VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI

GDPR 2016/679

Azienda/Organizzazione **N2O S.r.l.**

TITOLARE	Amalia Ciaramitaro
SEDE	Sede Legale Via dei Chiosi 4, 20064 Gorgonzola - MI

Data revisione: 03/09/2018

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 X C

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

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

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

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

CONSEGUENZE	
1	Trascurabili
2	Marginali
3	Limitate
4	Gravi
5	Gravissime

MATRICE DEI RISCHI

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

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

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

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

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

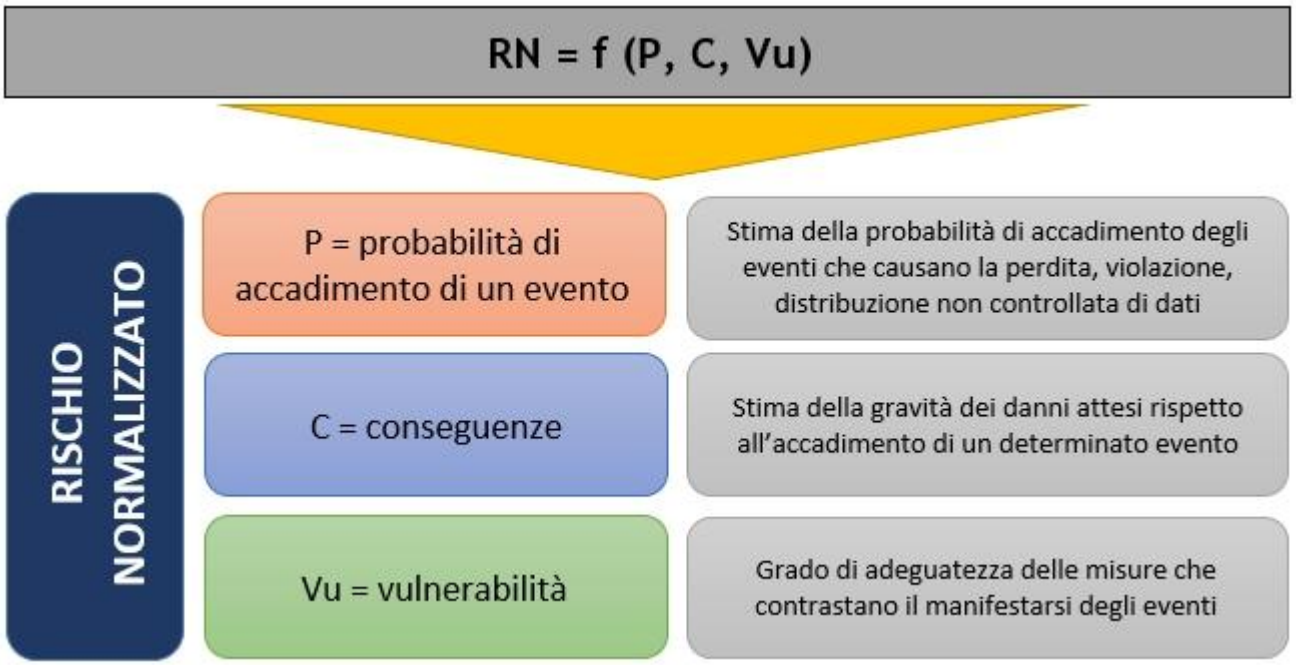
Ai sensi dell'art. 35 del GDPR, vengono individuate tutte le attività di trattamento che in prima analisi presentano un livello di rischio alto e/o prevendono due o più criteri di obbligo DPIA.
Nel caso in cui, quindi, l'indice di rischio si colloca nel range 15 ÷ 25, l'attività necessita di una valutazione 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*** ≤ 2	3 ≤ ***RN*** ≤ 4	6 ≤ ***RN*** ≤ 9	12 ≤ ***RN*** ≤ 16
	0,5	0,5 < ***RN*** ≤ *1*	1,5 ≤ ***RN*** ≤ 2	3 < ***RN*** ≤ 5	6 ≤ ***RN*** ≤ 8
	0,25	0,25 ≤ ***RN*** ≤ 0,5	0,75 ≤ ***RN*** ≤ 1	1,5 ≤ ***RN*** < 3	3 ≤ ***RN*** ≤ 4
		1 ≤ ***Ri*** ≤ 2	3 ≤ ***Ri*** ≤ 4	6 ≤ ***Ri*** ≤ 9	12 ≤ ***Ri*** ≤ 16
		Ri			

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

- Manutenzione attrezzature antincendio
- Gestione dei fornitori (contratti, ordini, arrivi, fatture)
- Gestione dei clienti (contratti, ordini, arrivi, fatture)
- Attività di consulenza
- Gestione amministrativa
- Attività di formazione
- Videosorveglianza

Manutenzione attrezzature antincendio

Struttura	• Sede operativa

Personale coinvolto	
Responsabile del trattamento	Sprotetto Michele
Persone autorizzate	Sprotetto Michele, c.f. SPRMHL73T07D643Z • Consultazione • Conservazione
Partners	
Altro	

