VALUTAZIONE DEI RISCHI E PIANO D'AZIONE RACCOMANDATO

Azienda / Titolare: **C.I.A.P.I. (REGIONE SICILIANA) - Dott. Scala Giacomo**

Ex S.S 114, SNC - 96010 PRIOLO GARGALLO (SR) – C.F. 80001330895

1. OBIETTIVI DELLA VALUTAZIONE DEI RISCHI

L'attività di audit sulla valutazione dei rischi si è concentrata sui seguenti aspetti:

1.1 Gestione della protezione dei dati

L'attività di audit ha verificato fino a che punto sono attuati i principi di responsabilità nella protezione dei dati, le politiche e le procedure, i controlli in grado di misurare il livello di prestazione della protezione; i meccanismi di individuazione e segnalazione della congruità con i vigenti regolamenti in materia di protezione dei dati personali. Questa attività è stata svolta in tutti i dipartimenti dell'organizzazione.

1.2 Addestramento e sensibilizzazione

L'attività di audit ha verificato le modalità con cui è stata impartita e tenuta sotto controllo la formazione dei soggetti coinvolti nella protezione e trattamento dei dati personali, nonché la dettagliata conoscenza dei requisiti in materia di protezione dei dati personali, in relazione ai ruoli ed alle responsabilità dei singoli soggetti coinvolti. In particolare, l'Auditor ha verificato se tutti questi soggetti hanno sottoscritto uno specifico obbligo di riservatezza sul trattamento dei dati loro affidati, o se esiste altro obbligo formalizzato di riservatezza.

1.3 Gestione manuale ed elettronica dei dati personali

L'attività di audit ha verificato i processi che sono attuati dall'organizzazione per la gestione di supporti, sia manuali (cartacei) sia elettronici, che contengono dati personali. L'attività di audit la verificato inoltre i controlli in essere, in grado di monitorare la creazione, la manutenzione, l'archiviazione, il trasporto, la comunicazione e la diffusione, la conservazione e la distruzione di supporti contenenti dati personali.

1.4 Sicurezza dei dati personali

L'attività di audit ha verificato le misure tecniche ed organizzative in essere, in grado di garantire che sia mantenuto un adeguato livello di sicurezza sui dati personali, custoditi su supporti cartacei od elettronici.

1.5 Congruità della informativa

Come più volte sottolineato nel Regolamento UE sulla protezione dei dati, una informativa accurata, intelligibile e corretta rappresenta un aspetto essenziale in qualsiasi forma di acquisizione e trattamento di dati. In fase di audit, sono state esaminate tutte le varie informative che vengono fornite dal titolare del trattamento, preferibilmente conformi ai modelli proposti dal Parlamento Europeo, o da altri modelli che potranno essere predisposti dalla Unione Europea, cercando di esaminarli dal punto di vista di un interessato non particolarmente competente e preparato nel settore.

1.6 – Correttezza delle procedure di raccolta del consenso

La raccolta del consenso rappresenta il naturale completamento della offerta di informativa. Si ripete a questo proposito, la necessità che il consenso sia espresso in forma "granulare", in modo che siano da evitare consensi generalizzati, afferenti a molteplicità di utilizzo dei dati personali raccolti. Anche in questo caso, l'Auditor ha esaminato il modulo di raccolta del consenso, mettendosi nei panni di un interessato non particolarmente competente preparato nel settore.

1.7 Determinazione del tempo di conservazione del dato

Come regola generale, un dato deve essere conservato per il tempo minimo necessario per raggiungere le finalità, per le quali il dato è stato raccolto. In fase di raccolta del dato, è pertanto indispensabile attribuire ad esso se non un periodo minimo di conservazione, almeno un criterio, sulla base del quale possa essere successivamente determinata la data ultima di conservazione. Attenzione deve anche essere prestata alle modalità grazie alle quali i dati, al termine del periodo utile di trattamento vengono eliminati. Esistono procedure normative europee applicabili sia alla cancellazione di dati su supporto cartaceo, sia su altri supporti.

1.8 Attività di comunicazione e diffusione di dati personali

L'attività di audit ha verificato se le procedure in essere, afferenti alla comunicazione e diffusione di dati personali, siano pienamente rispettose dei vigenti regolamenti congrue con le indicazioni date dal responsabile e dall'incaricato del trattamento dei dati personali. In questo ambito, verranno in particolare analizzate le modalità di gestione di siti internet ed intranet, alla luce del fatto che questi siti abbiano o meno la possibilità di raccogliere dati personali; in fase di consultazione.

