



REGISTRO DELLE ATTIVITA' DI TRATTAMENTO DATI PERSONALI

ai sensi dell'art. 30 del GDPR 2016/679 e della normativa nazionale in vigore

Azienda/Organizzazione

LICEO CARMINE SYLOS AP

REGISTRO

DSGA

SEDE

Sede Centrale P.zza C. Sylos
Piazza Carmine Sylos 6, 70032
Bitonto - BA

Data revisione: 23/11/2022

Il presente registro è una rappresentazione dell'organizzazione sotto il profilo delle attività di trattamento dati. Esso ha lo scopo di informare, dare consapevolezza e condivisione interna del processo di gestione del dato.

Ai sensi dell'art. 30 del GDPR, il Registro riporta le seguenti informazioni:

- dati di contatto del titolare del trattamento e, dove applicabile, del contitolare del trattamento e del Responsabile della protezione dei dati;
- **finalità del trattamento**, le finalità per le quali sono trattati tali dati;
- categorie di interessati;
- categorie di dati personali;
- categorie di destinatari a cui i dati personali sono stati o saranno comunicati;
- ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale;
- ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
- ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative.

Titolare trattamento dati	Cognome	VITELLI
	Nome	FRANCESCA ROSARIA
	E-mail	
	PEC	
	N° telefono	

Responsabile trattamento dati	Cognome	SCARAGGI
	Nome	MARIA PIA
	E-mail	
	PEC	
	N° telefono	

Responsabile protezione dati (DPO)	Ragione sociale	LABSYSTEM SRL
	P. Iva	06562980729
	E-mail	
	PEC	
	N° telefono	

VALUTAZIONE DEL RISCHIO E MATRICE DI RISCHIO

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:

P r o b a b i l i t à	5	5	10	15	20	25
	4	4	8	12	16	20
	3	3	6	9	12	15
	2	2	4	6	8	10
	1	1	2	3	4	5
		1	2	3	4	5
Conseguenze						

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

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

ELENCO ATTIVITA' INSERITE NEL REGISTRO

- Attività formazione alunni
- Scuole ed Università
- Gestione del personale
- Gestione dei fornitori (contratti, ordini, arrivi, fatture)

TRATTAMENTO: Attività formazione alunni

Scheda creata in data: 23/11/2022

Ultimo aggiornamento avvenuto in data: 23/11/2022

Struttura	<ul style="list-style-type: none"> • Amministrazione • Sede operativa
------------------	---

Personale coinvolto

Persone autorizzate	
Partners - Responsabili esterni	
Altro	

Processo di trattamento

Descrizione	Politica Amministrazioni Pubbliche che riguarda la gestione dei dati Alunni in merito a: attività formative, valutazioni, pagamenti, ecc
Fonte dei dati personali	Raccolti direttamente
Base giuridica per il trattamento per dati comuni (art. 6 GDPR)	Consenso
Base giuridica per il trattamento per dati particolari (art. 9 GDPR)	Consenso
Finalità del trattamento	Accertamento e riscossione di tasse e imposte Acquisizione di prove Attività sportive Istituzione ed assistenza scolastica
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.) Codice fiscale ed altri numeri di identificazione personale (carte sanitarie) Dati relativi alla famiglia e a situazioni personali (stato civile, minori, figli, soggetti a carico, consanguinei, altri appartenenti al nucleo familiare)
Categorie di interessati	Alunni Familiari dell'interessato
Categorie di destinatari	Amministrazioni Pubbliche Familiari dell'interessato Interessati
Informativa	Si
Profilazione	Non presente
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)	Non presente

Modalità di elaborazione dati: Mista - elettronica e cartacea

Strumenti	Software gestionale
------------------	---------------------

	Registro elettronico Spaggiari
Archiviazione	Armadi Blindati
Strutture informatiche di archiviazione	
Strutture informatiche di backup	

VALUTAZIONE DEL LIVELLO DI RISCHIO		
PROBABILITÀ	CONSEGUENZE	LIVELLO DI RISCHIO
Poco probabile	Marginali	Medio-basso