Processo di trattamento	
Descrizione	Attività di manutenzione delle attrezzature antincendio presso le sedi dei clienti
Fonte dei dati personali	Raccolti direttamente
Base giuridica per il trattamento per dati comuni (art. 6 GDPR)	Consenso Contratto
Base giuridica per il trattamento per dati particolari (art. 9 GDPR)	
Finalità del trattamento	Erogazione del servizio prodotto Programmazione delle attività (pianificazione e monitoraggio del lavoro)
Tipo di dati personali	Beni, proprietà, possessi (proprietà, possessi e locazioni; beni e servizi forniti o ottenuti) Dati identificativi (ragione o denominazione sociale, ovvero nome e cognome delle persone fisiche, indirizzo sede, telefono, fax, e-mail, dati fiscali, ecc.) Dati relativi alla prestazione lavorativa
Categorie di interessati	Clienti ed utenti Condomini
Categorie di destinatari	

Informativa	Si
Profilazione	Non necessario
Dati particolari	Non presenti
Consenso minori	Non necessario
Frequenza trattamento	Semestrale
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	Archivio elettronico
Strutture informatiche di archiviazione	
Dropbox	Struttura esterna
Azienda proprietaria	Dropbox
Personale con diritti di accesso	
Software utilizzati	
Strutture informatiche di backup	
Dropbox	Struttura esterna
Azienda proprietaria	Dropbox
Frequenza di backup	1 giorni
Tempo di storicizzazione	1 giorni
Personale con diritti di accesso	
Note	
Software utilizzati	

VALUTAZIONE DEL LIVELLO DI RISCHIO		
PROBABILITÀ	**CONSEGUENZE**	**LIVELLO DI RISCHIO**
Poco probabile	Trascurabili	Accettabile

MISURE DI SICUREZZA TECNICHE ED ORGANIZZATIVE

- Autorizzazione del singolo incaricato al trattamento e alla modifica dei dati
- Dispositivi antincendio
- E' applicata una gestione della password degli utenti
- E' presenta una politica per la sicurezza e la protezione dei dati
- Impianto elettrico dotato di misure salvavita atte anche ad evitare cortocircuiti e possibili incendi
- Le password sono costituite da almeno otto caratteri alfanumerici
- L'impianto elettrico è certificato ed a norma
- Porte dotate di serratura in tutti i locali contenenti fisicamente le banche dati elettroniche e cartacee
- Sistemi di allarme e di sorveglianza anti-intrusione
- Sono definiti i ruoli e le responsabilità
- Sono definiti i termini di conservazione e le condizioni di impiego dei dati.
- Sono gestiti i back up
- Sono stabiliti programmi di formazione e sensibilizzazione
- Sono utilizzati software antivirus e anti intrusione
- Viene eseguita opportuna manutenzione
- Viene eseguita una regolare formazione del personale
- Adozione di cifratura e anonimizzazione dei dati su stato di salute e vita sessuale
- E' applicata una procedura per la gestione degli accessi
- E' eseguita la DPIA
- I dati sono crittografati

VALUTAZIONE ADEGUATEZZA DELLE MISURE DI SICUREZZA ADOTTATE

MISURE DI SIUREZZA	PERICOLI ASSOCIATI	LIVELLO DI ADEGUATEZZA
Adozione di cifratura e anonimizzazione dei dati su stato di salute e vita sessuale	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)	
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.)	
Dispositivi antincendio	• Agenti fisici (incendio, allagamento, attacchi esterni)	
E' applicata una gestione della password degli utenti	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT) • Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)	
E' applicata una procedura per la gestione degli accessi	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.) • Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti	

	servizio IT)	
E' eseguita la DPIA	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)	
E' presenta una politica per la sicurezza e la protezione dei dati	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.) • Eventi naturali (terremoti, eruzioni vulcaniche, ecc.)	
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.)	
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)	
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.)	

L'impianto elettrico è certificato ed a norma	• Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.) • Agenti fisici (incendio, allagamento, attacchi esterni)	
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.)	
Sistemi di allarme e di sorveglianza anti-intrusione	• Agenti fisici (incendio, allagamento, attacchi esterni) • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • Eventi naturali (terremoti, eruzioni vulcaniche, ecc.)	
Sono definiti i ruoli e le responsabilità	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)	
Sono definiti i termini di conservazione e le condizioni di impiego dei dati.	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)	
Sono gestiti i back up	• Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.) • Agenti fisici (incendio, allagamento, attacchi esterni) • Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)	
Sono stabiliti programmi di formazione e	• Azioni non autorizzate (Errori volontari o involontari, virus, uso	

sensibilizzazione	non autorizzato di strumentazione, ecc.)	
Sono utilizzati software antivirus e anti intrusione	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)	
Viene eseguita opportuna manutenzione	• Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)	
Viene eseguita una regolare formazione del personale	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)	

Nessuna valutazione DPIA

Gestione dei fornitori (contratti, ordini, arrivi, fatture)

Struttura	• Sede operativa

Personale coinvolto	
Responsabile del trattamento	Sprotetto Michele
Persone autorizzate	Sprotetto Michele, c.f. SPRMHL73T07D643Z
Partners	Studio Zucchet, p.iva 12647120158 Servizi e Recapiti SG srl, p.iva 01649460191
Altro	