1.9 Attività di trattamento svolta in paesi terzi

L'attività di audit ha infine verificato se le procedure in essere, afferenti all'eventuale trattamento di dati in paesi terzi, siano pienamente rispettose dei vigenti regolamenti e congrue con le indicazioni date dal responsabile e dall'incaricato del trattamento dei dati personali.

2. I LIVELLI DELLA VALUTAZIONE

Le osservazioni e le raccomandazioni che seguono, sono classificate secondo un livello di importanza, che viene definito in questa tabella.

L'Auditor auspica che il responsabile e l'incaricato del trattamento prendano buona nota di questi livelli di valutazione, in modo da pianificare appropriatamente le eventuali attività correttive e migliorative.

COLORE	OPINIONE DELL' AUDITOR	LIVELLO DI PRIORITA' – RACC.	DEFINIZIONE
VERDE	Elevato livello di congruità	Vengono evidenziati solo aspetti di modesta rilevanza	Vi è un elevato livello di fiducia sul fatto che i processi e le procedure in atto garantiscano un adeguato livello di protezione dei dati. L'audit ha individuato solo alcune aree di modesta rilevanza per interventi di miglioramento alla situazione esistente e, pertanto non si ritiene che siano, necessari ulteriori significativi interventi per ridurre il rischio di non conformità con i dettati del regolamento.
GIALLO	Accettabile livello di congruità	Gli aspetti esaminati sono a bassa priorità	Vi è un elevato livello di fiducia sul fatto che i processi e le procedure in atto garantiscano un adeguato livello di protezione dei dati. Vi è un elevato livello di fiducia sul fatto che i processi e le procedure in atto garantiscano un adeguato livello di protezione dei dati.
ARANCIO	Scarso livello di congruità	Gli aspetti esaminati sono a media priorità	Vi è un modesto livello di fiducia sul fatto che i processi e le procedure in atto garantiscano un adeguato livello di protezione dei dati. L'audit ha individuato varie aree bisognose di interventi di miglioramento alla situazione esistente, onde ridurre il rischiò di non conformità con i dettati del regolamento.
ROSSO	Insoddisfacente livello di congruità	Gli aspetti esaminati sono ad alta priorità	Vi è un basso livello di fiducia sul fatto che i processi e le procedure in atto garantiscano un adeguato livello di protezione dei dati. L'audit ha individuato rischi significativi di mancato rispetto dei dettati di regolamento in varie aree.

3. ILLUSTRAZIONE DETTAGLIATA DELLE RISULTANZE E PIANO DI AZIONE RACCOMANDATO

GESTIONE DELLA PROTEZIONE DEI DATI		TABELLA -A-
CODICE E TITOLO	**RISULTATO**	**RACCOMANDAZIONE**
Risultanza A1 Organigramma aziendale	A livello strutturale e di lettere di nomina l'azienda è conforme a Reg. UE. 2016/679.	Nessuna raccomandazione
Risultanza A2 Procedure tecniche ed organizzative di verifica e controllo	L'azienda ha previsto che le procedure vengano verificate direttamente da Titolare del trattamento.	Nessuna raccomandazione
Risultanza A3 Predisposizione di Audit periodici	Non sono ancora stati predisposti, da parte dell'azienda, Audit periodici per l'individuazione e la segnalazione della congruità con i vigenti regolamenti in materia di protezione dei dati personali Per conseguenza si avanzano la seguente raccomandazione.	In prospettiva predisporre almeno semestralmente degli Audit di controllo.
ADDESTRAMENTO E SENSIBILIZZAZIONE		**TABELLA -B-**
CODICE E TITOLO	**RISULTATO**	**RACCOMANDAZIONE**