MISURE DI SICUREZZA TECNICHE ED ORGANIZZATIVE

- E' applicata una gestione della password degli utenti	
Pericoli associati	Rischi
Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)	<ul style="list-style-type: none"> - 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.)	<ul style="list-style-type: none"> - 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.)	<ul style="list-style-type: none"> - Perdita - Distruzione non autorizzata - Modifica non autorizzata

- E' presente una politica per la sicurezza e la protezione dei dati	
Pericoli associati	Rischi
Eventi naturali (terremoti, eruzioni vulcaniche, ecc.)	<ul style="list-style-type: none"> - Perdita - Distruzione non autorizzata
Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)	<ul style="list-style-type: none"> - 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.)	<ul style="list-style-type: none"> - Perdita - Distruzione non autorizzata - Modifica non autorizzata

- I dati sono crittografati	
Pericoli associati	Rischi
Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)	<ul style="list-style-type: none"> - 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.)	<ul style="list-style-type: none"> - Perdita - Distruzione non autorizzata - Modifica non autorizzata
---	--

- 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

Pericoli associati	Rischi
Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)	<ul style="list-style-type: none"> - Perdita - Distruzione non autorizzata - Modifica non autorizzata

- Le password sono modificate ogni 3 mesi

Pericoli associati	Rischi
Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)	<ul style="list-style-type: none"> - 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.)	<ul style="list-style-type: none"> - Perdita - Distruzione non autorizzata - Modifica non autorizzata

- Sono applicate regole per la gestione delle password.

Pericoli associati	Rischi
Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)	<ul style="list-style-type: none"> - 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.)	<ul style="list-style-type: none"> - Perdita - Distruzione non autorizzata - Modifica non autorizzata

- Sono gestiti i back up

Pericoli associati	Rischi
Eventi naturali (terremoti, eruzioni vulcaniche, ecc.)	<ul style="list-style-type: none"> - Perdita - Distruzione non autorizzata
Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)	<ul style="list-style-type: none"> - Perdita - Distruzione non autorizzata - Modifica non autorizzata - Divulgazione non autorizzata - Accesso dati non autorizzato
Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.)	<ul style="list-style-type: none"> - Perdita - Distruzione non autorizzata - Modifica non autorizzata - Divulgazione non autorizzata - Accesso dati non autorizzato
Agenti fisici (incendio, allagamento, attacchi esterni)	<ul style="list-style-type: none"> - Perdita

	- Distruzione non autorizzata
--	-------------------------------

- Sono utilizzati software antivirus e anti intrusione

Pericoli associati	Rischi
Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)	<ul style="list-style-type: none"> - 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.)	<ul style="list-style-type: none"> - Perdita - Distruzione non autorizzata - Modifica non autorizzata

- Viene eseguita opportuna manutenzione

Pericoli associati	Rischi
Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)	<ul style="list-style-type: none"> - Perdita - Distruzione non autorizzata - Modifica non autorizzata - Divulgazione non autorizzata - Accesso dati non autorizzato

TRATTAMENTO: Scuole ed Università
 Scheda creata in data: 23/11/2022
 Ultimo aggiornamento avvenuto in data: 23/11/2022

Struttura	<ul style="list-style-type: none"> • Amministrazione • Sede operativa
------------------	---

Personale coinvolto	
Persone autorizzate	
Partners - Responsabili esterni	
Altro	

Processo di trattamento	
Descrizione	Trattamento di dati personali dei dipendenti: Docenti, Ricercatori, Dirigenti, Tecnici ed Amministrativi
Fonte dei dati personali	Raccolti direttamente
Base giuridica per il trattamento per dati comuni (art. 6 GDPR)	Consenso
Base giuridica per il trattamento per dati particolari (art. 9 GDPR)	Consenso
Finalità del trattamento	Contratto di assunzione Libri ed altre attività editoriali Istituzione ed assistenza scolastica Reclutamento, selezione, valutazione e monitoraggio del personale: test attitudinali Igiene e sicurezza del lavoro
Tipo di dati personali	Curriculum di studi e accademico, pubblicazioni, articoli, monografie, relazioni, materiale audiovisivo, titoli di studio, ecc. 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 Codice fiscale ed altri numeri di identificazione personale (carte sanitarie) Personalità
Categorie di interessati	Docenti Familiari dell'interessato Collaboratori Dipendenti
Categorie di destinatari	Soggetti che svolgono attività di archiviazione della documentazione Familiari dell'interessato Datore di lavoro Associazioni ed enti locali Amministrazioni Pubbliche
Informativa	Si
Profilazione	Non presente
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)	Non presente