Processo di trattamento	
Descrizione	Gestore dei contratti di fornitura
Fonte dei dati personali	Raccolti direttamente
Base giuridica per il trattamento per dati comuni (art. 6 GDPR)	Contratto Consenso
Base giuridica per il trattamento per dati particolari (art. 9 GDPR)	
Finalità del trattamento	Gestione dei fornitori (contratti, ordini, arrivi, fatture) Elaborazione, stampa, imbustamento e spedizione delle fatture Adempimento di obblighi fiscali o contabili Gestione del contenzioso (contratti, ordini, arrivi, fatture)

	Operazioni di trasporto (passeggeri e merci)
Tipo di dati personali	Nominativo, indirizzo o altri elementi di identificazione personale (nome, cognome, età, sesso, luogo e data di nascita, indirizzo privato, indirizzo di lavoro) Codice fiscale ed altri numeri di identificazione personale (carte sanitarie) Dati identificativi (ragione o denominazione sociale, ovvero nome e cognome delle persone fisiche, indirizzo sede, telefono, fax, e-mail, dati fiscali, ecc.)
Categorie di interessati	Fornitori
Categorie di destinatari	Società che effettuano il servizio di logistica di magazzino e trasporto Società e imprese Consulenti e liberi professionisti anche in forma associata Responsabili esterni
Informativa	Si
Profilazione	Non necessario
Dati particolari	Si
Consenso minori	Non necessario
Frequenza trattamento	Mensile
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	Archivio elettronico
Strutture informatiche di archiviazione	
Dropbox	Struttura esterna
Azienda proprietaria	Dropbox
Personale con diritti di accesso	
Software utilizzati	
Strutture informatiche di backup	
Dropbox	Struttura esterna
Azienda proprietaria	Dropbox
Frequenza di backup	1 giorni
Tempo di storicizzazione	1 giorni
Personale con diritti di accesso	
Note	
Software utilizzati	

VALUTAZIONE DEL LIVELLO DI RISCHIO		
PROBABILITÀ	**CONSEGUENZE**	**LIVELLO DI RISCHIO**
Poco probabile	Trascurabili	Accettabile

MISURE DI SICUREZZA TECNICHE ED ORGANIZZATIVE
- Sono gestiti i back up - Sono utilizzati software antivirus e anti intrusione - E' applicata una gestione della password degli utenti - Sono definiti i ruoli e le responsabilità - Autorizzazione del singolo incaricato al trattamento e alla modifica dei dati - Dispositivi antincendio

- E' presenta una politica per la sicurezza e la protezione dei dati
- Impianto elettrico dotato di misure salvavita atte anche ad evitare cortocircuiti e possibili incendi
- Le password sono costituite da almeno otto caratteri alfanumerici
- L'impianto elettrico è certificato ed a norma
- Porte dotate di serratura in tutti i locali contenenti fisicamente le banche dati elettroniche e cartacee
- Sistemi di allarme e di sorveglianza anti-intrusione
- Sono definiti i termini di conservazione e le condizioni di impiego dei dati.
- Sono stabiliti programmi di formazione e sensibilizzazione
- Viene eseguita opportuna manutenzione
- Viene eseguita una regolare formazione del personale
- Adozione di cifratura e anonimizzazione dei dati su stato di salute e vita sessuale
- E' applicata una procedura per la gestione degli accessi
- E' eseguita la DPIA
- I dati sono crittografati

VALUTAZIONE ADEGUATEZZA DELLE MISURE DI SICUREZZA ADOTTATE

MISURE DI SIUREZZA	PERICOLI ASSOCIATI	LIVELLO DI ADEGUATEZZA
Adozione di cifratura e anonimizzazione dei dati su stato di salute e vita sessuale	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)	
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.)	
Dispositivi antincendio	• Agenti fisici (incendio, allagamento, attacchi esterni)	
E' applicata una gestione della password degli utenti	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT) • Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica,	

	ecc.)	
E' applicata una procedura per la gestione degli accessi	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.) • Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)	
E' eseguita la DPIA	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)	
E' presenta una politica per la sicurezza e la protezione dei dati	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.) • Eventi naturali (terremoti, eruzioni vulcaniche, ecc.)	
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.)	
Impianto elettrico dotato di misure salvavita atte anche ad evitare	• Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione	

cortocircuiti e possibili incendi	collegamenti di rete, ecc.) • Agenti fisici (incendio, allagamento, attacchi esterni)	
Le password sono costituite da almeno otto caratteri alfanumerici	• Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.) • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)	
L'impianto elettrico è certificato ed a norma	• Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.) • Agenti fisici (incendio, allagamento, attacchi esterni)	
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.)	
Sistemi di allarme e di sorveglianza anti-intrusione	• Agenti fisici (incendio, allagamento, attacchi esterni) • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • Eventi naturali (terremoti, eruzioni vulcaniche, ecc.)	
Sono definiti i ruoli e le responsabilità	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)	
Sono definiti i termini di conservazione e le condizioni di impiego dei dati.	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)	