Risultanza B1 Svolgimento di corsi di Formazione sulla Privacy	Alla data di compilazione del Questionario di raccolta dati, non risultano effettuati Corsi di formazione sulla privacy documentati.	Pianificare la Formazione in materia privacy.
Risultanza B2 Predisposizione di corsi specifici in base all'area di competenza	Sono stati predisposti corsi specifici in base all'area di competenza.	Nessuna raccomandazione
Risultanza B3 Predisposizione di un piano formativo	È stato predisposto un piano formativo.	Nessuna raccomandazione
Risultanza B4 Sottoscrizione dell'obbligo di riservatezza del trattamento dei dati	È stata espressamente specificata la parte inerente all'obbligo di riservatezza del trattamento dei dati all'interno delle lettere di nomina.	Nessuna raccomandazione
GESTIONE MANUALE ED ELETTRONICA DEI DATI PERSONALI		**TABELLA -C-**
CODICE E TITOLO	**RISULTATO**	**RACCOMANDAZIONE**
Risultanza C1 Definizione di chi può trattare i dati	I documenti contenenti dati personali non vengono trattati solo da personale nominato e debitamente formato.	Provvedere alla nomina degli Addetti al trattamento dati.
Risultanza C2 Presenza di registri di accesso a dati sensibili e giudiziari	Sono stati previsti registri di accesso al trattamento di dati sensibili e giudiziari al di fuori dell'orario lavorativo.	Nessuna raccomandazione
Risultanza C3 Distruzione dei documenti contenenti dati personali	Tutti i documenti da cestinare contenenti dati personali vengono strappati a mano o triturati con il trita-carte.	Nessuna raccomandazione
Risultanza C4 Separazione dei dati sensibili e giudiziari	I dati sensibili e giudiziari vengono conservati separatamente dagli-altri documenti e riposti in archivi chiusi a chiave.	Nessuna raccomandazione
Risultanza C5 Sicurezza dello strumento elettronico incustodito	A dispositivo incustodito non si attiva il salvaschermo che slogga l'utente.	Provvedere ad attivare le procedure di salvaschermo in tutti i dispositivi che trattano dati personali.
Risultanza C6 Disciplinare di posta elettronica ed internet	È presente un disciplinare di posta elettronica ed internet.	Nessuna raccomandazione
SICUREZZA DEI DATI PERSONALI		**TABELLA -D-**
CODICE E TITOLO	**RISULTATO**	**RACCOMANDAZIONE**
Risultanza D1 Autenticazione informatica	È stata predisposta l'autenticazione informatica per ogni utente che si logga al sistema tramite Username/Password	Nessuna raccomandazione
Risultanza D2 Procedura per l'affidamento delle credenziali	Esiste una procedura per l'affidamento delle credenziali.	Nessuna raccomandazione
Risultanza D3 Istruzioni sulle modalità di conservazione, composizione e aggiornamento della parola chiave	All'interno delle lettere di nomina predisposte sono specificate istruzioni sulle modalità di conservazione, composizione e aggiornamento della parola chiave.	Nessuna raccomandazione

Risultanza D4 Disattivazione delle credenziali non utilizzate da almeno 6 mesi	È stata predisposta la disattivazione delle credenziali non utilizzate da almeno 6 mesi.	Nessuna raccomandazione
Risultanza D5 Sistema di autorizzazione	Attualmente è previsto un sistema di autorizzazione di accesso al PC.	Nessuna raccomandazione
Risultanza D6 Antivirus	Ogni PC è dotato di Antivirus che viene aggiornato giornalmente e rinnovato alla scadenza.	Nessuna raccomandazione
Risultanza D7 Aggiornamento dei programmi	I programmi gestionali vengono aggiornati costantemente dal titolare.	Nessuna raccomandazione
Risultanza D8 Modalità salvataggio dei dati	Viene effettuato il salvataggio dei dati.	Nessuna raccomandazione
Risultanza D9 Procedure tecniche per il salvataggio dei dati	Il salvataggio è automatico o manuale ad opera dell'incaricato.	Nessuna raccomandazione
Risultanza D10 Procedute organizzative per il salvataggio dei dati	Il titolare vigila sul corretto salvataggio dei dati	Nessuna raccomandazione
Risultanza D11 Firewall	Il sistema informatico è protetto da firmali aggiornati	Nessuna raccomandazione
Risultanza D12 Procedure per la gestione dei dispositivi removibili	All'interno delle lettere di nomina e del Modello organizzativo privacy vengono descritte le procedure per la gestione dei dispositivi removibili.	Nessuna raccomandazione
Risultanza D13 Ripristino dei dati	Recupero dei dati tramite copie di backup.	Nessuna raccomandazione
Risultanza D14 Piano di Emergenza	Non se ne rileva la necessità in relazione all'attività svolta, tuttavia al punto 9. ne viene dettagliato uno.	Nessuna raccomandazione
Risultanza D15 Pseudonomizzazione dei dati	Non se ne rileva la necessità in relazione all'attività svolta.	Nessuna raccomandazione
Risultanza D16 Utilizzo di piattaforme in Cloud	Attualmente per accedere è previsto un sistema di Autorizzazione.	Nessuna raccomandazione
Risultanza D17 Valutazione d'impatto	L'azienda ha analizzato che in base alla struttura aziendale e all'entità di dati trattati non è necessario effettuare la valutazione d'impatto.	Nessuna raccomandazione
CONGRUITA' DELL'INFORMATIVA		**TABELLA -E-**
CODICE E TITOLO	**RISULTATO**	**RACCOMANDAZIONE**
Risultanza E1 Procedura di consegna dell'informativa	Ad ogni nuovo Cliente viene fatta firmare l'informativa.	Nessuna raccomandazione
Risultanza E2 Informative diversificate per tipologia di interessato	L'azienda diversifica la tipologia di informativa fornita in base alla categoria di interessato cui si riferisce.	Nessuna raccomandazione
CORRETTEZZA DELLE PROCEDURE DI RACCOLTA DEL CONSENSO		**TABELLA -F-**

