VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI

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

Azienda/Organizzazione	**STUDIO CONSULENZA DOTT. SAVERIO DI TRAPANI / SAVEL GROUP SOC. COOP. Start up innovativa**

TITOLARE	**DI TRAPANI SAVERIO**

SEDE	Via CELESTE 96 90047 Partinico - PA

Data rev. 3: 10/01/2020

VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI

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

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

OBBLIGO DPIA

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

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

CRITERI DA CONSIDERARE PER OBBLIGO DPIA

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

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

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

REVISIONE

Secondo le buone prassi, la valutazione d'impatto sulla protezione dei dati viene riesaminata continuamente e rivalutata con regolarità.

ALGORITMO VALUTAZIONE

1° STEP: identificazione dei trattamenti

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

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

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

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

$$LR = P \times C$$

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

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

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

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

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

MATRICE DEI RISCHI

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

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

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

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

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

1. Valutazione o assegnazione di un punteggio

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

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

3 STEP: DPIA – valutazione del rischio normalizzato

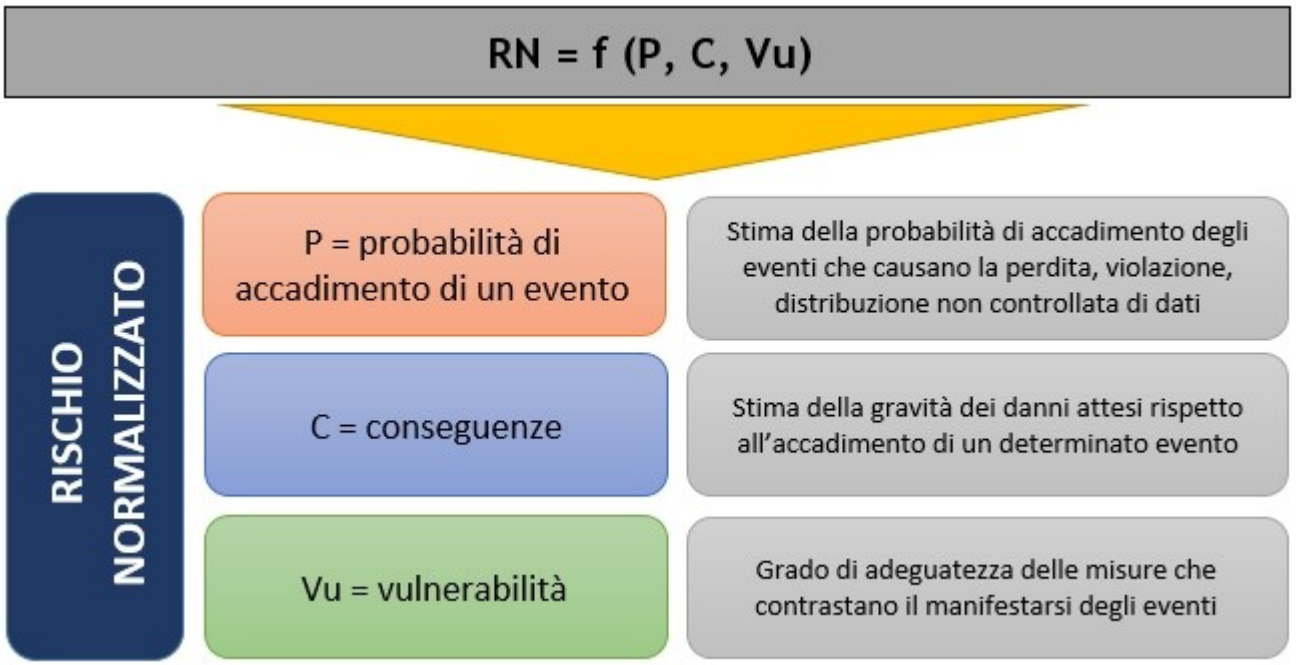
Ai sensi dell'art. 35 del GDPR, vengono individuate tutte le attività di trattamento che in prima analisi presentano un livello di rischio alto e/o prevendono due o più criteri di obbligo DPIA.
Nel caso in cui, quindi, l'indice di rischio si colloca nel range 15 ÷ 25, l'attività necessita di una valutazione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

