Croce Rossa Italiana
Comitato di Chieri

Croce Rossa Italiana

MANUALE DI GESTIONE DELLA PRIVACY

Documento di Valutazione dei Rischi nel trattamento di dati personali

Rev.3 del 19/4/2023

Approvato dal Presidente GianPiero Del Tito
DPO, Responsabile della protezione dei dati: Andrea Aulisi

Cronologia delle revisioni

Data	Rev.	creata da	Descrizione del cambiamento
23/05/2018	0	GianPiero Del Tito	documento di base
01/08/2019	1	GianPiero Del Tito	Modificato organigramma
29/04/2021	2	GianPiero Del Tito	Approfondite le modalità di backup e ripristino
19/4/2023	3	GianPiero Del Tito	Introdotto il ruolo del DPO

Sono allegati al presente documento di Valutazione dei Rischi:

1. Accordo contitolarità
2. Sintesi Accordo contitolarità
3. Atto nomina addetto trattamento dati
4. Linee guida Privacy - Per Le Persone
5. Informativa Privacy - Per Le Persone
6. Informativa – Volontari
7. Informativa – Dipendenti
8. Informativa – Utenti
9. Informativa – Utenti non pazienti
10. Informativa – Prestatori
11. Informativa – Fornitori
12. Atto designazione Responsabile della protezione dei Dati
13. Dati in emergenza
14. Nomina Responsabile esterno del Trattamento
15. Lettera di riservatezza per l'autorizzazione di dipendenti e volontari

Sommario

1. SCOPO E CAMPO DI APPLICAZIONE

Scopo di questo documento è di delineare il quadro delle misure di sicurezza da adottare per il trattamento dei dati personali effettuato presso CRI COMITATO DI CHIERI.

Nel seguito del documento i termini: Titolare, Contitolare, Responsabile, e Dato personale sono utilizzati in conformità alle definizioni del Regolamento UE 2016/679. Il Documento di Valutazione dei Rischi viene applicato a tutti i trattamenti dei dati personali effettuati sia per mezzo di strumenti elettronici sia di strumenti cartacei di elaborazione. Il Documento di Valutazione dei Rischi deve essere conosciuto dai responsabili e dagli incaricati autorizzati ed applicato nelle strutture organizzative dove i dati vengono conservati. Le procedure per un corretto trattamento dei dati, secondo le disposizioni del Regolamento UE 2016/679 sono comunicate e spiegate ai dipendenti dai responsabili del trattamento in occasione di ogni nuovo ingresso in servizio, di cambiamento di mansione, di introduzione di nuovi strumenti utilizzabili per il trattamento dei dati.

Titolare del trattamento: CRI COMITATO DI CHIERI, con sede in Strada S. Silvestro, 14, 10023 Chieri (TO) CF/PI 11053660012 nella persona del Legale Rappresentante.

Contitolare del trattamento: Associazione della Croce Rossa Italiana – Organizzazione di Volontariato, (C.F./P.IVA n. 13669721006) in persona del suo Legale Rappresentante, con sede a Roma nella via Toscana n. 12.

Il Titolare, tenendo conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi per i diritti e le libertà delle persone fisiche:

- Definisce ed attua politiche adeguate in materia di protezione dei dati e mette in atto misure tecniche ed organizzative adeguate a garantire ed essere in grado di dimostrare che:
  - il trattamento sia effettuato conformemente al Regolamento;
  - siano trattati, per impostazione predefinita, solo i dati necessari per ogni specifica finalità del trattamento (in termini di quantità dei dati raccolti, portata del trattamento, periodi di conservazione, accessibilità dell'interessato);
  - non siano resi accessibili, per impostazione predefinita, dati personali ad un numero indefinito di persone fisiche, senza l'intervento della persona fisica.
- Individua, autorizza gli incaricati del trattamento e ne promuove la formazione.
- Redige ed aggiorna il registro dei trattamenti.
- Predispone, approva ed aggiorna periodicamente, un "Documento di Valutazione dei Rischi" privacy.
- Qualora i trattamenti effettuati presentino "rischi elevati" per i dati delle persone, predispone ed approva una "valutazione d'impatto".
- Notifica al Garante, quale Autorità di controllo, ogni violazione dei dati personali di cui venga a conoscenza, qualora da questa derivino rischi per i diritti e le libertà degli interessati.

Il Titolare deve precostituire un apparato documentale per poter dimostrare di aver valutato tutti i parametri della propria responsabilità

Responsabile del trattamento: Viene designato dal Titolare, con un incarico formale che ne specifica compiti e responsabilità: durata dei trattamenti, natura e finalità dei trattamenti, tipo dei dati personali e categorie di interessati, obblighi e diritti del Titolare, come indicato al capitolo 7.1.

Personale autorizzato incaricato del trattamento: Svolgono le attività previste dai trattamenti secondo le prescrizioni contenute nel Regolamento UE 2016/679 e le direttive del titolare. Non modificano trattamenti esistenti e non introducono nuovi trattamenti senza l'autorizzazione del titolare.

Rispettano e fanno rispettare le norme di sicurezza e protezione dei dati personali; informano il titolare in caso di incidenti di sicurezza che coinvolgono i dati personali trattati.

Parole chiavi: Gestite in modo autonomo da ogni operatore e conservate direttamente.

1.1. Contitolarità con l'Associazione della Croce Rossa Italiana

L'Associazione della Croce Rossa Italiana – ODV, i Comitati territoriali della Croce Rossa Italiana lavorano in stretta collaborazione per l'erogazione dei servizi di assistenza.

Le parti hanno stabilito di comune accordo le modalità di trattamento dei dati personali nelle singole fasi del processo e perciò esse sono contitolari per la protezione dei dati.

L'Associazione della Croce Rossa Italiana - ODV, mediante i propri operatori della Centrale di Risposta Nazionale, svolge l'attività di raccolta, condivisione e conservazione dei dati forniti, anche utilizzando strumenti elettronici.

Il Comitato di Chieri, così come gli altri Comitati territoriali della Croce Rossa, effettuano la raccolta, la lettura, l'utilizzazione e l'aggiornamento delle informazioni, al fine di espletare il servizio richiesto.

1.2. DATA PROTECTION BY DESIGN

Intesa come modo di operare di default all'interno della nostra Organizzazione. I principi della DATA PROTECTION by Design sono applicati a tutti i tipi di informazioni personali, con particolare vigore ai dati sensibili, e si riassumono in:

- Proattività non reattività (prevenire non correggere): anticipare e prevenire gli eventi invasivi della DATA PROTECTION prima che essi accadano
- DATA PROTECTION come impostazione di default: realizzare il massimo livello di DATA PROTECTION assicurando che i dati siano automaticamente protetti in un qualunque sistema
- DATA PROTECTION incorporata nella progettazione: componente essenziale per la realizzazione del nucleo funzionale del nostro sistema di trattamento e protezione dei dati
- Massima funzionalità: conciliare tutti gli interessi legittimi e gli obiettivi comuni con modalità di valore positivo "vantaggioso per tutti"
- Sicurezza: estensione del sistema per l'intero ciclo vitale dei dati per assicurare che tutti i dati siano conservati con cura e poi distrutti in modo sicuro alla fine del processo

- Visibilità e trasparenza: informazioni ed obiettivi stabiliti, soggetti a verifica indipendente
- Rispetto per la DATA PROTECTION dell'utente: considerare prioritari gli interessi degli individui offrendo efficaci interventi di default della DATA PROTECTION, informazioni appropriate e potenziando opzioni di facile utilizzo per l'utente

1.3. DATA PROTECTION BY DEFAULT

Intesa come messa in pratica di meccanismi per garantire che siano trattati, di default, solo i dati necessari per ciascuna finalità specifica del trattamento e che, in particolare, la quantità dei dati raccolti e la durata della loro conservazione non vadano oltre il minimo necessario per le finalità perseguite. In particolare, detti meccanismi garantiscono che, di default, non siano resi accessibili dati a un numero indefinito di persone

1.4. SICUREZZA DEI DATI

Inteso come sicurezza dei dati, livello di protezione, ad esempio, da forze "distruttive" e dalle azioni indesiderate di utenti non autorizzati

Nella stesura del documento, il Responsabile della Privacy ha concepito i protocolli operativi e gestionali di riferimento per garantire le corrette metodologie di trattamento e protezione dei dati, approvando in tal senso il Codice di condotta che tutto il personale (interno ed esterno) che collabora con Comitato di Chieri O.d.V. è tenuto a rispettare. In particolare, il nostro Codice di condotta rappresenta il vero e proprio Sistema di Gestione della Protezione dei Dati (di seguito anche SGPD) che interpreta la corretta applicazione del Regolamento CE 679/2016.