Sono gestiti i back up	• Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.) • Agenti fisici (incendio, allagamento, attacchi esterni) • Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)	
Sono stabiliti programmi di formazione e sensibilizzazione	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)	
Sono utilizzati software antivirus e anti intrusione	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)	
Viene eseguita opportuna manutenzione	• Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)	
Viene eseguita una regolare formazione del personale	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)	

Nessuna valutazione DPIA

Gestione dei clienti (contratti, ordini, arrivi, fatture)

Struttura	• Sede operativa • Sede legale

Personale coinvolto	
Responsabile del trattamento	Sprotetto Michele
Persone autorizzate	Sprotetto Michele, c.f. SPRMHL73T07D643Z
Partners	Studio Zucchet, p.iva 12647120158

	Servizi e Recapiti SG srl, p.iva 01649460191
Altro	

Processo di trattamento	
Descrizione	Gestore dei contratti di vendita
Fonte dei dati personali	Raccolti direttamente
Base giuridica per il trattamento per dati comuni (art. 6 GDPR)	Contratto Consenso
Base giuridica per il trattamento per dati particolari (art. 9 GDPR)	
Finalità del trattamento	Gestione della clientela (contratti, ordini, spedizioni e fatture) Elaborazione, stampa, imbustamento e spedizione delle fatture Adempimento di obblighi fiscali o contabili Gestione del contenzioso (contratti, ordini, arrivi, fatture) Operazioni di trasporto (passeggeri e merci)
Tipo di dati personali	Nominativo, indirizzo o altri elementi di identificazione personale (nome, cognome, età, sesso, luogo e data di nascita, indirizzo privato, indirizzo di lavoro) Codice fiscale ed altri numeri di identificazione personale (carte sanitarie) Dati identificativi (ragione o denominazione sociale, ovvero nome e cognome delle persone fisiche, indirizzo sede, telefono, fax, e-mail, dati fiscali, ecc.)
Categorie di interessati	Condomini Clienti ed utenti Potenziali clienti
Categorie di destinatari	Società che effettuano il servizio di logistica di magazzino e trasporto Clienti ed utenti Società e imprese Consulenti e liberi professionisti anche in forma associata Responsabili esterni
Informativa	Si
Profilazione	Non necessario
Dati particolari	Si
Consenso minori	Non necessario
Frequenza trattamento	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	Software gestionale Archivio elettronico
Strutture informatiche di archiviazione	
Invoicex	Struttura esterna
Azienda proprietaria	Invoicex Enterprice
Personale con diritti di accesso	Sprotetto Michele, c.f. SPRMHL73T07D643Z Amalia Ciaramitaro, c.f. CRMMLA90M70G273Y
Software utilizzati	- Invoicex
Dropbox	Struttura esterna
Azienda proprietaria	Dropbox
Personale con diritti di accesso	

Software utilizzati	
Strutture informatiche di backup	
Invoicex	Struttura esterna
Azienda proprietaria	Invoicex Enterprice
Frequenza di backup	1 giorni
Tempo di storicizzazione	1 giorni
Personale con diritti di accesso	Sprotetto Michele, c.f. SPRMHL73T07D643Z Amalia Ciaramitaro, c.f. CRMMLA90M70G273Y
Note	
Software utilizzati	- Invoicex
Dropbox	Struttura esterna
Azienda proprietaria	Dropbox
Frequenza di backup	1 giorni
Tempo di storicizzazione	1 giorni
Personale con diritti di accesso	
Note	
Software utilizzati	

VALUTAZIONE DEL LIVELLO DI RISCHIO		
PROBABILITÀ	**CONSEGUENZE**	**LIVELLO DI RISCHIO**
Poco probabile	Trascurabili	Accettabile

MISURE DI SICUREZZA TECNICHE ED ORGANIZZATIVE
- Sono gestiti i back up - Sono utilizzati software antivirus e anti intrusione - E' applicata una gestione della password degli utenti - Sono definiti i ruoli e le responsabilità - Autorizzazione del singolo incaricato al trattamento e alla modifica dei dati - Dispositivi antincendio - E' presenta una politica per la sicurezza e la protezione dei dati - Impianto elettrico dotato di misure salvavita atte anche ad evitare cortocircuiti e possibili incendi - Le password sono costituite da almeno otto caratteri alfanumerici - L'impianto elettrico è certificato ed a norma - Porte dotate di serratura in tutti i locali contenenti fisicamente le banche dati elettroniche e cartacee - Sistemi di allarme e di sorveglianza anti-intrusione - Sono definiti i termini di conservazione e le condizioni di impiego dei dati. - Sono stabiliti programmi di formazione e sensibilizzazione - Viene eseguita opportuna manutenzione - Viene eseguita una regolare formazione del personale - Adozione di cifratura e anonimizzazione dei dati su stato di salute e vita sessuale - E' applicata una procedura per la gestione degli accessi - E' eseguita la DPIA - I dati sono crittografati