Il rischio viene calcolato in funzione dei 3 fattori seguenti:

RN = f (P, C, Vu)

Dove:

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



In prima battuta viene ricavato il rischio intrinseco Ri come prodotto della probabilità P e delle conseguenze C, in base agli indici numerici assegnati ad entrambi i fattori.

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

Probabilità	
1	Improbabile
2	Poco probabile
3	Probabile
4	Quasi certo

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

CONSEGUENZE	
1	Trascurabili
2	Marginali
3	Limitate
4	Gravi

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

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

RISCHIO INTRINSECO	
Ri = P x C	**Valori di riferimento**
Molto basso	*(1 ≤ **Ri** ≤ 2)*
Basso	*(3 ≤ **Ri** ≤ 4)*
Rilevante	*(6 ≤ **Ri** ≤ 9)*
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 ≤ ***RN*** ≤ 0,5	0,75 ≤ ***RN*** ≤ 1	1,5 ≤ ***RN*** < 3	3 ≤ ***RN*** ≤ 4
		1 ≤ ***Ri*** ≤ 2	3 ≤ ***Ri*** ≤ 4	6 ≤ ***Ri*** ≤ 9	12 ≤ ***Ri*** ≤ 16
		Ri			

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

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

RISULTATI DPIA

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

Elenco attività sottoposte a DPIA

- CONSULENZA FISCALE E CONSULENZA DEL LAVORO

CONSULENZA FISCALE E CONSULENZA DEL LAVORO

Struttura	• Amministrazione • Sede legale • Sede operativa

Personale coinvolto	
Titolare del trattamento	DI TRAPANI SAVERIO C.F. DTRSVR71C19G348E
Persone autorizzate	RAPPA ELEONORA, c.f. RPPLNR71D53G348R • Cancellazione • Comunicazione • Conservazione • Consultazione • Elaborazione • Modifica • Organizzazione • Raccolta **VISCONTE CARMELO DANIELE**, c.f. VSCCML90H11G273Y • Cancellazione • Comunicazione • Conservazione • Consultazione • Elaborazione • Modifica • Organizzazione • Raccolta ANSELMO FRANCESCA MARIA (Collaboratrice) NSLFNC86T59G348O • Cancellazione • Comunicazione • Conservazione • Consultazione • Elaborazione • Modifica • Organizzazione • Raccolta DI BARTOLO TIZIANA, c.f. DBRTZN71S42G273F • Cancellazione

	• Comunicazione • Conservazione • Consultazione • Elaborazione • Modifica • Organizzazione • Raccolta
Partners - Responsabili esterni	Dott. PROVENZANO GIOACCHINO, consulente del lavoro, C.F. PRVGCH71L23G348L • Comunicazione • Conservazione • Consultazione • Elaborazione • Organizzazione • Raccolta SAVEL GROUP SOC. COOP., p.iva 05319320825 • Comunicazione • Conservazione • Consultazione • Elaborazione • Organizzazione • Raccolta MULTIENENRGY SRL (centro elaborazione dati) 05244840822 a. Comunicazione b. Conservazione c. Consultazione d. Elaborazione e. Organizzazione f. Raccolta
Altro	