Oltre che a essere una linea guida progettuale ed operativa, il presente documento deve essere utilizzato costantemente per il miglioramento continuo della gestione della protezione dei dati e per la limitazione del rischio sanzionatorio. A questo fine, i contenuti sono stati comunicati a tutto il personale attraverso attività di formazione programmata.

Chiunque ha la possibilità di consultarlo nel caso di necessità e/o di richiederne copia conforme all'originale. Tale documento viene presentato in fase di inserimento nella struttura organizzativa dallo stesso Responsabile, o da persona incaricata, all'eventuale neoassunto. Ogni aggiornamento del presente documento viene comunicato attraverso sessioni informative e formative a tutte le risorse che collaborano con la nostra Organizzazione.

I principi applicabili al trattamento dei dati personali per quanto di competenza della nostra Organizzazione, ai sensi anche dell'Art. 5 CE 679/2016, sono:

- **LICEITÀ, CORRETTEZZA E TRASPARENZA**: i dati personali devono essere trattati in modo lecito, corretto e trasparente nei confronti dell'interessato
- **LIMITAZIONE DELLA FINALITÀ**: i dati personali devono essere raccolti per finalità determinate, esplicite e legittime e successivamente trattati in modo che non sia incompatibile con tali finalità
- **MINIMIZZAZIONE DEI DATI**: i dati personali devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati

- **ESATTEZZA**: i dati personali devono essere esatti e, se necessario, aggiornati. Devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati
- **LIMITAZIONE DELLA CONSERVAZIONE**: i dati personali devono essere conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati
- **INTEGRITÀ E RISERVATEZZA**: i dati personali devono essere trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali

1.5. Alcune definizioni

Dato personale: qualsiasi informazione riguardante una persona fisica identificata o identificabile ("interessato"). Si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.

Dati relativi alla salute: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute (dati sensibili).

Dato sensibile (Art. 9 - Categorie particolari di dati personali): qualsiasi informazione riguardante una persona fisica identificata o identificabile ("interessato") idonea a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale ed eventuali altri Diritti fondamentali garantiti dalla costituzione Europea.

Destinatario: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi.

Diffusione: il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

Documento cogente di riferimento: Regolamento CE 679/2016 del Parlamento Europeo e del Consiglio del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati) - Gazzetta ufficiale dell'Unione europea - 4 maggio 2016

Interessato: la persona fisica cui si riferiscono i dati personali.

Limitazione di trattamento: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro.

Persone autorizzate: le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dai responsabili.

Profilazione: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica.

Pseudonimizzazione: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile.

Rappresentante: la persona fisica o giuridica stabilita nell'Unione che, designata dal titolare del trattamento o dal responsabile del trattamento per iscritto, li rappresenta per quanto riguarda gli obblighi rispettivi a norma del documento cogente di riferimento.

Responsabile della protezione dei dati - Data Protection Officer (DPO): la persona fisica designata dal titolare del trattamento e dal responsabile del trattamento incaricata di informare e fornire consulenza, sorvegliare l'osservanza della normativa cogente e del codice di condotta in ambito protezione dati personali, fornire pareri sulla valutazione d'impatto, cooperare e fungere da punto di contatto con l'autorità di controllo per tutte le questioni inerenti alla protezione dati personali.

Responsabile del trattamento: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento.

Rischio: effetto dell'incertezza che può avere effetti positivi o negativi.

Sistema antintrusione: l'insieme di tecnologie informatiche e non atte ad evitare l'ingresso non autorizzato dall'esterno ai locali e ai dati di proprietà della nostra Organizzazione.

Terzo: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile.

Titolare del trattamento: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri.

Trattamento: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.

Violazione dei dati personali: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

2. Finalità della raccolta dati e dei trattamenti.

CRI COMITATO DI CHIERI svolge:

- Servizi di emergenza-urgenza su incarico dell'Azienda Ospedaliera Universitaria Città della Salute e della Scienza di Torino.
- Servizi di trasporto sanitario di pazienti, di pazienti nefropatici, disabili.
- Servizi di trasporto sociale di persone disabili.
- Servizi di assistenza sanitaria ad eventi e manifestazioni.
- Formazione sociale e sanitaria, breve e ricorrente, nel campo del primo soccorso e della prevenzione sanitaria.
- attività "Officine della salute" progetto per migliorare l'accesso ai servizi sociosanitari delle fasce di popolazione rientranti in uno stato di fragilità, attraverso la costruzione e l'offerta di una rete di servizi di assistenza sanitaria. L'avvio di tale progetto è previsto nel mese di aprile/maggio in collaborazione con il Comitato Nazionale di Croce Rossa Italiana.

Utilizza, per la realizzazione dei servizi, proprio personale dipendente e volontario. I dati trattati sono pertanto dati personali dei dipendenti e dei volontari, degli utenti dei servizi di trasporto sanitari e sociali, degli utenti dei servizi di formazione.

Nel Documento di Valutazione dei Rischi vengono di seguito specificati:

- Le finalità della raccolta e del trattamento dei dati
- La tipologia dei dati trattati,
- L'elenco dei trattamenti utilizzati,
- L'elenco degli archivi dati dove risiedono i dati trattati,
- L'elenco delle sedi e degli uffici dove i dati vengono conservati e trattati,
- L'individuazione dei sistemi di elaborazione utilizzati per il trattamento.

In questa sezione sono specificate le finalità della raccolta dati effettuati CRI Comitato di Chieri con l'indicazione della natura dei dati trattati, della struttura che effettua il trattamento.

Le finalità della raccolta dati effettuato da CRI Comitato di Chieri, sono i seguenti e riguardano:

- La gestione delle risorse umane, (dipendenti e volontari) utilizzati per la realizzazione dei servizi di trasporto sanitario e sociale.
- La gestione dei servizi di trasporto sanitario di emergenza urgenza.

- La gestione dei servizi di trasporto sociale.
- La gestione dei servizi di assistenza sanitaria ad eventi e manifestazioni.
- La progettazione e realizzazione di servizi formativi, di formazione breve e ricorrente, in ambito sanitario.

Queste attività sono legittime, individuate e descritte nell'Atto Costitutivo e nello Statuto e normate da leggi nazionali e regionali. I servizi vengono realizzati in convenzione con le strutture sanitarie regionali, in primo luogo AREU, con le strutture sanitarie territoriali, singoli comuni. Possono essere erogati anche su richiesta diretta dei cittadini e delle imprese.

Di seguito si specificano la tipologia dei dati richiesti e gestiti ed i loro trattamenti.