VALUTAZIONE ADEGUATEZZA DELLE MISURE DI SICUREZZA ADOTTATE

MISURE DI SIUREZZA	PERICOLI ASSOCIATI	LIVELLO DI ADEGUATEZZA
Adozione di cifratura e	• Azioni non autorizzate (Errori	

anonimizzazione dei dati su stato di salute e vita sessuale	volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)	
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.)	
Dispositivi antincendio	• Agenti fisici (incendio, allagamento, attacchi esterni)	
E' applicata una gestione della password degli utenti	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT) • Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)	
E' applicata una procedura per la gestione degli accessi	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.) • Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)	
E' eseguita la DPIA	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • Compromissione informazioni (intercettazioni, rivelazione	

	informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)	
E' presenta una politica per la sicurezza e la protezione dei dati	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.) • Eventi naturali (terremoti, eruzioni vulcaniche, ecc.)	
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.)	
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)	
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.)	
L'impianto elettrico è certificato ed a norma	• Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.) • Agenti fisici (incendio, allagamento, attacchi esterni)	

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.)	
Sistemi di allarme e di sorveglianza anti-intrusione	• Agenti fisici (incendio, allagamento, attacchi esterni) • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • Eventi naturali (terremoti, eruzioni vulcaniche, ecc.)	
Sono definiti i ruoli e le responsabilità	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)	
Sono definiti i termini di conservazione e le condizioni di impiego dei dati.	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)	
Sono gestiti i back up	• Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.) • Agenti fisici (incendio, allagamento, attacchi esterni) • Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)	
Sono stabiliti programmi di formazione e sensibilizzazione	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)	
Sono utilizzati software antivirus e anti intrusione	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • Compromissione informazioni	

	(intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)	
Viene eseguita opportuna manutenzione	• Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)	
Viene eseguita una regolare formazione del personale	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)	

Nessuna valutazione DPIA

Attività di consulenza

Struttura	• Sede operativa

Personale coinvolto	
Responsabile del trattamento	Sprotetto Michele
Persone autorizzate	Sprotetto Michele, c.f. SPRMHL73T07D643Z Amalia Ciaramitaro, c.f. CRMMLA90M70G273Y
Partners	ABE Sicurezza e servizi per imprese S.r.l., p.iva 03760270987 Studio di Medicina del Lavoro D.ssa Marina Morari, p.iva 03305610960, nella persona di Marina Morari
Altro	

Processo di trattamento	
Descrizione	Attività di supporto alle imprese attraverso servizi di consulenza
Fonte dei dati personali	Raccolti direttamente
Base giuridica per il trattamento per dati comuni (art. 6 GDPR)	Contratto Consenso
Base giuridica per il trattamento per dati particolari (art. 9 GDPR)	
Finalità del trattamento	Attività di consulenza Erogazione del servizio prodotto Programmazione delle attività (pianificazione e monitoraggio del lavoro) Gestione l. 81/2008 Igiene e sicurezza del lavoro
Tipo di dati personali	Personali Dati identificativi (ragione o denominazione sociale, ovvero nome e cognome delle persone fisiche, indirizzo sede, telefono, fax, e-mail, dati fiscali, ecc.)

Categorie di interessati	Potenziali clienti Clienti ed utenti
Categorie di destinatari	Persone autorizzate Responsabili esterni
Informativa	Si
Profilazione	Non necessario
Dati particolari	Non presenti
Consenso minori	Non necessario
Frequenza trattamento	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	Archivio elettronico Software gestionale
Strutture informatiche di archiviazione	
Dropbox	Struttura esterna
Azienda proprietaria	Dropbox
Personale con diritti di accesso	
Software utilizzati	
Strutture informatiche di backup	
Dropbox	Struttura esterna
Azienda proprietaria	Dropbox
Frequenza di backup	1 giorni
Tempo di storicizzazione	1 giorni
Personale con diritti di accesso	
Note	
Software utilizzati	

VALUTAZIONE DEL LIVELLO DI RISCHIO		
PROBABILITÀ	**CONSEGUENZE**	**LIVELLO DI RISCHIO**
Poco probabile	Trascurabili	Accettabile

MISURE DI SICUREZZA TECNICHE ED ORGANIZZATIVE

- Autorizzazione del singolo incaricato al trattamento e alla modifica dei dati
- Viene eseguita opportuna manutenzione
- Sono gestiti i back up
- I sistemi di autorizzazione prevedono: la presenza di diversi profili di autorizzazione, l'individuazione preventiva per incaricato, l'individuazione preventiva per classi omogenee di incaricati, la verifica almeno annuale dei profili
- Sono utilizzati software antivirus e anti intrusione
- Sono definiti i ruoli e le responsabilità
- Dispositivi antincendio
- E' applicata una gestione della password degli utenti
- E' presenta una politica per la sicurezza e la protezione dei dati
- Impianto elettrico dotato di misure salvavita atte anche ad evitare cortocircuiti e possibili incendi
- Le password sono costituite da almeno otto caratteri alfanumerici
- L'impianto elettrico è certificato ed a norma
- Porte dotate di serratura in tutti i locali contenenti fisicamente le banche dati elettroniche e cartacee

- Sistemi di allarme e di sorveglianza anti-intrusione
- Sono definiti i termini di conservazione e le condizioni di impiego dei dati.
- Sono stabiliti programmi di formazione e sensibilizzazione
- Viene eseguita una regolare formazione del personale
- Adozione di cifratura e anonimizzazione dei dati su stato di salute e vita sessuale
- E' applicata una procedura per la gestione degli accessi
- E' eseguita la DPIA
- I dati sono crittografati