Processo di trattamento	
Descrizione	Il trattamento ha luogo al fine di supportare le imprese attraverso servizi di consulenza fiscale e contabile, assistendole negli adempimenti previsti per legge derivanti dall'esercizio dell'attività commerciale e da rapporti di lavoro subordinati e assimilabili.
Fonte dei dati personali	Raccolti direttamente
Base giuridica per il trattamento per dati comuni (art. 6 GDPR)	Consenso Contratto Legge
Base giuridica per il trattamento per dati particolari (art. 9 GDPR)	Contratto Legge
Finalità del trattamento	Gestione della clientela (contratti, ordini, spedizioni e fatture) Gestione del contenzioso (contratti, ordini, arrivi, fatture) Attività di consulenza Adempimento di obblighi di legge connessi a rapporti commerciali Adempimento di obblighi fiscali o contabili Elaborazione dei documenti riguardanti i rapporti di lavoro instaurati con dipendenti o collaboratori Elaborazione, stampa, imbustamento e spedizione delle fatture

	Elaborazioni delle dichiarazioni fiscali Presentazione telematica delle dichiarazioni fiscali obbligatorie Attività di previdenza Comunicazione dati a terze parti per svolgere funzioni ed attività tecniche necessarie al servizio Elaborazione, stampa e spedizione delle buste paga Trattamento giuridico ed economico del personale
Tipo di dati personali	Dati identificativi (ragione o denominazione sociale, ovvero nome e cognome delle persone fisiche, indirizzo sede, telefono, fax, e-mail, dati fiscali, ecc.) Particolari (sensibili) Personali Dati relativi alla famiglia e a situazioni personali (stato civile, minori, figli, soggetti a carico, consanguinei, altri appartenenti al nucleo familiare) Nominativo, indirizzo o altri elementi di identificazione personale (nome, cognome, età, sesso, luogo e data di nascita, indirizzo privato, indirizzo di lavoro) Beni, proprietà, possessi (proprietà, possessi e locazioni; beni e servizi forniti o ottenuti) Codice fiscale ed altri numeri di identificazione personale (carte sanitarie) Dati di comunicazione elettronica Dati finanziari Adesione a sindacati o organizzazioni a carattere sindacale Amministrazione personale Dati relativi alla prestazione lavorativa Dati sulla salute Informazioni per la fatturazione e dati di pagamento (ragione sociale, P.IVA, coordinate bancarie, codice fiscale, indirizzo) Lavoro (occupazione attuale e precedente, informazioni sul reclutamento, sul tirocinio o sulla formazione professionale, informazioni sulla sospensione o interruzione del rapporto di lavoro o sul passaggio ad altra occupazione, curriculum vitae
Categorie di interessati	Consulenti e liberi professionisti, anche in forma associata Clienti ed utenti Dipendenti Collaboratori Fornitori
Categorie di destinatari	Camere di commercio, industria, artigianato ed agricoltura Banche e istituti di credito Consulenti e liberi professionisti anche in forma associata Enti previdenziali ed assistenziali Organismi paritetici in materia di lavoro Responsabili esterni Persone autorizzate Soggetti che svolgono attività di archiviazione della documentazione Studi legali
Informativa	Si
Profilazione	Non necessario
Dati particolari	Si
Consenso minori	Non necessario
Frequenza trattamento	Mensile - annuale
Termine cancellazione dati	I dati saranno trattati per tutto il tempo necessario allo svolgimento del rapporto commerciale in essere e per i successivi dieci anni dalla data di acquisizione degli stessi.