CRI Comitato di Chieri tratta i seguenti dati delle persone fisiche:

a) Dati personali comuni

- Dati comuni del personale dipendente, necessari alla gestione del rapporto di lavoro, alla loro reperibilità, alla gestione delle comunicazioni personali, o richiesti ai fini fiscali e previdenziali od al pagamento delle prestazioni.
- Dati comuni dei volontari, necessari per la realizzazione dei servizi assegnati, concernenti la reperibilità e le comunicazioni con gli stessi, nonché inerenti a finalità assicurative o normative.
- Dati comuni degli utenti dei servizi di traporto sanitario o sociale e dei servizi di formazione sanitaria.

Tali dati vengono trattati sia in formato cartaceo che informatico e gestiti da personale incaricato del trattamento, sia dipendenti che volontari. I dati sono utilizzati essenzialmente per:

- L'erogazione dei servizi,
- La predisposizione delle attestazioni di partecipazione alla formazione, nelle forme eventualmente richieste dalle normative vigenti.

I dati possono essere gestiti e conservati anche, direttamente, sui portali degli enti convenzionati, (AREU) o di organizzazioni appartenenti al sistema nazionale della Croce Rossa Italiana. In questi casi la responsabilità della protezione dei dati ricade anche sugli enti convenzionati o partner, in quanto titolari del portale informatico.

b) Dati personali "particolari" (sensibili)

- Dati del personale dipendente, conseguenti il rapporto di lavoro, inerenti cioè i rapporti con gli enti previdenziali ed assistenziali, i certificati di malattia, l'iscrizione alle organizzazioni sindacali, certificazioni del casellario giudiziario.
- Dati dei volontari riguardanti lo stato di salute.
- Dati degli utenti dei servizi sanitari, concernenti lo stato di salute o disabilità.

Questi dati vengono trattati sia in formato cartaceo che informatico e gestiti dal personale incaricato in modo riservato e protetto; possono essere trasmessi, alle istituzioni pubbliche convenzionate o partner, per la

gestione delle procedure obbligatorie. Possono essere ricevuti/inviati anche per mail, che vengono conservate sul server destinati alla posta elettronica (protetto con sistemi antivirus e firewall).

Per ciascuno trattamento sono riportate le seguenti informazioni:

Finalità e processo	Indicazione della finalità della raccolta dati e del processo operativo
Descrizione sintetica	Specificazione dell'attività che viene svolta per realizzare il processo
Natura dei dati trattati	Viene detto se tra i dati trattati vi sono anche dati sensibili, oltre ai dati personali
Struttura di riferimento	Indica la funzione o l'ufficio all'interno del quale viene effettuato il trattamento dei dati
Altre funzioni che concorrono al trattamento	Nel caso in cui al trattamento dei dati concorrono più funzioni, o servizi esterni, vengono citati nella tabella
Archivio	Nome o identificativo dell'archivio in cui sono conservati i dati che sono trattati
Ubicazione fisica dei supporti di memorizzazione:	Contiene l'indicazione del luogo in cui risiedono fisicamente i dati, cartacei ed informatici
Tipologia di dispositivi di accesso	Sono gli accessi fisici o quelli digitali, richiesti o usati nel trattamento dei dati

2.1. Finalità e processi gestiti: informazioni di base

Finalità e processo	Descrizione sintetica	Natura dei dati trattati		Struttura di riferimento	Altre strutture che concorrono al trattamento
Gestione del personale e dei volontari	Raccolta dati per l'assunzione e l'amministrazione del personale e la gestione dei volontari	S	G	Segreteria amministrativa	FP Consulting Srl – Gi Group Spa
Gestione Contabile	Elaborazione dei dati ai fini amministrativi, contabili e fiscali	S	G	Segreteria amministrativa	Studio Boidi & Partners – Dott. Danna Federico (revisore contabile)
Gestione dei servizi di trasporto di emergenza urgenza	Raccolta dati per la realizzazione dei servizi di trasporto sanitario di emergenza urgenza	S	G	Segreteria	A.O.U. Città della Salute e della Scienza di Torino
Gestione dei servizi di trasporto sanitario	Raccolta dati per la realizzazione dei servizi di trasporto sanitario	S	G	Segreteria	ASL TO5 – ASL Città di Torino

Finalità e processo	Descrizione sintetica	Natura dei dati trattati		Struttura di riferimento	Altre strutture che concorrono al trattamento
Gestione dei servizi di trasporto sociale	Raccolta dati per la realizzazione dei servizi di trasporto sociale	S	G	Segreteria	Comune di Chieri
Gestione dei servizi di assistenza eventi	Raccolta dati per la realizzazione di servizi	S	G	Segreteria	Associazioni sportive e culturali, pro loco
Erogazione di servizi di formazione sanitaria	Raccolta dati per la realizzazione di servizi di formazione		G	Segreteria	Portale formazione sanità Regione Piemonte

Tabella 1 - Finalità e processi gestiti: informazioni di base

2.2. Elenco delle finalità e dei processi: descrizione degli strumenti utilizzati.

Finalità e processo	Archivi	Ubicazione fisica dei supporti di memorizzazione	Tipologia di dispositivi di accesso
Gestione del personale e dei volontari	Personale e volontari	Armadi chiusi Sistema informativo interno	Ufficio chiuso al pubblico Personal computer in rete locale e remota
Gestione dei servizi di trasporto di emergenza	Utenti dei servizi di emergenza	Sistema informativo in rete esterna	Locali non accessibili al pubblico. PC dedicato in rete con AOU Città della Salute e della Scienza di Torino
Gestione dei servizi di trasporto sanitario	Utenti dei servizi sanitari	Armadi chiusi Sistema informativo interno	Locali non accessibili al pubblico. Personal computer in rete locale e remota
Gestione dei servizi di trasporto sociale	Utenti dei servizi sociali	Armadi chiusi Sistema informativo interno	Locali non accessibili al pubblico. Personal compute in rete locale e remota
Erogazione di corsi di formazione	Partecipanti ai servizi di formazione	Armadi chiusi Sistema informativo interno	Ufficio chiuso al pubblico Personal computer in rete locale e remota e remota

Tabella 2 - Elenco delle finalità e dei processi: descrizione degli strumenti utilizzati

I dati trattati vengono conservati nelle seguenti modalità:

2.3. Periodo di conservazione dei dati.

Tipologia di dati	Tempo di conservazione
Data anagrafici e sensibili degli utenti dei servizi sanitari e sociali	Per il periodo d'uso ed al massimo per 10 anni
Dati anagrafici dei partecipanti ai corsi di formazione contenuti nelle schede di iscrizione	Per il periodo d'uso ed al massimo per 5 anni
Attestazioni di partecipazione al corso di formazione	Per un massimo di 10 anni
Dati anagrafici e fiscali dei dipendenti	Per 10 anni dopo la cessazione dell'incarico per dimissioni o pensionamento
Dati anagrafici dei volontari	Per 2 anni dopo la cessazione dell'incarico

Tabella 3 - Periodo di conservazione dei dati.

2.4. Descrizione delle sedi dei sistemi di trattamento dei dati personali.

Nessun dato viene diffuso all'estero in paesi extra-europei.

CRI COMITATO DI CHIERI tratta e conserva i dati sopra descritti nelle seguenti sedi operative:

Id sede	Nome sede	Indirizzo della sede
01	CRI COMITATO DI CHIERI	Strada San Silvestro, 14 10023 Chieri (TO)
02	CRI COMITATO DI CHIERI	Parco della Rimembranza 9 10020 Pecetto Torinese (TO)
03	CRI COMITATO DI CHIERI	Via Pietra del Gallo 2 10025 Pino Torinese (TO)

I dati sopradescritti vengono trattate e conservati in fascicoli riposti in schedari od armadi dotati di chiusura presenti nei diversi uffici. Le sedi dove sono trattati i dati sono dotate di porte che vengono regolarmente chiuse a chiave al termine delle attività. La sicurezza degli stabili è altresì garantita da sistemi di sorveglianza.