CODICE E TITOLO	RISULTATO	RACCOMANDAZIONE
Risultanza F1 Procedure per raccolta del consenso granulare	Il consenso è attualmente predisposto come da normativa italiana.	Nessuna raccomandazione
Risultanza F2 Procedure per la gestione dei consensi	È stata predisposta la procedura di gestione dei consensi richiesti.	Nessuna raccomandazione
PROCEDURE DI CLASSIFICAZIONE DEL LIVELLO DI PROTEZIONE DEI DATI		**TABELLA -G-**
CODICE E TITOLO	**RISULTATO**	**RACCOMANDAZIONE**
Risultanza G1 Procedure di classificazione del livello di protezione dei dati	Sono state predisposte le procedure di classificazione di tipologie di dato.	Nessuna raccomandazione
DETERMINAZIONE DEL TEMPO DI CONSERVAZIONE DEL DATO		**TABELLA -H-**
CODICE E TITOLO	**RISULTATO**	**RACCOMANDAZIONE**
Risultanza H1 Determinazione del tempo di conservazione del dato	È stato determinato un tempo per la conservazione dei dati personali, specificato nell'informativa.	Nessuna raccomandazione
ATTIVITA' DI MARKETING, UTILIZZANDO VARI CANALI DI COMUNICAZIONE		**TABELLA -I-**
CODICE E TITOLO	**RISULTATO**	**RACCOMANDAZIONE**
Risultanza I1 Attività di marketing effettuate nel rispetto delle disposizioni di legge	L'azienda non effettua operazioni di marketing di nessun tipo.	Nessuna raccomandazione
PROCEDURE DI RISPOSTA A RICHIESTE DI INTERESSATI		**TABELLA -J-**
CODICE E TITOLO	**RISULTATO**	**RACCOMANDAZIONE**
Risultanza J1 Richieste afferenti a dati personali	Sono state predisposte procedure di risposta a richieste di interessati.	Nessuna raccomandazione
ATTIVITA' DI COMUNICAZIONE E DIFFUSIONE DI DATI PERSONALI		**TABELLA -K-**
CODICE E TITOLO	**RISULTATO**	**RACCOMANDAZIONE**
Risultanza K1 Gestione del sito web alle normative vigenti	L'azienda **dispone** di un sito web.	Nessuna raccomandazione
Risultanza K2 Gestione della rete intranet conformemente alle normative vigenti	La intranet-aziendale è protetta e vi accedono solo gli Addetti debitamente nominati.	Nessuna raccomandazione
Risultanza K3 Impianto di Video Sorveglianza conforme al Reg. UE 2016/679 e ai Provvedimenti del Garante	L'azienda **ha** un impianto di Video Sorveglianza.	Nessuna raccomandazione
ATIVITA' DI TRATTAMENTO SVOLTA IN PAESI TERZI		**TABELLA -L-**
CODICE E TITOLO	**RISULTATO**	**RACCOMANDAZIONE**

Risultanza L1 Procedure per trattamento dati all'estero congrue al vigente Regolamento UE	Non vengono effettuati trattamenti di dati all'estero.	Nessuna raccomandazione
RAPPORTI CON CORRESPONSABILI E RAPPRESENTANTI DI RESPONSABILI		**TABELLA -M-**
CODICE E TITOLO	**RISULTATO**	**RACCOMANDAZIONE**
Risultanza M1 Congruità della nomina di corresponsabili o rappresentanti	Non vi sono Corresponsabili né Rappresentanti di responsabili.	Nessuna raccomandazione
NOMINA DEL RESPONSABILE PER LA PROTEZIONE DEI DATI		**TABELLA -N-**
CODICE E TITOLO	**RISULTATO**	**RACCOMANDAZIONE**
Risultanza N1 Necessità e Congruità della nomina di DPO	L'azienda non ha provveduto a una nomina formale del DPO, in quanto non obbligata, né necessaria.	Nessuna raccomandazione