Modalità di elaborazione dati: Mista - elettronica e cartacea

Strumenti	Software gestionale
Archiviazione	
Strutture informatiche di archiviazione	
Strutture informatiche di backup	

VALUTAZIONE DEL LIVELLO DI RISCHIO

PROBABILITÀ	CONSEGUENZE	LIVELLO DI RISCHIO
Poco probabile	Marginali	Medio-basso

MISURE DI SICUREZZA TECNICHE ED ORGANIZZATIVE

- E' applicata una gestione della password degli utenti	
Pericoli associati	Rischi
Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)	<ul style="list-style-type: none"> - 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.)	<ul style="list-style-type: none"> - 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.)	<ul style="list-style-type: none"> - Perdita - Distruzione non autorizzata - Modifica non autorizzata

- E' presente una politica per la sicurezza e la protezione dei dati

Pericoli associati	Rischi
Eventi naturali (terremoti, eruzioni vulcaniche, ecc.)	- Perdita - Distruzione non autorizzata
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

- I dati sono crittografati

Pericoli associati	Rischi
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

- 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

Pericoli associati	Rischi
Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)	- Perdita - Distruzione non autorizzata - Modifica non autorizzata

- Le password sono modificate ogni 3 mesi

Pericoli associati	Rischi
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

- Sono applicate regole per la gestione delle password.

Pericoli associati	Rischi
Compromissione informazioni (intercettazioni,	- Perdita

rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)	<ul style="list-style-type: none"> - 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.)	<ul style="list-style-type: none"> - Perdita - Distruzione non autorizzata - Modifica non autorizzata

- Sono definiti i ruoli e le responsabilità	
Pericoli associati	Rischi
Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)	<ul style="list-style-type: none"> - Perdita - Distruzione non autorizzata - Modifica non autorizzata

- Sono gestiti i back up	
Pericoli associati	Rischi
Eventi naturali (terremoti, eruzioni vulcaniche, ecc.)	<ul style="list-style-type: none"> - Perdita - Distruzione non autorizzata
Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)	<ul style="list-style-type: none"> - Perdita - Distruzione non autorizzata - Modifica non autorizzata - Divulgazione non autorizzata - Accesso dati non autorizzato
Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.)	<ul style="list-style-type: none"> - Perdita - Distruzione non autorizzata - Modifica non autorizzata - Divulgazione non autorizzata - Accesso dati non autorizzato
Agenti fisici (incendio, allagamento, attacchi esterni)	<ul style="list-style-type: none"> - Perdita - Distruzione non autorizzata

- Sono utilizzati software antivirus e anti intrusione	
Pericoli associati	Rischi
Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)	<ul style="list-style-type: none"> - 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.)	<ul style="list-style-type: none"> - Perdita - Distruzione non autorizzata - Modifica non autorizzata

- Viene eseguita opportuna manutenzione	
Pericoli associati	Rischi
Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)	<ul style="list-style-type: none"> - Perdita - Distruzione non autorizzata - Modifica non autorizzata - Divulgazione non autorizzata - Accesso dati non autorizzato

TRATTAMENTO: Gestione del personale

Scheda creata in data: 23/11/2022

Ultimo aggiornamento avvenuto in data: 23/11/2022

Struttura	<ul style="list-style-type: none"> • Amministrazione • Sede operativa
-----------	---

Personale coinvolto	
Persone autorizzate	
Partners - Responsabili esterni	
Altro	

Processo di trattamento	
Descrizione	Politica aziendale che riguarda la gestione del personale in merito a: assunzione, attività formative, valutazioni, pagamenti, ecc
Fonte dei dati personali	Raccolti direttamente
Base giuridica per il trattamento per dati comuni (art. 6 GDPR)	Consenso
Base giuridica per il trattamento per dati particolari (art. 9 GDPR)	Consenso
Finalità del trattamento	Reclutamento, selezione, valutazione e monitoraggio del personale: formazione professionale Gestione del contenzioso (contratti, ordini, arrivi, fatture) Gestione del personale
Tipo di dati personali	Personalì 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	Docenti Collaboratori Dipendenti
Categorie di destinatari	Enti pubblici economici Società e imprese Enti previdenziali ed assistenziali Amministrazioni Pubbliche
Informativa	Si
Profilazione	Non presente
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)	Non presente