Gli spazi adibiti ad uffici amministrativi sono sempre presidiati ed il loro accesso è controllato. I dati presenti negli archivi informatici sono trattati attraverso reti locali e remote di personal computer e server. Il sistema informativo è dotato di computer in rete con connessione internet protetta tramite firewall e antivirus.

Le caratteristiche tecniche del sistema informatico sono le seguenti:

- sistema informatico basato su rete con architettura Client-Server e servizi intranet ed internet.

Sono presenti apparecchiature hardware con funzioni di server, unità di accesso per gli utenti, periferiche di acquisizione immagine, periferiche di stampa in rete e locali, dispositivi di connessione verso reti internet condivise, dispositivi di protezione degli accessi interni ed esterni, strumenti dedicati all'archiviazione ed al salvataggio dei dati, sistemi di accesso remoto.

Il sistema informativo non è accessibile dall'esterno se non per mezzo di connessioni protette da rete VPN o da connessioni provenienti solo da indirizzi IP attendibili.

3. Distribuzione dei compiti e delle responsabilità

In questa sezione è costruita una mappa che associa ad ogni funzione/ufficio i trattamenti da questa effettuati, descrivendo sinteticamente l'organizzazione della struttura e le relative responsabilità.

Informazioni essenziali.

Struttura aziendale	È lo stesso identificativo usato nelle tabelle precedenti.
Responsabilità della struttura	Indica il ruolo o la qualifica del responsabile della struttura
Trattamenti operati dalla struttura	Contiene l'elenco dei trattamenti per i quali ciascuna struttura ha la responsabilità.
Compiti della struttura	Contiene una descrizione sintetica dei compiti assegnati alla struttura in ciascuno dei trattamenti di competenza.

3.1. Strutture aziendali preposte ai trattamenti.

Struttura	Responsabile	Trattamenti operati dalla struttura	Compiti della struttura
Segreteria	Presidente	Gestione del personale e dei volontari	Gestione dei dati del personale, dei volontari per la loro gestione amministrativa, contabile, assicurativa, fiscale e tributaria
Segreteria	Presidente	Raccolta dati per la realizzazione dei servizi di trasporto sanitario di emergenza urgenza	Gestione dei dati delle persone soccorse e trasportate per i servizi di emergenza urgenza
Segreteria	Presidente	Raccolta dati per la realizzazione dei servizi di trasporto sanitario	Gestione dei dati per la realizzazione dei servizi di trasporto sanitario e la gestione delle procedure organizzative ed amministrative connesse
Segreteria	Presidente	Raccolta dati per la realizzazione dei servizi di trasporto sociale	Gestione dei dati per la realizzazione dei servizi di trasporto sociale e la gestione delle procedure organizzative ed amministrative connesse

Struttura	Responsabile	Trattamenti operati dalla struttura	Compiti della struttura
Segreteria	Responsabile di segreteria corsi	Gestione dei dati degli utenti dei corsi di formazione	Gestione dei dati dei partecipanti per la realizzazione dei servizi formativi.

Tabella 4 - Strutture aziendali preposte ai trattamenti

I dati sensibili, quando sono presenti, sono trattati unicamente da persona autorizzate, incaricate del trattamento, nominate dal Titolare, con accesso controllato da apposite procedure. La persona incaricato del trattamento ne cura l'archiviazione e l'accesso controllato degli altri operatori. I dati sensibili, quando sono su supporto cartaceo, sono fisicamente separati dai dati comuni; quelli su supporto informatico sono separati attraverso le procedure di accesso controllato.

3.2. Archivi, responsabili, incaricati del trattamento.

Archivio	Responsabile di funzione	Struttura che esegue il trattamento	Incaricato del trattamento
Personale e volontari	Presidente	Segreteria	Dipendenti e volontari incaricati
Utenti dei servizi sanitari di emergenza urgenza	Presidente	Segreteria	Dipendenti e volontari incaricati
Utenti dei servizi di trasporto sanitari	Presidente	Segreteria	Dipendenti e volontari incaricati
Utenti dei servizi di trasporto sociali	Presidente	Segreteria	Dipendenti e volontari incaricati
Partecipanti ai servizi di formazione	Responsabile Formazione	Segreteria	Dipendenti e volontari incaricati

Tabella 5 – Archivi, responsabili, incaricati del trattamento.

4. Analisi dei rischi che incombono sui dati.

In questa sezione vengono individuati i principali eventi potenzialmente dannosi per la sicurezza dei dati, vengono valutate le possibili conseguenze e la loro gravità e descritte le misure di protezione previste.

Informazioni essenziali.

Elenco degli eventi	Contiene l'elenco degli eventi che possono generare danni e che comportano quindi rischi per la sicurezza dei dati personali
Impatto sulla sicurezza dei dati	Contiene la descrizione delle principali conseguenze individuate per la sicurezza dei dati, in relazione a ciascun evento ed una valutazione della gravità delle stesse, anche in relazione alla probabilità stimata dell'evento.
Riferimento misure d'azione	Contiene il riferimento alla contromisura adottata.

In termini generali il rischio legato alla gestione dei dati trattati da CRI COMITATO DI CHIERI si può definire basso, sia per i dati comuni sia per i dati sensibili.

La valutazione dei rischi viene svolta utilizzando due indicatori:

- la possibilità di accadimento dell'evento critico (improbabile, possibile, probabile)
- la gravità del danno per la protezione delle persone riguardo i loro dati, che hanno affidato al Comitato (lieve, media, grave).

Gravità / Probabilità	Improbabile (2)	Possibile (4)	Probabile (6)
Lieve (2)	4	8	12
Medio (4)	8	16	24
Grave (6)	12	24	36

Ad ogni indicatore vengono assegnati 2-4-6 punti; viene costruita in questo modo una scala di valutazione che definisce anche il livello di rischio e le priorità di intervento / attenzione.

a	Rischio inesistente o limitato (4 punti)	Nessun intervento da realizzare, da verificare annualmente
b	Rischio basso (8 punti)	Nessun intervento da realizzare ma da controllare semestralmente
c	Rischio medio (12 punti)	Viene richiesto un presidio ed un controllo costante
d	Rischio medio-grave (24 punti)	Viene richiesto un piano di intervento per una progressiva messa in sicurezza
e	Rischio grave (36 punti):	Viene richiesto un intervento immediato di messa in sicurezza e miglioramento

4.1. Analisi dei rischi

Evento		Impatto sulla sicurezza dei dati		Riferimento misure di azione
		Descrizione	**Gravità stimata**	
Comportamenti degli operatori	Furto di credenziali di autenticazione	Modifica non autorizzata di dati	Media	Le credenziali sono personali e conservate dall'incaricato
	Carenza di consapevolezza, disattenzione od incuria	Modifica non corretta dei dati	Bassa	Il personale è formato alla gestione delle procedure operative
	Comportamenti sleali o fraudolenti	Modifica non autorizzata di dati	Bassa	Il personale è coinvolto e motivato