Trasferimento dati (paesi terzi)	No
Autorizzazione del Garante	Non presente

Modalità di elaborazione dati: Mista - elettronica e cartacea	
Strumenti	Quick Heal Total Security – Managed Antivirus E-BRIDGE WINDOWS 7 WINDOWS 10
Strutture informatiche di archiviazione	
SERVER FUJISTU	Struttura interna
Sede di riferimento	VIA CELESTE 96 PARTINICO
Personale con diritti di accesso	DI TRAPANI SAVERIO RAPPA ELEONORA VISCONTE CARMELO DANIELE ANSELMO FRANCESCA MARIA DI BARTOLO TIZIANA SAVEL GROUP SOC. COOP.
Software utilizzati	- Windows 10 pro - Managed Antivirus - EBRIDGE - Desktop telematico
DELL	Struttura interna
Sede di riferimento	VIA CELESTE 96 PARTINICO
Personale con diritti di accesso	DI TRAPANI SAVERIO RAPPA ELEONORA VISCONTE CARMELO DANIELE ANSELMO FRANCESCA MARIA DI BARTOLO TIZIANA SAVEL GROUP SOC. COOP.
Software utilizzati	- Windows 10 pro - Quick Heal Total Security - EBRIDGE - Desktop telematico
LENOVO	Struttura interna
Sede di riferimento	VIA CELESTE 96 PARTINICO
Personale con diritti di accesso	DI TRAPANI SAVERIO RAPPA ELEONORA VISCONTE CARMELO DANIELE ANSELMO FRANCESCA MARIA DI BARTOLO TIZIANA SAVEL GROUP SOC. COOP.
Software utilizzati	- Windows 10 pro - Quick Heal Total Security - EBRIDGE - Desktop telematico
FUJISTU	Struttura interna
Sede di riferimento	VIA CELESTE 96 PARTINICO
Personale con diritti di accesso	DI TRAPANI SAVERIO RAPPA ELEONORA VISCONTE CARMELO DANIELE ANSELMO FRANCESCA MARIA DI BARTOLO TIZIANA SAVEL GROUP SOC. COOP.
Software utilizzati	- Windows 10 pro - Quick Heal Total Security - EBRIDGE - Desktop telematico

THINK SERVER	Struttura interna
Sede di riferimento	VIA CELESTE 96 PARTINICO
Personale con diritti di accesso	DI TRAPANI SAVERIO RAPPA ELEONORA VISCONTE CARMELO DANIELE ANSELMO FRANCESCA MARIA DI BARTOLO TIZIANA SAVEL GROUP SOC. COOP.
Software utilizzati	- Windows 10 pro - Managed Antivirus - EBRIDGE - Desktop telematico
JEPSEN	Struttura interna
Sede di riferimento	VIA CELESTE 96 PARTINICO
Personale con diritti di accesso	DI TRAPANI SAVERIO RAPPA ELEONORA VISCONTE CARMELO DANIELE ANSELMO FRANCESCA MARIA DI BARTOLO TIZIANA SAVEL GROUP SOC. COOP.
Software utilizzati	- Windows 10 pro - Quick Heal Total Security - EBRIDGE - Desktop telematico
ASUS - PORTATILE	Struttura interna
Sede di riferimento	VIA CELESTE 96 PARTINICO
Personale con diritti di accesso	DI TRAPANI SAVERIO RAPPA ELEONORA VISCONTE CARMELO DANIELE ANSELMO FRANCESCA MARIA DI BARTOLO TIZIANA SAVEL GROUP SOC. COOP.
Software utilizzati	- Windows 10 pro - Quick Heal Total Security - EBRIDGE - Desktop telematico
Strutture informatiche di backup	
Server tower - fujitsu	Struttura interna
Sede di riferimento	VIA CELESTE 96 PARTINICO
Frequenza di backup	1 giorni in remoto – settimanale su hard disk esterno
Tempo di storicizzazione	5 giorni
Personale con diritti di accesso	DI TRAPANI SAVERIO RAPPA ELEONORA VISCONTE CARMELO DANIELE ANSELMO FRANCESCA MARIA DI BARTOLO TIZIANA SAVEL GROUP SOC. COOP.
Note	L'accesso è consentito esclusivamente al titolare del trattamento e a persone autorizzate.
Software utilizzati	- Windows server 2016 essentials - EBRIDGE - Desktop telematico