Modalità di elaborazione dati: Mista - elettronica e cartacea	
Strumenti	Software gestionale
Archiviazione	Armadi Blindati

Strutture informatiche di archiviazione**Strutture informatiche di backup****VALUTAZIONE DEL LIVELLO DI RISCHIO**

PROBABILITÀ	CONSEGUENZE	LIVELLO DI RISCHIO
Poco probabile	Marginali	Medio-basso

MISURE DI SICUREZZA TECNICHE ED ORGANIZZATIVE**- E' applicata una gestione della password degli utenti**

Pericoli associati	Rischi
Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)	<ul style="list-style-type: none"> - 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.)	<ul style="list-style-type: none"> - 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.)	<ul style="list-style-type: none"> - Perdita - Distruzione non autorizzata - Modifica non autorizzata

- E' presente una politica per la sicurezza e la protezione dei dati

Pericoli associati	Rischi
Eventi naturali (terremoti, eruzioni vulcaniche, ecc.)	<ul style="list-style-type: none"> - Perdita - Distruzione non autorizzata
Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)	<ul style="list-style-type: none"> - 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.)	<ul style="list-style-type: none"> - Perdita - Distruzione non autorizzata - Modifica non autorizzata

- I dati sono crittografati

Pericoli associati	Rischi
Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)	<ul style="list-style-type: none"> - 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.)	<ul style="list-style-type: none"> - Perdita - Distruzione non autorizzata

	- Modifica non autorizzata
--	----------------------------

- 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

Pericoli associati	Rischi
Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)	<ul style="list-style-type: none"> - Perdita - Distruzione non autorizzata - Modifica non autorizzata

- Le password sono modificate ogni 3 mesi

Pericoli associati	Rischi
Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)	<ul style="list-style-type: none"> - 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.)	<ul style="list-style-type: none"> - Perdita - Distruzione non autorizzata - Modifica non autorizzata

- Sono applicate regole per la gestione delle password.

Pericoli associati	Rischi
Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)	<ul style="list-style-type: none"> - 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.)	<ul style="list-style-type: none"> - Perdita - Distruzione non autorizzata - Modifica non autorizzata

- Sono gestiti i back up

Pericoli associati	Rischi
Eventi naturali (terremoti, eruzioni vulcaniche, ecc.)	<ul style="list-style-type: none"> - Perdita - Distruzione non autorizzata
Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)	<ul style="list-style-type: none"> - Perdita - Distruzione non autorizzata - Modifica non autorizzata - Divulgazione non autorizzata - Accesso dati non autorizzato
Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.)	<ul style="list-style-type: none"> - Perdita - Distruzione non autorizzata - Modifica non autorizzata - Divulgazione non autorizzata - Accesso dati non autorizzato
Agenti fisici (incendio, allagamento, attacchi esterni)	<ul style="list-style-type: none"> - Perdita - Distruzione non autorizzata

- Sono utilizzati software antivirus e anti intrusione	
Pericoli associati	Rischi
Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)	<ul style="list-style-type: none"> - 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.)	<ul style="list-style-type: none"> - Perdita - Distruzione non autorizzata - Modifica non autorizzata

- Viene eseguita opportuna manutenzione	
Pericoli associati	Rischi
Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)	<ul style="list-style-type: none"> - Perdita - Distruzione non autorizzata - Modifica non autorizzata - Divulgazione non autorizzata - Accesso dati non autorizzato

TRATTAMENTO: Gestione dei fornitori (contratti, ordini, arrivi, fatture)
 Scheda creata in data: 23/11/2022
 Ultimo aggiornamento avvenuto in data: 23/11/2022

Struttura	<ul style="list-style-type: none"> • Amministrazione • Sede operativa
------------------	---