Evento		Impatto sulla sicurezza dei dati		Riferimento misure di azione
		Descrizione	Gravità stimata	
	Errore materiale	Modifica non corretta dei dati	Bassa	Il personale è formato alla gestione delle procedure
Eventi relativi agli strumenti tecnologici	Azioni di *virus* informatici o di codici malefici	Rischio di perdita e danneggiamento	Bassa	Antivirus sul SI aggiornato periodicamente ed automaticamente
	Spamming o altre tecniche di sabotaggio	Rischio di perdita e danneggiamento	Bassa	Il SI è protetto contro gli accessi non autorizzati da antivirus e firewall
	Malfunzionamenti, indisponibilità o degrado degli strumenti	Rischio di perdita e danneggiamento	Bassa	Gli strumenti sono costantemente manutenuti e controllati da un servizio di assistenza
	Accessi esterni non autorizzati	Rischio di modifica non autorizzata	Media	Il server è collocato in un ambiente ad accesso controllato
	Intercettazione di informazioni in rete	Rischio di modifica non autorizzata	Bassa	Il SI è protetto contro le intrusioni in rete da antivirus e firewall; le password vengono periodicamente aggiornate
Eventi relativi al contesto	Accessi non autorizzati a locali ad accesso ristretto	Rischio di manipolazione e perdita di dati	Bassa	I dati sono conservati in locali non direttamente accessibili agli utenti od a estranei
	Asportazione e furti di strumenti contenenti dati	Rischio di perdita dei dati	Bassa	Le sedi sono protette con sistemi di sicurezza
	Eventi distruttivi, naturali od artificiali, dolosi, accidentali o dovuti ad incuria	Rischio di perdita dei dati	Bassa	I dati sono duplicati su NAS e sul server, con backup periodici
	Guasto ai sistemi complementari (impianto elettrico, climatizzazione ecc.)	Rischio di perdita dei dati recenti	Bassa	È presente un sistema di continuità di emergenza, per il gestore della rete
	Errori umani nella gestione della sicurezza fisica	Rischio di perdita di dati	Bassa	Il sistema di sicurezza è monitorato periodicamente

Tabella 6 - Analisi dei rischi

5. Misure organizzative e tecniche per la protezione dei dati

In questa sezione sono riportate in forma sintetica le misure in essere o da adottare a contrasto dei rischi individuati dall'analisi dei rischi. Per misure si intendono sia lo specifico intervento tecnico ed organizzativo di prevenzione, contrasto e riduzione di una minaccia, ma anche le attività di controllo e monitoraggio periodici.

Informazioni essenziali.

Misure	La descrizione sintetica della misura di sicurezza adottata
Rischio contrastato	Per ogni misura si indica il riferimento all'analisi dei rischi che ne ha motivato l'adozione
Archivio interessato	Si riporta l'identificativo dell'archivio e dei trattamenti interessati per ciascuna delle misure adottate
Riferimento scheda analitica	Contiene il riferimento alla scheda analitica descrittiva della misura
Attivazione misure	Per ogni misura si indica se è già in essere oppure se deve essere attivata
Periodicità e modalità di controllo	Contiene l'indicazione della periodicità con cui sono verificate le funzionalità e l'efficacia della misura e della struttura operativa che ne ha la responsabilità

Tabella 7 - Le misure di sicurezza adottate o da adottare

5.1. Informazioni descrittive analitiche delle misure di sicurezza

Si allegano delle schede analitiche sulle singole misure di sicurezza, specificando le attività di verifica e controllo. Gli aspetti presi in esame nelle schede sono:

- la minaccia che si intende contrastare,
- la tipologia della misura di sicurezza,
- le informazioni relative alla responsabilità dell'attuazione e della gestione della specifica misura.

5.2. Le misure di sicurezza adottate o da adottare

Misura	Rischio contrastato	Rif. Scheda analitica	Misura già in essere o da adottare	Periodicità / responsabilità controlli
Le sedi sono protette con sistemi di sorveglianza	Rischio di modifica non autorizzata	Cap. 5.3	Già in essere	Costante, Amministrazione
Le credenziali sono conservate direttamente dagli incaricati	Modifica non autorizzata di dati	Cap. 5.3	Già in essere	Semestralmente, automaticamente
Il personale è selezionato, formato e motivato	Modifica non corretta dei dati	Cap. 5.3	Già in essere	Annualmente, Presidente
Antivirus sul SI aggiornato periodicamente	Modifica non autorizzata di dati	Cap. 5.3	Già in essere	Il server viene automaticamente
Il SI è protetto contro gli accessi non autorizzati	Modifica non corretta dei dati	Cap. 5.3	Già in essere	Semestralmente, Amministrazione
Gli strumenti sono manutenuti ed aggiornati	Rischio di perdita e danneggiamento	Cap. 5.3	Da adottare	Periodica ed a chiamata per l'assistenza

Misura	Rischio contrastato	Rif. Scheda analitica	Misura già in essere o da adottare	Periodicità / responsabilità controlli
Il SI è protetto contro le intrusioni	Rischio di perdita e danneggiamento	Cap. 5.3	Già in essere	Periodica ed a chiamata per l'assistenza
I dati sono conservati in locali non accessibili agli utenti	Rischio di perdita e danneggiamento	Cap. 5.3	Già in essere	Costante, Amministrazione
I dati sono duplicati e conservati in luoghi diversi	Rischio di modifica non autorizzata	Cap. 5.3	Già in essere	Costante, Amministrazione
È presente un sistema di continuità, gestito dal gestore dei server	Rischio di manipolazione e perdita di dati	Cap. 5.3	Già in essere	Dopo 30 minuti di blackout, spegnimento automatico del S.I.
Il sistema di sicurezza è monitorato periodicamente	Rischio di perdita dei dati	Cap. 5.4	Già in essere	Costanti, da sistema automatici

Tabella 8 - Le misure di sicurezza adottate o da adottare

5.3. Le misure tecniche di protezione dei dati

La protezione di aree e locali

I locali del Comitato CRI di Chieri sono situati all'interno di un fabbricato di 2 piani con ingressi presidiati, sia per l'ingresso delle persone tramite porta presidiata da personale, sia per l'ingresso dei mezzi tramite cancello azionabile elettricamente.

Gli impianti ed i sistemi di cui è dotata la nostra Organizzazione sono soddisfacenti, in funzione della tecnologia disponibile e sostenibile, al fine di garantire le opportune misure di sicurezza, al trattamento di dati personali da essa svolti.

Autorizzazioni di accesso, custodia e archiviazione di atti, dati e documenti

Alle persone autorizzate al trattamento viene spiegato di accedere ai soli dati strettamente necessari per svolgere i compiti, per poi restituirli all'archivio, al termine di tale ciclo.

Le cartelle elettroniche sono dotate di privilegi di accesso a seconda delle autorizzazioni delle singole persone.

Cautele particolari sono previste per gli atti, documenti e supporti contenenti dati sensibili: in questi casi viene prescritto di provvedere al controllo ed alla custodia in modo tale che ai dati non possano accedere persone prive di autorizzazione. A tale fine le persone autorizzate sono state dotate di:

- armadi e cassetti sia muniti di serratura che non
- stanze chiudibili a chiave

devono riporre i documenti, contenenti dati sensibili negli archivi controllati prima di assentarsi dal posto di lavoro, anche temporaneamente. Per quanto concerne l'archiviazione, il Titolare ha adibito apposite aree, nelle quali conservare ordinatamente documenti, atti e supporti contenenti dati.

Gli archivi contenenti dati sensibili sono controllati mediante l'accesso regolato da badge con limitazione di accesso in base alle necessità e ai ruoli.