VALUTAZIONE DEL LIVELLO DI RISCHIO

PROBABILITÀ	CONSEGUENZE	LIVELLO DI RISCHIO
Poco probabile	Gravissime	Rilevante

MISURE DI SICUREZZA TECNICHE ED ORGANIZZATIVE
- Autorizzazione del singolo incaricato al trattamento e alla modifica dei dati - E' eseguita la DPIA - I dati sono crittografati - Impianto elettrico dotato di misure salvavita atte anche ad evitare cortocircuiti e possibili incendi - Le password sono costituite da almeno otto caratteri alfanumerici - Porte dotate di serratura in tutti i locali contenenti fisicamente le banche dati elettroniche e cartacee - Sono definiti i ruoli e le responsabilità - Sono gestiti i back up - Sono utilizzati software antivirus e anti intrusione - Viene eseguita opportuna manutenzione - Sistema di video sorveglianza - contratto di vigilanza

VALUTAZIONE ADEGUATEZZA DELLE MISURE DI SICUREZZA ADOTTATE

MISURE DI SIUREZZA	PERICOLI ASSOCIATI	LIVELLO DI ADEGUATEZZA
Autorizzazione del singolo incaricato al trattamento e alla modifica dei dati	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)	Adeguate
E' eseguita la DPIA	• Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.) • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)	Adeguate
I dati sono crittografati	• Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.) • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)	Adeguate

Impianto elettrico dotato di misure salvavita atte anche ad evitare cortocircuiti e possibili incendi	• Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.) • Agenti fisici (incendio, allagamento, attacchi esterni)	Adeguate
Le password sono costituite da almeno otto caratteri alfanumerici	• Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.) • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)	Adeguate
Porte dotate di serratura in tutti i locali contenenti fisicamente le banche dati elettroniche e cartacee	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)	Adeguate
Sono definiti i ruoli e le responsabilità	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)	Adeguate
Sono gestiti i back up	• Eventi naturali (terremoti, eruzioni vulcaniche, ecc.) • Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT) • Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.) • Agenti fisici (incendio, allagamento, attacchi esterni)	Adeguate
Sono utilizzati software antivirus e anti intrusione	• Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.) • Azioni non autorizzate (Errori volontari o involontari, virus, uso	Adeguate

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

VALUTAZIONE DEI RISCHI

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

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

PERICOLO
Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione,

interruzione collegamenti di rete, ecc.)		
RISCHI		
• Perdita • Distruzione non autorizzata • Modifica non autorizzata • Divulgazione non autorizzata • Accesso dati non autorizzato		
VALUTAZIONE RISCHIO INTRINSECO		
Probabilità	**Conseguenza**	**Rischio intrinseco - Ri**
Probabile	Marginali	Rilevante
VALUTAZIONE RISCHIO NORMALIZZATO *Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi*		
Rischio intrinseco - Ri	**Vulnerabilità - Vu**	**Rischio normalizzato - RN**
Rilevante	0,25	Basso

PERICOLO		
Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)		
RISCHI		
• Perdita • Distruzione non autorizzata • Modifica non autorizzata • Divulgazione non autorizzata • Accesso dati non autorizzato		
VALUTAZIONE RISCHIO INTRINSECO		
Probabilità	**Conseguenza**	**Rischio intrinseco - Ri**
Poco probabile	Gravi	Rilevante
VALUTAZIONE RISCHIO NORMALIZZATO *Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi*		
Rischio intrinseco - Ri	**Vulnerabilità - Vu**	**Rischio normalizzato - RN**
Rilevante	0,25	Basso

PERICOLO		
Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)		
RISCHI		
• Perdita • Distruzione non autorizzata • Modifica non autorizzata • Divulgazione non autorizzata		

• Accesso dati non autorizzato		
VALUTAZIONE RISCHIO INTRINSECO		
Probabilità	**Conseguenza**	**Rischio intrinseco - Ri**
Poco probabile	Gravi	Rilevante
VALUTAZIONE RISCHIO NORMALIZZATO *Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi*		
Rischio intrinseco - Ri	**Vulnerabilità - Vu**	**Rischio normalizzato - RN**
Rilevante	0,25	Basso

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

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

Savel Group
Soc. Coop. Start Up Innovativa
Il Legale Rappresentante