4. SINTESI DELLE RISULTANZE DELL'AUDIT

Aree esaminate

A. Gestione della protezione dei dati;

B. Addestramento e sensibilizzazione;

C. Gestione manuale ed elettronica dei dati personali;

D. Sicurezza dei dati personali;

E. Congruità dell'informativa;

F. Correttezza delle procedure di raccolta del consenso;

G. Procedure di classificazione del livello di protezione dei dati;

H. Determinazione del tempo di conservazione del dato;

I. Attività di marketing, utilizzando vari canali di comunicazione;

J. Procedure di risposta a richieste di interessati;

K. Attività di comunicazione e diffusione di dati personali;

L. Attività di trattamento svolta in paesi terzi;

M. Rapporti con corresponsabili e Rappresentanti di responsabili;

N. Nomina del Responsabile per la protezione dei dati (DPO).

❖ INTERVENTI MIGLIORATIVI RACCOMANDATI:

▪ RACCOMANDAZIONI TECNOLOGICHE

- Provvedere ad attivare le procedure di salvaschermo su tutti i dispositivi;
- Provvedere a comunicare a tutti i dipendenti come utilizzare i dispositivi removibili;
- Provvedere a rendere anonimi i dati utilizzati, entro il termine definito nell'Informativa;

▪ RACCOMANDAZIONI ORGANIZZATIVE

- Provvedere alla nomina degli addetti al trattamento debitamente formati.

5. OPIONIONE DELL'AUDITOR

L'obiettivo dell'audit è quello di offrire al titolare agli eventuali responsabili ed agli incaricati del trattamento una valutazione oggettiva ed indipendente del livello con cui l'attività svolta dall'organizzazione in materia di trattamento di dati, è congrua con il vigente Regolamento UE 2016/679.

Per facilitare la lettura dell'opinione dell'Auditor, i commenti sono inseriti nella tabella seguente, e classificati in funzione del livello di assicurazione di congruità, maturato dall'Auditor stesso.