VALUTAZIONE ADEGUATEZZA DELLE MISURE DI SICUREZZA ADOTTATE

MISURE DI SIUREZZA	PERICOLI ASSOCIATI	LIVELLO DI ADEGUATEZZA
Adozione di cifratura e anonimizzazione dei dati su stato di salute e vita sessuale	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)	
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.)	
Dispositivi antincendio	• Agenti fisici (incendio, allagamento, attacchi esterni)	
E' applicata una gestione della password degli utenti	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT) • Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)	
E' applicata una procedura per la gestione degli accessi	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)	

	• Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.) • Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)	
E' eseguita la DPIA	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)	
E' presenta una politica per la sicurezza e la protezione dei dati	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.) • Eventi naturali (terremoti, eruzioni vulcaniche, ecc.)	
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.)	
I sistemi di autorizzazione prevedono: la presenza di diversi profili di autorizzazione, l'individuazione preventiva per incaricato, l'individuazione preventiva per classi omogenee di incaricati, la verifica	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)	

almeno annuale dei profili		
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)	
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.)	
L'impianto elettrico è certificato ed a norma	• Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.) • Agenti fisici (incendio, allagamento, attacchi esterni)	
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.)	
Sistemi di allarme e di sorveglianza anti-intrusione	• Agenti fisici (incendio, allagamento, attacchi esterni) • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • Eventi naturali (terremoti, eruzioni vulcaniche, ecc.)	
Sono definiti i ruoli e le responsabilità	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)	
Sono definiti i termini di conservazione e le condizioni di impiego dei dati.	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • Compromissione informazioni (intercettazioni, rivelazione	

	informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)	
Sono gestiti i back up	• Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.) • Agenti fisici (incendio, allagamento, attacchi esterni) • Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)	
Sono stabiliti programmi di formazione e sensibilizzazione	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)	
Sono utilizzati software antivirus e anti intrusione	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)	
Viene eseguita opportuna manutenzione	• Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)	
Viene eseguita una regolare formazione del personale	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)	

Nessuna valutazione DPIA

Gestione amministrativa

Struttura	• Sede operativa

Personale coinvolto

Responsabile del trattamento	Sprotetto Michele
Persone autorizzate	Sprotetto Michele, c.f. SPRMHL73T07D643Z
Partners	Studio Zucchet, p.iva 12647120158
Altro	

Processo di trattamento	
Descrizione	Politica aziendale che riguarda la gestione del personale in merito a: assunzione, attività formative, valutazioni, pagamenti, ecc. E tutte le attività in ambito amministrativo della società
Fonte dei dati personali	Raccolti direttamente
Base giuridica per il trattamento per dati comuni (art. 6 GDPR)	Consenso Contratto
Base giuridica per il trattamento per dati particolari (art. 9 GDPR)	Consenso Contratto
Finalità del trattamento	Trattamento giuridico ed economico del personale Reclutamento, selezione, valutazione e monitoraggio del personale: test attitudinali Reclutamento, selezione, valutazione e monitoraggio del personale: formazione professionale Gestione del contenzioso (contratti, ordini, arrivi, fatture) Gestione del personale Reclutamento, selezione, valutazione e monitoraggio del personale: collocazione personale dipendente all'estero
Tipo di dati personali	Personali Dati identificativi (ragione o denominazione sociale, ovvero nome e cognome delle persone fisiche, indirizzo sede, telefono, fax, e-mail, dati fiscali, ecc.) Codice fiscale ed altri numeri di identificazione personale (carte sanitarie) 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	Dipendenti
Categorie di destinatari	Altre amministrazioni pubbliche Enti pubblici economici Società e imprese Clienti ed utenti Enti previdenziali ed assistenziali Responsabili esterni
Informativa	Si
Profilazione	Non necessario
Dati particolari	Si
Consenso minori	Non necessario
Frequenza trattamento	Mensile
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	Archivio elettronico
Strutture informatiche di archiviazione	
Dropbox	Struttura esterna

Azienda proprietaria	Dropbox
Personale con diritti di accesso	
Software utilizzati	
Strutture informatiche di backup	
Dropbox	Struttura esterna
Azienda proprietaria	Dropbox
Frequenza di backup	1 giorni
Tempo di storicizzazione	1 giorni
Personale con diritti di accesso	
Note	
Software utilizzati	

VALUTAZIONE DEL LIVELLO DI RISCHIO		
PROBABILITÀ	**CONSEGUENZE**	**LIVELLO DI RISCHIO**
Poco probabile	Trascurabili	Accettabile