User-ID e sistemi di parole chiave (password)

Per i trattamenti effettuati con strumenti elettronici (elaboratori in rete locale, programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato), si adotta un sistema di autenticazione informatica per disciplinare gli accessi a tutti gli strumenti elettronici tramite l'utilizzo di User ID e Password a livello di:

- User ID e Password all'accensione del PC come utente o come amministratore
- User ID e Password per l'accesso ai programmi applicativi gestionali
    - GAIA
    - Gestione CRI

Regole per la definizione delle password

Le regole per la definizione delle credenziali sono così definite (a meno di limitazioni del singolo dispositivo):

- Lunghezza di almeno 10 caratteri
- I caratteri scelti devono essere alfanumerici (sono accettate sia lettere maiuscole che minuscole, numeri o simboli) e deve di includere almeno un simbolo tra: +(. \ * ? [^] $ ( ) { } = ! < > | : -)

Sicurezza delle trasmissioni

Le trasmissioni di dati devono esser protette in maniera da rendere i dati inaccessibili a terze parti indesiderate. Le misure adottate sono cifratura, utilizzo di router portatili con firewall (per garantire che i dati non siano fisicamente raggiungibili) e Firewall.

Antivirus/antimalware

I sistemi di protezione sono aggiornati automaticamente attraverso il semplice accesso ad Internet. Tale sistema di protezione viene aggiornato ed attivato automaticamente ad ogni avvio degli stessi terminali.

- Sophos Antivirus e Sophos InterceptX contro i malware. Il software è di fascia "enterprise" con licenza a pagamento.

Aggiornamento dei sistemi e patch management

Periodicamente un tecnico del fornitore di servizi IT si occupa di fare gli aggiornamenti a sistemi e software obsoleti o con vulnerabilità note per evitare che i sistemi siano inutilmente esposti a minacce informatiche.

Backup

L'organizzazione del backup e della struttura dei dati sottoposta a backup viene individuata dall'Incaricato **delle copie di sicurezza delle banche dati**.

Il backup dei dati viene eseguito in automatico tutte le notti su apposito supporto, con rapporto di corretta esecuzione. I supporti sono inoltre duplicati quotidianamente anche in cloud con specifico contratto.

Ci sono 3 livelli di backup: 2 gestiti internamente e uno dal fornitore di servizi IT.

- Backup dei dati su NAS interno
- Backup del server su NAS interno
- Backup del server "off site" presso il fornitore di servizi IT.

Il terzo invece lo gestiamo noi e lo verifichiamo quotidianamente

Dove vengono salvate le copie di backup?

- I backup gestiti da CRI sono su NAS interno di CRI, sotto la responsabilità di CRI.
- Il backup eseguito presso Techsystem è attualmente conservato su backup in cloud con file criptati e protetti da password, sotto la responsabilità di Techsystem.

Un paio di volte all'anno l'**Incaricato delle copie di sicurezza delle banche dati** esegue dei test di ripristino per assicurarsi che il supporto e la procedura di backup siano perfettamente funzionanti.

Videosorveglianza CCTV

Per garantire la protezione e sicurezza del proprio patrimonio immateriale, del personale, dei clienti e dei fornitori, è installato un sistema di videosorveglianza CCTV.

Le immagini rilevate e registrate dall'impianto di videosorveglianza si collocano nella categoria dei dati personali, in quanto le persone riprese sono (potenzialmente ed effettivamente) riconoscibili.

L'installazione di un sistema di videosorveglianza ha **finalità** di controllo e identificazione dei visitatori che si accingono ad accedere alla sede e di protezione dell'area dai tentativi di intrusione in relazione all'esigenza di perseguire fini di **tutela di persone e beni** rispetto a possibili aggressioni, furti, rapine, danneggiamenti, atti di vandalismo.

Ogni uso superfluo della videosorveglianza è escluso. L'attuale sistema di videosorveglianza consente di monitorare:

- Le sedi dedicate in corrispondenza dell'area perimetrale esterna, e in corrispondenza di aree interne considerate sensibili (aperte al pubblico)

Non è previsto **alcun collegamento diretto del sistema di videosorveglianza** con le forze dell'ordine e pertanto non sarà possibile la visione in tempo reale delle immagini da postazione remota.

Il comitato garantisce però che l'esistenza del sistema di videosorveglianza è conosciuta dai dipendenti attraverso una adeguata informativa agevolmente rilevabile e dalla presenza di appositi cartelli nelle zone oggetto di ripresa.

In tale modo gli interessati sono sempre informati che stanno per accedere o che si trovano in una zona videosorvegliata.

5.4. Le misure organizzative di protezione dei dati

Informative e lettere di riservatezza per persone autorizzate dipendenti e volontari

Dipendenti e volontari si impegnano a mantenere la riservatezza dei dati e dei dati personali di cui vengono a conoscenza durante il loro servizio in CRI Chieri e sottoscrivono un'apposita lettera di riservatezza: "Lettera di riservatezza per l'autorizzazione di dipendenti e volontari"

I nuovi volontari e dipendenti sottoscrivono la lettera di riservatezza al momento in cui diventano soci. Al momento della consegna delle divise, ricevono la lettera dal Responsabile del magazzino vestiario anche la lettera di riservatezza che verrà poi consegnata all'amministrazione.

Uso di fotocopiatrici, scanner, supporti di memoria rimovibili

Non è consentito effettuare operazioni di copiatura, salvo le operazioni di backup, dei dati personali, se non per esigenza lavorativa giustificabile. Le copie di dati personali o sensibili devono essere distrutte al termine della necessità di trattamento in modo da non consentirne il recupero. L'uso di apparecchiature di copiatura non è generalmente consentito per fini diversi da quelli aziendali. In ogni caso l'autore delle copie è responsabile per il contenuto delle stesse obbligandosi a rispettare la normativa vigente (ad esempio quella in materia di diritto d'autore).

Uso dei telefoni

L'uso di telefoni è consentito per motivi legati alle attività del comitato. In casi particolari anche per motivi personali. Non possono essere utilizzati né telefoni per trasmettere dati sensibili.

Pseudonimizzazione e mascheramento

Consiste nel trattamento dei dati personali in modo tale che non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile.

Nella nostra azienda **NON È** messa in atto la pseudonimizzazione.

Ci sono dei casi in cui invece vengono messe in atto delle misure di **mascheramento**: i casi più comuni sono:

- I biglietti delle missioni devono essere ripiegati in modo da non rendere visibili i nomi degli assistiti, prima di essere pubblicati in bacheca
- Le lettere e in generale i documenti con riportato il nome della persona, devono essere piegati in modo da non rendere visibili i nomi dei destinatari o essere messi all'interno di una busta

Raccolta del consenso degli interessati

I dati degli interessati possono essere raccolti durante eventi, convegni o altro tipo di incontri. La raccolta del consenso avviene tramite apposita modulistica per utenti o utenti assistiti.

Cessione dati all'esterno

SONO VIETATE duplicazioni di supporti contenenti dati personali (es. documenti / screenshot su cifratura, ecc.) se non espressamente autorizzata dal **PRESIDENTE**.

Nei casi in cui i trattamenti di dati vengano affidati all'esterno della struttura del Titolare, in conformità a quanto previsto dal Regolamento CE 679/2016, si adottano i criteri descritti al capitolo 7 per garantire che il soggetto destinatario adotti misure di sicurezza conformi a quelle minime. Nel dettaglio, il destinatario esterno viene nominato dal Titolare come Responsabile del Trattamento dei dati in outsourcing, mediante apposita lettera sottoscritta.

Comunicazione verbale

Anche durante la comunicazione verbale, i dati personali di colleghi, assistiti e altri volontari dovranno essere sempre trattati in maniera lecita, corretta e trasparente, facendo attenzione a non fornire informazioni personali a persone non autorizzate durante le conversazioni telefoniche o di persona.