LIVELLO DI CONGRUITA'	COMMENTI DELL'AUDITOR
MOLTO BASSO	Il livello di assicurazione di congruità, come valutato dall'Auditor, porta a ritenere che il rispetto del regolamento e disposizioni in materia di dati personali, a livello di processi e procedure, sia basso. L'audit ha identificato alcune aree, dove è possibile effettuare interventi di miglioramento, per raggiungere un accettabile livello di congruità con le esigenze di protezione dei dati. Nello specifico: ▪ Pianificare la formazione in materia privacy; ▪ Provvedere alla nomina degli addetti al trattamento dati; ▪ Provvedere ad attivare le procedure di salvaschermo su tutti i dispositivi; ▪ Provvedere a comunicare a tutti gli addetti come utilizzare i dispositivi removibili. Un piano dettagliato dei possibili interventi migliorativi, afferenti alle carenze individuate, viene presentato successivamente nella sezione dedicata alla illustrazione dettagliata dell'audit e di un piano di azione.
BASSO	Il livello di assicurazione di congruità, come valutato dall'Auditor, porta a ritenere che il rispetto dei regolamenti e disposizioni in materia di dati personali, a livello di processi e procedure, sia basso. L'audit ha identificato delle aree, dove è possibile effettuare interventi di miglioramento, per raggiungere un accettabile livello di congruità con le esigenze di protezione dei dati. Nello specifico: ▪ Provvedere a rendere anonimi i dati utilizzati, entro il termine definito nell'Informativa.
ACCETTABILE	Il livello di assicurazione di congruità, come valutato dall'Auditor, porta a ritenere che il rispetto dei regolamenti e disposizioni in materia di dati personali, a livello di processi e procedure, sia accettabile. L'audit ha identificato alcune aree, dove è possibile effettuare interventi di miglioramento, per raggiungere un accettabile livello di congruità con le esigenze di protezione dei dati. Nello specifico: ▪ Nessuna rilevanza.
SODDISFACENTE	Il livello di assicurazione di congruità, come valutato dall'Auditor, porta a ritenere che il rispetto dei regolamenti e disposizioni in materia di dati personali, a livello di processi e procedure, sia soddisfacente. L'audit ha identificato le aree, dove è stato raggiunto un soddisfacente livello di congruità con le esigenze di protezione dei dati. Nello specifico: **A1.** A livello strutturale e di lettere di nomina l'Azienda è conforme al Reg. UE. 2016/679; **A2.** L'Azienda ha previsto che le procedure vengano verificate direttamente dal titolare del trattamento o da un suo delegato; **B2.** Sono stati predisposti corsi specifici in base all'area di competenza; **B3.** È stato predisposto un piano formativo; **B4.** È stata espressamente specificata la parte inerente all'obbligo di riservatezza del trattamento dei dati all'interno delle lettere di nomina; **C2.** Sono stati previsti registri di accesso al trattamento di dati sensibili e giudiziari al di fuori dell'orario lavorativo; **C3.** Tutti i documenti da cestinare contenenti dati personali vengono strappati a mano o triturati con il trita-carte; **C4.** I dati sensibili e giudiziari vengono conservati separatamente dagli-altri documenti e riposti in archivi chiusi a chiave.; **C6.** È presente un disciplinare di posta elettronica ed internet; **D1.** È stata predisposta l'autenticazione informatica per ogni utente che si logga al sistema tramite Username/Password; **D2.** Esiste una procedura per l'affidamento delle credenziali; **D3.** All'interno delle lettere di nomina predisposte sono specificate istruzioni sulle modalità di conservazione, composizione e aggiornamento della parola chiave; **D4.** È stata predisposta la disattivazione delle credenziali non utilizzate da almeno 6 mesi; **D5.** Attualmente è previsto un sistema di autorizzazione di accesso al PC; **D6.** Ogni PC è dotato di Antivirus che viene aggiornato giornalmente e rinnovato alla scadenza; **D7.** I programmi gestionali vengono aggiornati costantemente dal titolare; **D8.** Viene effettuato il salvataggio dei dati; **D9.** Il salvataggio è automatico o manuale ad opera dell'incaricato; **D10.** Il titolare vigila sul corretto salvataggio dei dati; **D11.** Il sistema informatico è protetto da firmali aggiornati; **D12.** All'interno delle lettere di nomina e del Modello organizzativo privacy vengono descritte le procedure per la gestione dei dispositivi removibili;

	D13. Recupero dei dati tramite copie di backup; **D14.** Non se ne rileva la necessità in relazione all'attività svolta, tuttavia al punto 9. ne viene dettagliato uno; **D15.** Non se ne rileva la necessità in relazione all'attività svolta; **D16.** Attualmente per accedere è previsto un sistema di Autorizzazione; **D17.** L'azienda ha analizzato che in base alla struttura aziendale e all'entità di dati trattati non è necessario effettuare la valutazione d'impatto; **E1.** Ad ogni nuovo Cliente viene fatta firmare l'informativa; **E2.** L'azienda diversifica la tipologia di informativa fornita in base alla categoria di interessato cui si riferisce; **F1.** Il consenso è attualmente predisposto come da normativa italiana; **F2.** È stata predisposta la procedura di gestione dei consensi richiesti; **G1.** Sono state predisposte le procedure di classificazione di tipologie di dato; **H1.** È stato determinato un tempo per la conservazione dei dati personali, specificato nell'informativa; **I1.** L'azienda non effettua operazioni di marketing di nessun tipo; **J1.** Sono state predisposte procedure di risposta a richieste di interessati; **K1.** L'azienda **dispone** di un sito web; **K2.** La intranet-aziendale è protetta e vi accedono solo gli Addetti debitamente nominati; **K3.** L'azienda **ha** un impianto di Video Sorveglianza; **L1.** Non vengono effettuati trattamenti di dati all'estero; **M1.** Non vi sono Corresponsabili né Rappresentanti di responsabili; **N1.** L'azienda non ha provveduto a una nomina formale del DPO, in quanto non obbligata, né necessaria.

6. RIEPILOGO DI NON CONFORMITA'

In virtù delle risultanze precedentemente definite e specificate, si evince, come da grafico successivo che, in base alla valutazione dei rischi, la struttura ha attualmente un rischio medio-basso in quanto le carenze e le inosservanze riferibili alle violazioni contrassegnate in rosso ed arancione nel grafico sono da considerare mediamente e potenzialmente dannose rispetto alle inosservanze rilevate in verde e giallo nel suddetto grafico.

