancellazione dei dati presenti prima di procedere alla sua eliminazione**								

10. CONCLUSIONI11

Le fasi di trattamento dei dati del Titolare sono state valutate e dovranno costantemente essere monitorate al fine di verificare se le misure di sicurezza rimangono appropriate. Si ricorda la normativa prevede che il Titolare, prima di iniziare un trattamento, deve effettuare un'analisi delle misure che intende adottare per una tutela dei dati in suo possesso. Quindi il Titolare dovrà non solo per i nuovi trattamenti ma anche per quelli in essere verificare annualmente una analisi dei trattamenti al fine di garantire la conformità delle misure di sicurezza adottate. Mentre gli adempimenti documentali sono in linea generale previsti dal Regolamento 679/2016 e quindi obbligatori, gli adempimenti tecnici-organizzativi non sono da considerare né tassativi, né esaustivi; ogni Titolare dovrà quindi valutarne l'adozione a seconda della propria situazione; si consiglia almeno una valutazione annuale.

11 ESEMPIO DI CONTROLLO ANNUALE

Adempimenti Documentali da valutare	
CLIENTI	
CLIENTI CESSATI	
FORNITORI	
DITTA ASSISTENZA SOFTWARE	
INTERNI ALLO STUDIO	
DIPENDENTI IN ESSERE	
DIPENDENTI CESSATI	

Adempimenti Tecnici	
PC PRESNTI	
INTERNET E POSTA ELETTRONICA	
ARCHIVIAZIONE DATI	

Adempimenti Organizzativi	
CONSERVAZIONE DOCUMENTI E BACKUP DEI DATI	
GESTIONE E DOCUMENTI NON UTILIZZATI	
FORMAZIONE NUOVI ASUNTI	
AGGIORNAMENTO FORMAZIONE	

Ad oggi la valutazione d'impatto effettuata rileva una situazione di rischio BASSA quindi le misure di sicurezza documentali, Tecniche ed organizzative risultano congrue.

12 ALLEGATI

1- INFORMATIVA CLIENTI
2- INFORMATIVA LAVORATORI
3- NOMINA ADDETTO INCARICATO – PERSONA AUTORIZZATA AL TRATTAMENTO
4- ELENCO SOCIETA' – PERSONE FISICHE CHE FUNGONO DA RESPONSABILI ESTERNI
5- NOMINA RESPONSABILI ESTERNI (si ricorda che vi deve essere sempre un contratto)
6- NOMINA TITOLARE DEL TRATTAMENTO (esempio Medico del lavoro)
7- ISTRUZIONI OPERATIVE
    a. Utilizzo dei sistemi informatici
    b. Videosorveglianza
    c. Data Breach
    d. Incaricato trattamento Dati
8- MODELLO VIOLAZIONE DATI PERSONALI per il Garante
9- MODELLO DEI DIRITTI DEGLI INTERESSATI