Se non per finalità inerenti alla prestazione del servizio, i dati personali di dipendenti, volontari e assistiti non devono essere ricercati all'interno dei sistemi informativi del comitato, né comunicati ad alta voce quando si è al telefono o si parla con terzi.

Conservazione ed eliminazione dei dati

Sul Registro dei trattamenti è stato documentato il periodo di conservazione dei dati in base ai requisiti minimi di legge, come riportato nella tabella 2.3. Tale periodo indica il periodo di conservazione massimo dei dati personali e, a parte un periodo ragionevole basato su motivazioni organizzative, al termine del periodo tali dati devono essere eliminati, sia i dati elettronici, sia i dati cartacei.

Ripristino dati (Disaster recovery)

Per i server sono previste procedure di backup, attraverso le quali viene periodicamente effettuata una copia di tutti i dati presenti nel sistema.

In particolare, tali misure garantiscono la possibilità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico, fatto salvo il caso di eventi di forza maggiore (per esempio incendio o inagibilità dei locali) per i quali, alla data odierna, ci si affida alle attività di mirroring dei sistemi informativi effettuate sempre da parte dell'IT. In particolare, dovranno essere considerati almeno i seguenti aspetti:

- le attività che dovranno essere eseguite per il ripristino delle normali attività
- le specifiche attività che dovranno essere eseguite per rimediare temporaneamente l'interruzione (ad esempio lo spostamento di servizi essenziali in locazioni temporanee, l'adozione di processi alternativi temporanei, ecc.)
- verifica e di test della procedura
- l'individuazione dei responsabili per l'esecuzione delle procedure attraverso anche, se ritenuto opportuno, un piano di reperibilità
- la scala dei tempi di reazione e ripristino alla normalità dal verificarsi dell'evento che ha causato l'interruzione

Comportamento in caso di incidente (DATA BREACH)

Comitato di Chieri O.d.V. ha attivato una procedura di gestione degli incidenti che riguardano la sicurezza dei dati personali.

Si definisce incidente qualsiasi evento che possa avere un impatto tale da mettere in pericolo la sicurezza dei dati personali degli interessati, dal punto di vista della riservatezza, integrità o disponibilità. Nel caso in cui si tratti di un incidente che comporti la perdita di riservatezza di una

quantità consistente di dati personali, si procederà all'elaborazione di una specifica relazione da comunicare al Garante della privacy (LINK al modulo del garante per la Privacy).

Come esempi vengono descritte le seguenti definizioni:

- Riservatezza:
  - Questioni relative alle esigenze degli utenti e dei pazienti in materia di riservatezza dei dati personali
  - Rilevamento di accessi eccessivi o imprevisti
- Integrità:
  - Dati non aggiornati
  - Dati non corretti
- Disponibilità:
  - Incidenti causati da problemi presenti nelle copie di sicurezza o disponibilità di informazioni al personale autorizzato ad usarlo
  - Mancanza di permesso di accesso ai dati da parte di personale che ne ha bisogno per motivi di lavoro

Regole generali da seguire in caso di incidente:

- In caso di incidente o di sospetto incidente deve esserne data immediata comunicazione al Responsabile della Privacy. L'utente deve evitare di compiere qualsiasi attività od operazione sul sistema che possa pregiudicare in qualche modo la rilevazione dell'incidente e le indagini conseguenti
- In caso di incidente o sospetto incidente legato alla rete l'utente può scollegare fisicamente la macchina dalla rete. Per nessun motivo la macchina deve essere spenta. L'utente deve fornire agli incaricati della sicurezza tutta la collaborazione e le informazioni richieste relative all'incidente.

6. Interventi formativi

In questa sezione sono riportate le informazioni necessarie per disporre di un quadro sintetico dell'impegno formativo che si prevede di sostenere in attuazione della normativa.

Informazioni essenziali.

Corso di formazione	Riporta l'identificativo del corso di formazione
Descrizione sintetica	Contiene la descrizione sintetica degli obiettivi del corso
Classi di incarico interessate	Contiene l'elenco delle classi omogenee di incarico a cui il corso è destinato e/o le tipologie di incaricati interessati
Calendario	Periodo di svolgimento degli interventi di informazione e formazione

6.1. Formazione dei collaboratori

Corso di formazione	Descrizione sintetica	Classi di incarico interessate	Calendario
Formazione generale alle norme sulla privacy	2 ore di presentazione del Documento di Valutazione dei Rischi e delle norme del Regolamento UE 2016/679 da DPO	Responsabili dei servizi	Dal 25.9.2023 al 30.9.2023
Formazione degli incaricati del trattamento	2 ore sul Documento di Valutazione dei Rischi ed i regolamenti da DPO	Dipendenti e volontari incaricati del trattamento	Dal 25.9.2023 al 30.9.2023
Funzionamento di anti malware e backup	Formazione sul Funzionamento di anti malware e backup da parte di Techsystem	Dipendenti e volontari incaricati del trattamento	Dal 25.9.2023 al 30.9.2023

Tabella 9 - Formazione dei collaboratori

7. Trattamenti affidati all'esterno

Obiettivo di questa sezione è di redigere un quadro sintetico delle attività trasferite a terzi che comportano il trattamento dei dati personali, con l'indicazione del quadro contrattuale in cui tale trasferimento si inserisce, in riferimento alla protezione dei dati personali.

Informazioni essenziali

Attività delegata	Contiene l'identificativo dell'attività che è stata delegata a terzi
Descrizione sintetica	Contiene una descrizione sintetica dell'attività
Dati personali, sensibili o giudiziari interessati	Contiene l'elenco dei dati personali, sensibili oggetto del trattamento per la realizzazione delle attività delegate
Soggetto delegato	Riporta l'identificativo della società o del consulente a cui è stato affidato l'incarico
Descrizione dei criteri per garantire l'adozione delle misure	Impegni contrattuali assunti dal soggetto esterno, sulla correttezza del trattamento dei dati

Gli impegni previsti contrattualmente sono precisati in una dichiarazione:

1. di essere consapevole che i dati che tratterà nell'espletamento dell'incarico ricevuto sono dati personali e come tali sono soggetti all'applicazione del Regolamento UE,
2. di ottemperare agli obblighi previsti dal Regolamento UE,
3. di adottare le istruzioni specifiche eventualmente ricevute per il trattamento dei dati personali o di integrarle nelle procedure già in essere,
4. di impegnarsi a relazionare annualmente sulle misure di sicurezza adottate e di allertare immediatamente il proprio committente in caso di situazioni anomale o di emergenze,
5. di riconoscere il diritto del committente a verificare periodicamente l'applicazione delle norme di sicurezza adottate.

7.1. Trattamenti affidati all'esterno

Attività esternalizzata	Descrizione sintetica	Dati personali sensibili o giudiziari interessati	Soggetto esterno	Descrizione dei criteri per l'adozione delle misure
Gestione del personale	Gestione amministrativa del personale	Dati personali	FP Consulting Srl e Gi Group Spa	Contratto per la gestione del servizio con specificate le misure richieste per la sicurezza dei dati
Gestione Dei dati contabili	Gestione dati contabili di clienti, dipendenti, assistiti e fornitori	Dati personali	Studio Boidi & Partner e Dottor Danna Federico	Contratto per la gestione del servizio con specificate le misure richieste per la sicurezza dei dati
Gestione dei data base	Gestione dati contabili di clienti, dipendenti, assistiti e fornitori	Dati personali e particolari	Idea software Srl	Contratto per la gestione del servizio con specificate le misure richieste per la sicurezza dei dati

Tabella 10 - 8.1. Trattamenti affidati all'esterno

8. Cifratura dei dati o separazione dei dati identificativi

In questa sezione sono rappresentate le modalità di protezione adottate per i dati per cui è richiesta la cifratura o la separazione fra dati identificativi e dati personali, nonché i criteri e le modalità con le quali viene assicurata la sicurezza di tali trattamenti.