- Pianificare la formazione in materia privacy;
- Provvedere alla nomina degli addetti al trattamento dei dati;
- Provvedere ad attivare le procedure di salvaschermo su tutti i dispositivi;
- Provvedere a comunicare a tutti i dipendenti come utilizzare i dispositivi removibili;
- Provvedere a rendere anonimi i dati utilizzati, entro il termine definito nell'Informativa.

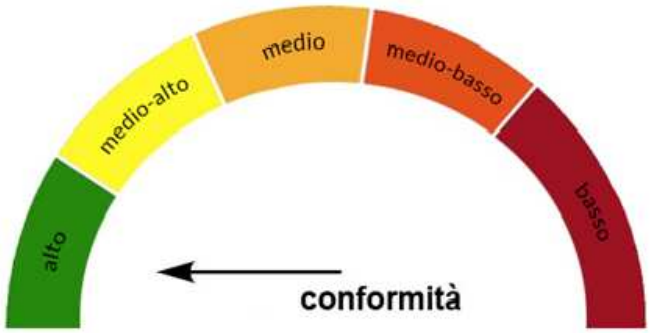
Ne deriva, secondo una media ponderata, un rischio medio-basso tendente al basso.

7. TABELLA E TEMPI DI ATTUAZIONE DELLE RACCOMANDAZIONI

RACCOMANDAZIONI DELL'AUDITOR	STATO DI ATTUAZIONE 3 MESI	STATO DI ATTUAZIONE 6 MESI
Pianificare la formazione in materia privacy.	**FORMAZIONE EFFETTUATA**	
Provvedere alla nomina degli addetti al trattamento dei dati.	**ADDETTI NOMINATI**	
Provvedere ad attivare le procedure di salvaschermo su tutti i dispositivi.	**PROCEDURE ATTIVATA**	
Provvedere a comunicare a tutti gli addetti come utilizzare i dispositivi removibili.	**COMUNICAZIONE EFFETTUATA**	
Provvedere a rendere anonimi i dati utilizzati, entro il termine definito nell'Informativa.		**IN FASE DI VALUTAZIONE**

8. CONCLUSIONI DELL'AUDIT

Osservando le raccomandazioni dell'Auditor e avendo proceduto alla generazione dei documenti così come previsti dalla normativa vigente, la situazione di conformità finale mostra un livello di conformità alto.



9. PIANO DI EMERGENZA

Nell'ottica dell'importanza della circolazione dei dati e della correlata necessità di gestirne il flusso e il lecito trattamento, bisogna provvedere a porre in essere azioni conseguenti al verificarsi di eventuali eventi dannosi o pericolosi per il trattamento dei dati personali.

In relazione alle misure di sicurezza predisposte il **C.I.A.P.I. (REGIONE SICILIANA)** ha predisposto un quadro delle possibili intromissioni o effrazioni ai sistemi informatici (attacco di un virus, hackeraggio, furto dati, programmatore che sbaglia una query ed estrae tutti i dati personali) alle quali ha associato le relative azioni correttive.

a) Nel caso di accessi non autorizzati verranno immediatamente bloccate tutte le operazioni su tutti i computer della rete e il responsabile della manutenzione dei computer disattiverà momentaneamente tutte le connessioni ad Internet. Verrà controllata tutta la rete dei computer, tutti i sistemi operativi, tutti i software installati e tutti i dati inseriti per verificare eventuali danni provocati dagli accessi non autorizzati al fine di un eventuale ripristino della normalità.

b) Nel caso l'accesso non autorizzato sia stato effettuato per scopi fraudolenti, o di sabotaggio si provvederà all'immediata denuncia pressò le forze di polizia e/o l'autorità giudiziaria dell'eventuale responsabile degli accessi non autorizzati.

c) Nel caso l'accesso non autorizzato sia stato effettuato con scopi non conformi alle norme interne della nostra organizzazione ma comunque non a scopo fraudolento o di sabotaggio verranno adottati tutti i provvedimenti previsti dalle leggi vigenti, dallo statuto dei lavoratori, dalle norme sindacali, dalle norme deontologiche.

In ogni caso per ognuna delle situazioni sopra citate o comunque per tutte le violazioni dei dati si provvederà a dare tempestiva comunicazione all'autorità garante come procedura prevista nel modulo in allegato.