Personale coinvolto	
Persone autorizzate	
Partners - Responsabili esterni	
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)	Consenso
Base giuridica per il trattamento per dati particolari (art. 9 GDPR)	Consenso
Finalità del trattamento	Gestione dei fornitori (contratti, ordini, arrivi, fatture) Adempimento di obblighi fiscali o contabili Gestione del contenzioso (contratti, ordini, arrivi, fatture)
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	PMI (Piccole e Medie Imprese) 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 Amministrazioni Pubbliche
Informativa	Si
Profilazione	Non presente
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)	Non presente

Modalità di elaborazione dati: Mista - elettronica e cartacea	
Strumenti	Software gestionale
Archiviazione	Armadi Blindati
Strutture informatiche di archiviazione	
Strutture informatiche di backup	

VALUTAZIONE DEL LIVELLO DI RISCHIO		
PROBABILITÀ	CONSEGUENZE	LIVELLO DI RISCHIO
Poco probabile	Marginali	Medio-basso

MISURE DI SICUREZZA TECNICHE ED ORGANIZZATIVE
--

- E' applicata una gestione della password degli utenti	
Pericoli associati	Rischi
Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)	<ul style="list-style-type: none"> - 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.)	<ul style="list-style-type: none"> - 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.)	<ul style="list-style-type: none"> - Perdita - Distruzione non autorizzata - Modifica non autorizzata

- E' presente una politica per la sicurezza e la protezione dei dati	
Pericoli associati	Rischi
Eventi naturali (terremoti, eruzioni vulcaniche, ecc.)	<ul style="list-style-type: none"> - Perdita - Distruzione non autorizzata
Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica)	<ul style="list-style-type: none"> - Perdita - Distruzione non autorizzata

di posta elettronica, ecc.)	<ul style="list-style-type: none"> - Modifica non autorizzata - Divulgazione non autorizzata - Accesso dati non autorizzato
Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)	<ul style="list-style-type: none"> - Perdita - Distruzione non autorizzata - Modifica non autorizzata

- I dati sono crittografati	
Pericoli associati	Rischi
Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)	<ul style="list-style-type: none"> - 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.)	<ul style="list-style-type: none"> - Perdita - Distruzione non autorizzata - Modifica non autorizzata

- 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	
Pericoli associati	Rischi
Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)	<ul style="list-style-type: none"> - Perdita - Distruzione non autorizzata - Modifica non autorizzata

- Le password sono modificate ogni 3 mesi	
Pericoli associati	Rischi
Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)	<ul style="list-style-type: none"> - 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.)	<ul style="list-style-type: none"> - Perdita - Distruzione non autorizzata - Modifica non autorizzata

- Sono applicate regole per la gestione delle password.	
Pericoli associati	Rischi
Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)	<ul style="list-style-type: none"> - 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.)	<ul style="list-style-type: none"> - Perdita - Distruzione non autorizzata - Modifica non autorizzata

- Sono definiti i ruoli e le responsabilità
--

Pericoli associati	Rischi
Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)	<ul style="list-style-type: none"> - Perdita - Distruzione non autorizzata - Modifica non autorizzata

- Sono gestiti i back up

Pericoli associati	Rischi
Eventi naturali (terremoti, eruzioni vulcaniche, ecc.)	<ul style="list-style-type: none"> - Perdita - Distruzione non autorizzata
Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)	<ul style="list-style-type: none"> - Perdita - Distruzione non autorizzata - Modifica non autorizzata - Divulgazione non autorizzata - Accesso dati non autorizzato
Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.)	<ul style="list-style-type: none"> - Perdita - Distruzione non autorizzata - Modifica non autorizzata - Divulgazione non autorizzata - Accesso dati non autorizzato
Agenti fisici (incendio, allagamento, attacchi esterni)	<ul style="list-style-type: none"> - Perdita - Distruzione non autorizzata

- Sono utilizzati software antivirus e anti intrusione

Pericoli associati	Rischi
Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)	<ul style="list-style-type: none"> - 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.)	<ul style="list-style-type: none"> - Perdita - Distruzione non autorizzata - Modifica non autorizzata

- Viene eseguita opportuna manutenzione

Pericoli associati	Rischi
Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)	<ul style="list-style-type: none"> - Perdita - Distruzione non autorizzata - Modifica non autorizzata - Divulgazione non autorizzata - Accesso dati non autorizzato