Informazioni essenziali

Dato	Contiene l'identificativo di un insieme di informazioni personali tra loro coerenti
Protezione scelta	Riporta la tipologia di protezione adottata, scelta fra quelle indicate dal codice od in base a considerazioni specifiche

Data di effettività	Contiene la data a partire dalla quale le misure adottate diventano operative
Tecnica adottata	Contiene una descrizione sintetica tecnica ed organizzativa della misura adottata

I dati sono trattati unicamente dagli incaricati e non sono comunicati esternamente. Non è richiesta pertanto alcuna misura di cifratura.

8.1. Cifratura o separazione dei dati identificativi.

Dato	Protezione scelta (cifratura/separazione)	Data di effettività	Tecnica adottata	
			Descrizione	Informazioni utili
Personale e volontari	Non applicabile			
Utenti servizi di emergenza urgenza	Non applicabile			
Utenti dei servizi sanitari	Non applicabile			
Utenti dei servizi sociali	Non applicabile			
Utenti servizi formativi	Non applicabile			

Tabella 11 - 9.1. Cifratura o separazione dei dati identificativi

9. Registri del trattamento dai dati

REGISTRO DEL TITOLARE

Titolare: CRI Comitato di CHIERI			
	Processi principali		
	Gestione del personale dipendente e dei volontari	Realizzazione di corsi di formazione	Servizi sanitari di emergenza urgenza
1. Finalità	Gestione amministrativa e fiscale dei dipendenti e dei volontari	Iscrizione al corso di formazione	Gestione del servizio di trasporto di emergenza urgenza

Titolare: CRI Comitato di CHIERI			
	Processi principali		
	Gestione del personale dipendente e dei volontari	**Realizzazione di corsi di formazione**	**Servizi sanitari di emergenza urgenza**
2. Dati	Dati anagrafici e fiscali, Iban; stato di famiglia per dipendenti; certificazioni mediche ed assicurative, dati giudiziari (L. 104)	Dati anagrafici, dati di contatto (residenza, telefono, mail – personali o aziendali)	Dati anagrafici e sanitari
3. Documento	Lettera di assunzione; documenti obbligatori della gestione amministrativa, assicurativa, fiscale e tributaria	Scheda di iscrizione al corso; attestato di partecipazione	Modulo AREU (MSB)
4. Presenza dati sensibili	Si, per i dipendenti ed i volontari dati sanitari, dati giudiziari; per i dipendenti iscrizione al sindacato,	No	Dati sulla salute
5. Incaricati	Amministrazione, Studio Grassi – Busto Arsizio	Segreteria	Equipaggio soccorritori, segreteria
6. Tipo di trattamento	Fogli di presenza; predisposizione dei cedolini paga e dei documenti assicurativi, fiscali e tributari. Per i volontari fogli presenza turni	Inserimento nel registro del corso, nel data base per le informazioni organizzative; conservazione ed estrazione, emissione attestato finale	Compilazione scheda operativa ed inserimento dei dati sul sistema AREU e sul gestionale interno
7. Luogo di conservazione dati generali	Segreteria Studio Grassi – Busto Arsizio	Segreteria; Sulla rete interna, sul server ed on line	Segreteria; Sulla rete interna e sul server
8. Luogo di conservazione dati sensibili	Segreteria Studio Grassi – Busto Arsizio	Nessun dato sensibile	Segreteria; Sulla rete interna e sul server
9. Tempo di conservazione	Per i dipendenti, 10 anno dopo la cessazione. Per i volontari 2 anni dopo la cessazione	Per il periodo di utilizzo e fino a 5 anni	Per il periodo di utilizzo e fino a 10 anni
10. Sistemi di protezione	Conservati: in armadi chiusi in luoghi riservati, con accessi riservati; sui server aziendali, locali e remoti, dotati di antivirus, firewall e sistemi di backup periodici	Conservati: in armadi chiusi in luoghi riservati, con accessi riservati; sui server aziendali, locali e remoti, dotati di antivirus, firewall e sistemi di backup periodici	Conservati: in armadi chiusi in luoghi riservati, con accessi riservati; sui server aziendali, locali, dotati di antivirus, firewall e sistemi di backup periodici
11. Diffusione dei dati	Diffusi solo agli enti istituzionali per obblighi normativi (Inps, Inail ecc.) Non sono diffusi all'estero.	Non sono diffusi; consegnati solo ai partecipanti e committenti	Ad AREU ed alla struttura ospedaliera, alle autorità giudiziarie

Tabella 12 - REGISTRO DEL TITOLARE

Titolare: CRI Comitato di CHIERI		
	Processi principali	
	Servizi di trasporto sanitari (tutti)	**Servizi di trasporto sociale**
1. Finalità	Gestione del servizio di trasporto sanitari	Gestione dei servizi di trasporto sociale
2. Dati	Dati anagrafici e sanitari	Dati anagrafici e sanitari
3. Documento	Scheda di richiesta di servizio	Scheda di richiesta di servizio
4. Presenza dati sensibili	Dati sulla salute	Dati sulla salute
5. Incaricati	Segreteria e operatori	Segreteria ed operatori
6. Tipo di trattamento	Compilazione scheda di richiesta, inserimento dati sul gestionale interno, conservazione	Compilazione scheda di richiesta, inserimento dati sul gestionale interno, conservazione
7. Luogo di conservazione dati generali	Segreteria; rete interna, server, su cloud	Segreteria; rete interna e server
8. Luogo di conservazione dati sensibili	Segreteria; rete interna, server, su cloud	Segreteria; rete interna e server
9. Tempo di conservazione	Per il periodo di utilizzo e fino a 10 anni	Per il periodo di utilizzo e fino a 10 anni
10. Sistemi di protezione	Conservati: in armadi chiusi in luoghi riservati, con accessi riservati; sui server aziendali, locali, dotati di antivirus, firewall e sistemi di backup periodici	Conservati: in armadi chiusi in luoghi riservati, con accessi riservati; sui server aziendali, locali e remoti, dotati di antivirus, firewall e sistemi di backup periodici
11. Diffusione dei dati	Se il servizio è in convenzione, all'ente convenzionato. Non sono diffuso all'estero	Se il servizio è in convenzione, all'ente convenzionato. Non sono diffusi all'estero

Data 19/4/2023

Timbro e Firma del Legale Rappresentante

_____

ALLEGATO 1: TABELLA DELLE PERSONE AUTORIZZATE ED INCARICATE DEL TRATTAMENTO DEI DATI

n.	Cognome e Nome	Area/Ruolo	Dati Personali	Dati sensibili			
				Personale	Emergenza 118	Trasporti sanitari	Trasporti sociali
1	GianPiero Del Tito	Presidente	X	X	X	X	X
2	Martano Michela	Segreteria	X	X	X	X	X
3	Monica Milan	Amministrazione	X	X	X	X	X
4	Giorgio Cavaglià	Segreteria	X	X	X	X	X
5	Fabrizio Raverdino	Coordinatore Tecnico	X		X	X	X
6	Elena Avidano	Amministrazione	X	X	X	X	X
7	Andrea Aulisi	DPO	X		X	X	X
8	Barbara Lazzerini	Volontari	X				
9	Gianni Morra	Volontari	X				
10	Luca Scavino	Responsabile sanitario	X	X	X	X	X
11	Nadia Actis	Volontari	X				

Data: 19/4/2023

Il Presidente: _____