MISURE DI SICUREZZA TECNICHE ED ORGANIZZATIVE

- Viene eseguita opportuna manutenzione
- Sono gestiti i back up
- Sono utilizzati software antivirus e anti intrusione
- Adozione di cifratura e anonimizzazione dei dati su stato di salute e vita sessuale
- Autorizzazione del singolo incaricato al trattamento e alla modifica dei dati
- Dispositivi antincendio
- E' applicata una gestione della password degli utenti
- E' applicata una procedura per la gestione degli accessi
- E' presenta una politica per la sicurezza e la protezione 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
- L'impianto elettrico è certificato ed a norma
- Porte dotate di serratura in tutti i locali contenenti fisicamente le banche dati elettroniche e cartacee
- Sistemi di allarme e di sorveglianza anti-intrusione
- Sono definiti i ruoli e le responsabilità
- Sono stabiliti programmi di formazione e sensibilizzazione
- Viene eseguita una regolare formazione del personale

VALUTAZIONE ADEGUATEZZA DELLE MISURE DI SICUREZZA ADOTTATE

MISURE DI SIUREZZA	PERICOLI ASSOCIATI	LIVELLO DI ADEGUATEZZA
Adozione di cifratura e anonimizzazione dei dati su stato di salute e vita sessuale	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica,	

	ecc.)	
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.)	
Dispositivi antincendio	• Agenti fisici (incendio, allagamento, attacchi esterni)	
E' applicata una gestione della password degli utenti	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT) • Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)	
E' applicata una procedura per la gestione degli accessi	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.) • Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)	
E' eseguita la DPIA	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)	
E' presenta una politica per la sicurezza e la protezione dei dati	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione,	

	ecc.) • Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.) • Eventi naturali (terremoti, eruzioni vulcaniche, ecc.)	
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.)	
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)	
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.)	
L'impianto elettrico è certificato ed a norma	• Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.) • Agenti fisici (incendio, allagamento, attacchi esterni)	
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.)	
Sistemi di allarme e di sorveglianza anti-intrusione	• Agenti fisici (incendio, allagamento, attacchi esterni)	

	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • Eventi naturali (terremoti, eruzioni vulcaniche, ecc.)	
Sono definiti i ruoli e le responsabilità	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)	
Sono gestiti i back up	• Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.) • Agenti fisici (incendio, allagamento, attacchi esterni) • Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)	
Sono stabiliti programmi di formazione e sensibilizzazione	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)	
Sono utilizzati software antivirus e anti intrusione	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)	
Viene eseguita opportuna manutenzione	• Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)	
Viene eseguita una regolare formazione del personale	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)	

Nessuna valutazione DPIA

Attività di formazione

Struttura	• Sede operativa

Personale coinvolto	
Responsabile del trattamento	Sprotetto Michele
Persone autorizzate	Sprotetto Michele, c.f. SPRMHL73T07D643Z Amalia Ciaramitaro, c.f. CRMMLA90M70G273Y
Partners	ABE Sicurezza e servizi per imprese S.r.l., p.iva 03760270987 Studio di Medicina del Lavoro D.ssa Marina Morari, p.iva 03305610960, nella persona di Marina Morari
Altro	

Processo di trattamento	
Descrizione	Percorsi formativi personalizzati
Fonte dei dati personali	Raccolti direttamente
Base giuridica per il trattamento per dati comuni (art. 6 GDPR)	Contratto Consenso
Base giuridica per il trattamento per dati particolari (art. 9 GDPR)	
Finalità del trattamento	Erogazione del servizio prodotto
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.) Personali
Categorie di interessati	Clienti ed utenti
Categorie di destinatari	Responsabili esterni Responsabili interni
Informativa	Si
Profilazione	Non necessario
Dati particolari	Non presenti
Consenso minori	Non necessario
Frequenza trattamento	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	Archivio elettronico
Strutture informatiche di archiviazione	
Dropbox	Struttura esterna
Azienda proprietaria	Dropbox
Personale con diritti di accesso	
Software utilizzati	
Strutture informatiche di backup	
Dropbox	Struttura esterna

Azienda proprietaria	Dropbox
Frequenza di backup	1 giorni
Tempo di storicizzazione	1 giorni
Personale con diritti di accesso	
Note	
Software utilizzati	

VALUTAZIONE DEL LIVELLO DI RISCHIO		
PROBABILITÀ	**CONSEGUENZE**	**LIVELLO DI RISCHIO**
Poco probabile	Trascurabili	Accettabile

MISURE DI SICUREZZA TECNICHE ED ORGANIZZATIVE
- Viene eseguita opportuna manutenzione - Sono gestiti i back up - I sistemi di autorizzazione prevedono: la presenza di diversi profili di autorizzazione, l'individuazione preventiva per incaricato, l'individuazione preventiva per classi omogenee di incaricati, la verifica almeno annuale dei profili - Sono utilizzati software antivirus e anti intrusione - Sono definiti i ruoli e le responsabilità - Adozione di cifratura e anonimizzazione dei dati su stato di salute e vita sessuale - Autorizzazione del singolo incaricato al trattamento e alla modifica dei dati - Dispositivi antincendio - E' applicata una gestione della password degli utenti - E' applicata una procedura per la gestione degli accessi - E' presenta una politica per la sicurezza e la protezione 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 - L'impianto elettrico è certificato ed a norma - Porte dotate di serratura in tutti i locali contenenti fisicamente le banche dati elettroniche e cartacee - Sistemi di allarme e di sorveglianza anti-intrusione - Sono stabiliti programmi di formazione e sensibilizzazione - Viene eseguita una regolare formazione del personale - Sono definiti i termini di conservazione e le condizioni di impiego dei dati.