Per accesso non autorizzato si intende:

- l'accesso effettuato da un operatore non autenticato utilizzando le credenziali di autenticazione di un addetto;
- l'accesso effettuato aggirando il sistema di autenticazione;
- l'accesso effettuato da un addetto autenticato in aree non previste dal sistema di autorizzazioni;
- l'accesso tramite intercettazioni di informazioni in rete;
- l'accesso non autorizzato a locali/aree ad accesso riservato;
- l'accesso a strumenti contenenti dati che sono stati sottratti.

d) Nel caso di comportamenti sleali e fraudolenti degli addetti sarà bloccato immediatamente l'accesso ai dati degli addetti e adottati i relativi provvedimenti previsti dalle leggi vigenti, dallo statuto dei lavoratori, dalle norme sindacali, dalle norme deontologiche.

e) Nel caso di azione di virus informatici verranno immediatamente bloccate tutte le operazioni su tutti i computer della rete attraverso l'utilizzo di un programma antivirus aggiornato e verrà immediatamente verificata e bonificata tutta la rete dei computer.

f) Nel caso di spamming verranno immediatamente bloccate tutte le operazioni su tutti i computer della rete e il responsabile della manutenzione dei computer disattiverà momentaneamente tutte le connessioni con Internet, verificherà i firewall su ogni computer e l'aggiornamento periodico dei programmi antivirus su ogni computer e tutta la rete dei computer.

g) Nel caso di azione dei programmi suscettibili di recare danno verranno immediatamente bloccate tutte le operazioni su tutti i computer della rete e il responsabile della manutenzione dei computer disattiverà i programmi dannosi e verrà immediatamente verificata e bonificata tutta la rete dei computer.

Valutando le criticità emerse dalla valutazione dei rischi si può considerare il livello di rischio del **C.I.A.P.I. (REGIONE SICILIANA)** come **BASSO** constatandosi un elevato livello di fiducia sul fatto che i processi e le procedure in atto garantiscano un adeguato livello di protezione dei dati.

Il Piano di emergenza elaborato dal **C.I.A.P.I. (REGIONE SICILIANA)** di cui sopra si riferisce a quelle azioni come elencate precedentemente.

In relazione a quegli eventi dannosi che comportano: un elevato livello di criticità per il dato personale stesso, il **C.I.A.P.I. (REGIONE SICILIANA)** ha previsto un tempo di ripristino pari a 7 giorni per i seguenti casi di violazioni illecite o accidentali di dati:

- Perdita;
- Distruzione;
- Modifica;
- Divulgazione non autorizzata
- Accesso ai dati personali che siano trasmessi, conservati o trattati.

Al fine di ripristinare gli archivi e i dati, si è provveduto a conservare in un luogo esterno alla sede, copie aggiornate settimanalmente.

In aggiunta a ciò il fornitore di fiducia della **C.I.A.P.I. (REGIONE SICILIANA)** garantisce la consegna di strumenti elettronici con la stessa configurazione entro tre giorni dall'avvenuta violazione, considerando il tempo minimo di un giorno per l'installazione del sistema operativo e dei software applicativi.

Il trattamento di tutti i dati processati sarà ripristinato entro i **7 giorni** del termine di cui sopra.

Nella definizione del piano di emergenza il **C.I.A.P.I. (REGIONE SICILIANA)** ha predisposto eventi formativi per tutti gli addetti e i responsabili del trattamento dati nell'ottica di definire le azioni consentite e quelle non consentite agli stessi soggetti interessati. Nello stesso ambito ha fornito dovuta e comprovata formazione dei possibili eventi negativi e delle relative azioni correttive da porre in essere, in modo tale da rendere note agli addetti ed ai responsabili del trattamento le procedure da attivare per risolvere oi contenere l'effetto negativo scaturito dagli eventi dannosi.

10. RESPONSABILI O CONSULENTI E AUTORITA' DA CONTATTARE IN CASO DI EMERGENZA

Il Titolare del trattamento a norma dell'art. 33 del Regolamento UE 2016/679, qualora la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche, è tenuto ad effettuare senza ingiustificato ritardo, entro massimo le 72 ore dal momento in cui ne è venuto a conoscenza, la notificazione presso l'autorità competente, di cui all'art.55, della avvenuta violazione.

Nel caso di violazione che comporti un rischio consistente per i diritti e le libertà delle persone fisiche la comunicazione va fatta all'autorità competente e contestualmente all'interessato come dispone l'art.34.

Il **C.I.A.P.I. (REGIONE SICILIANA)** si fa carico di adottare tutte le misure idonee a prevenire o risolvere eventuali eventi dannosi e di comunicare tempestivamente ogni violazione avvenuta presso l'autorità competente a norma dell'art. 83 del Regolamento UE 2016/679.