VALUTAZIONE ADEGUATEZZA DELLE MISURE DI SICUREZZA ADOTTATE

MISURE DI SIUREZZA	PERICOLI ASSOCIATI	LIVELLO DI ADEGUATEZZA
Adozione di cifratura e anonimizzazione dei dati su stato di salute e vita sessuale	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)	

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.)	
Dispositivi antincendio	• Agenti fisici (incendio, allagamento, attacchi esterni)	
E' applicata una gestione della password degli utenti	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT) • Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)	
E' applicata una procedura per la gestione degli accessi	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.) • Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)	
E' eseguita la DPIA	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)	
E' presenta una politica per la sicurezza e la protezione dei dati	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)	

	• Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.) • Eventi naturali (terremoti, eruzioni vulcaniche, ecc.)	
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.)	
I sistemi di autorizzazione prevedono: la presenza di diversi profili di autorizzazione, l'individuazione preventiva per incaricato, l'individuazione preventiva per classi omogenee di incaricati, la verifica almeno annuale dei profili	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)	
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)	
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.)	
L'impianto elettrico è certificato ed a norma	• Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.) • Agenti fisici (incendio,	

	allagamento, attacchi esterni)	
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.)	
Sistemi di allarme e di sorveglianza anti-intrusione	• Agenti fisici (incendio, allagamento, attacchi esterni) • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • Eventi naturali (terremoti, eruzioni vulcaniche, ecc.)	
Sono definiti i ruoli e le responsabilità	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)	
Sono definiti i termini di conservazione e le condizioni di impiego dei dati.	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)	
Sono gestiti i back up	• Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.) • Agenti fisici (incendio, allagamento, attacchi esterni) • Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)	
Sono stabiliti programmi di formazione e sensibilizzazione	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)	
Sono utilizzati software antivirus e anti intrusione	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione,	

	ecc.) • Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)	
Viene eseguita opportuna manutenzione	• Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)	
Viene eseguita una regolare formazione del personale	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)	

Nessuna valutazione DPIA

Videosorveglianza

Struttura	• Sede operativa

Personale coinvolto	
Responsabile del trattamento	Sprotetto Michele
Persone autorizzate	Sprotetto Michele, c.f. SPRMHL73T07D643Z
Partners	Verisure, p.iva PI: IT12454611000
Altro	

Processo di trattamento	
Descrizione	Sistemi di rilevazione delle immagini e delle intrusioni
Fonte dei dati personali	Raccolti direttamente
Base giuridica per il trattamento per dati comuni (art. 6 GDPR)	Contratto Consenso
Base giuridica per il trattamento per dati particolari (art. 9 GDPR)	Consenso Salvaguardia degli interessi vitali
Finalità del trattamento	Protezione e incolumità degli individui Protezione della proprietà Rilevazione, prevenzione e controllo delle infrazioni Acquisizione di prove Difesa del suolo, tutela dell'ambiente e della sicurezza della popolazione
Tipo di dati personali	Particolari (sensibili) Personali Dati sul comportamento (creazione di profili di utenti, consumatori, contribuenti, ecc.; profili della personalità e dei tratti caratteriali)
Categorie di interessati	Soggetti o organismi pubblici Dipendenti

	Clienti ed utenti
Categorie di destinatari	Autorità di vigilanza e controllo Uffici giudiziari Forze di polizia Datore di lavoro Responsabili esterni
Informativa	Si
Profilazione	Non necessario
Dati particolari	Si
Consenso minori	Non necessario
Frequenza trattamento	Giornaliera
Termine cancellazione dati	I dati saranno trattati per tutto il tempo necessario allo svolgimento del rapporto commerciale in essere e per i successivi dieci anni dalla data di acquisizione degli stessi.
Trasferimento dati (paesi terzi)	No
Autorizzazione del Garante	Non presente

Modalità di elaborazione dati: Informatica	
Strumenti	Archivio elettronico
Strutture informatiche di archiviazione	
Strutture informatiche di backup	

VALUTAZIONE DEL LIVELLO DI RISCHIO		
PROBABILITÀ	**CONSEGUENZE**	**LIVELLO DI RISCHIO**
Poco probabile	Trascurabili	Accettabile

MISURE DI SICUREZZA TECNICHE ED ORGANIZZATIVE
- Viene eseguita opportuna manutenzione - Sono gestiti i back up - L'impianto elettrico è certificato ed a norma - Sono utilizzati software antivirus e anti intrusione

VALUTAZIONE ADEGUATEZZA DELLE MISURE DI SICUREZZA ADOTTATE

MISURE DI SIUREZZA	PERICOLI ASSOCIATI	LIVELLO DI ADEGUATEZZA
L'impianto elettrico è certificato ed a norma	• Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.) • Agenti fisici (incendio, allagamento, attacchi esterni)	
Sono gestiti i back up	• Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.) • Agenti fisici (incendio,	

	allagamento, attacchi esterni) • Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)	
Sono utilizzati software antivirus e anti intrusione	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)	
Viene eseguita opportuna manutenzione	• Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)	

Nessuna valutazione DPIA