

***DOCUMENTO PROGRAMMATICO  
PROTEZIONE DATI PERSONALI***

Redatto in base a Testo Unico 196 del 2003 (Codice Privacy)  
modificato per la RE 679 - 2016

---

**Pubblica Assistenza CROCE BIANCA SAVONA  
O.N.L.U.S.**

Corso Mazzini 60 rosso

Via Montenotte 30/1

- 17100 - Savona -

**INDICE**

1. Premessa
2. Definizioni
3. Elenco dei trattamenti di dati personali
4. Distribuzione dei compiti e delle responsabilità
5. Analisi dei rischi che incombono sui dati
6. Misure in essere e da adottare
7. Criteri e modalità di ripristino della disponibilità dei dati
8. Pianificazione degli interventi formativi previsti
9. Trattamenti affidati all'esterno
10. Cifratura dei dati o separazione dei dati identificativi

## **1. Premessa**

***Il presente documento, pur non essendo richiesto dalla Nuova Privacy, per scelta aziendale, viene mantenuto aggiornato per poter garantire una corretta transizione tra il precedente sistema Privacy e la nuova regolamentazione Europea RE679.***

*Il trattamento dei dati personali si svolge nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale ed al diritto alla protezione dei dati personali.*

*Il trattamento è effettuato assicurando un elevato livello di tutela dei diritti e delle libertà, nel rispetto dei principi di semplificazione, armonizzazione ed efficacia delle modalità previste per il loro esercizio da parte degli interessati, nonché per l'adempimento degli obblighi da parte del Titolare del trattamento.*

*I dati in possesso del Titolare per l'esercizio dell'attività riguardano i dati personali e sensibili riferiti ai clienti ed al personale ed i dati personali dei fornitori.*

*Il trattamento dei dati avviene principalmente con l'ausilio di strumenti elettronici ed è effettuato presso la sede della Società, e, per gli adempimenti di competenza, presso Strutture di consulenza esterne (come meglio riportato nelle tabelle che seguono).*

*I dati oggetto di trattamento sono:*

*a) trattati in accordo alle disposizioni di legge ;*

*b) raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati in altre operazioni del trattamento in termini compatibili con tali scopi; I requisiti formali richiesti per la validità del consenso al trattamento dei dati personali da parte degli interessati sono stati adeguati in base alla RE 679: in particolare, è previsto che tale consenso sia valido solo quando sia stato reso attraverso un atto positivo inequivocabile, rimanendo quindi esclusa la possibilità di presumerlo dall'inattività, dal silenzio dell'interessato o dalla preselezione di caselle.*

*c) esatti ed aggiornati;*

*d) pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati;*

*e) conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi o stabilito dalle leggi, per i quali essi sono stati raccolti e successivamente trattati.*

*I sistemi informativi ed i programmi informatici sono stati configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante,*

*rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità.*

*I dati personali oggetto di trattamento sono custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.*

*Sono stati individuati il Titolare, gli incaricati del trattamento ed i Responsabili esterni ai quali sono stati date apposite istruzioni operative circa le modalità di corretto trattamento.*

*L'interessato è stato debitamente informato per iscritto circa le finalità e le modalità del trattamento cui sono destinati i dati; la natura obbligatoria o facoltativa del conferimento degli stessi; le conseguenze di un eventuale rifiuto di rispondere; i soggetti ai quali i dati personali possono essere comunicati; gli estremi identificativi del titolare, i diritti di cui all'articolo 7 del D.Lgs. 196/03 - "diritto di accesso ai dati personali e altri diritti" -, rivisto per effetto del RE679, che vengono di seguito riportati:*

*1. L'interessato ha diritto di ottenere la conferma dell'esistenza o meno di dati personali che lo riguardano, anche se non ancora registrati, e la loro comunicazione in forma intelligibile.*

*2. L'interessato ha diritto di ottenere l'indicazione:*

*a) dell'origine dei dati personali;*

*b) delle finalità e modalità del trattamento;*

*c) della logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici;*

*d) degli estremi identificativi del titolare, dei responsabili e del rappresentante designato ai sensi dell'articolo 5, comma 2;*

*e) dei soggetti o delle categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di rappresentante designato nel territorio dello Stato, di responsabili o incaricati.*

*3. L'interessato ha diritto di ottenere:*

*a) l'aggiornamento, la rettificazione ovvero, quando vi ha interesse, l'integrazione dei dati;*

*b) la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati;*

c) *l'attestazione che le operazioni di cui alle lettere a) e b) sono state portate a conoscenza, anche per quanto riguarda il loro contenuto, di coloro ai quali i dati sono stati comunicati o diffusi, eccettuato il caso in cui tale adempimento si rivela impossibile o comporta un impiego di mezzi manifestamente sproporzionato rispetto al diritto tutelato.*

4. *L'interessato ha diritto di opporsi, in tutto o in parte:*

a) *per motivi legittimi al trattamento dei dati personali che lo riguardano, ancorché pertinenti allo scopo della raccolta;*

b) *al trattamento di dati personali che lo riguardano a fini di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale.*

*Si è provveduto inoltre a raccogliere il consenso scritto dell'interessato al trattamento dei suoi dati personali e sensibili.*

*Sono state rispettate, per quanto applicabili, le indicazioni fornite dal Garante con la Prescrizione del 09 novembre 2005 e più precisamente:*

- *La prestazione medico/sanitaria e ogni operazione di trattamento dei dati personali avviene nel pieno rispetto della dignità dell'interessato.*
- *La tutela della dignità personale è garantita nei confronti di tutti i soggetti cui viene erogata una prestazione sanitaria, con particolare riguardo a fasce deboli quali i disabili, fisici e psichici, i minori, gli anziani e i soggetti che versano in condizioni di disagio o bisogno.*
- *Particolare riguardo è prestato nel rispettare la dignità di pazienti sottoposti a trattamenti medici invasivi o nei cui confronti è comunque doverosa una particolare attenzione anche per effetto di specifici obblighi di legge o di regolamento o della normativa comunitaria.*
- *Sono state adottate idonee cautele in relazione allo svolgimento di colloqui, specie con il personale sanitario per evitare che in tali occasioni le informazioni sulla salute dell'interessato possano essere conosciute da terzi. Le medesime cautele sono adottate nei casi di raccolta della documentazione di anamnesi, qualora avvenga in situazioni di promiscuità derivanti dai locali o dalle modalità utilizzate.*
- *La struttura sanitaria ha predisposto apposite distanze di cortesia, segnalate all'utenza, in tutti i casi in cui si effettua il trattamento di dati sanitari, nel rispetto dei canoni di confidenzialità e della riservatezza dell'interessato.*

- *All'interno dei locali della struttura sanitaria, sono state adottate soluzioni che prevedono un ordine di precedenza e di chiamata degli interessati che prescindono dalla loro individuazione nominativa.*
- *Il titolare del trattamento ha designato il responsabile al trattamento e ha nominato coloro che possono accedere ai dati personali trattati nell'erogazione delle prestazioni e dei servizi sanitari, nonché quelle amministrative correlate e ha provveduto a sottoporre ad idonea azione informativa e formativa i soggetti che non sono tenuti per legge al segreto professionale sottoponendoli a regole di condotta che garantiscano uguale grado di riservatezza.*
- *La documentazione sanitaria può essere ritirata anche da persona diversa dal diretto interessato, purché sulla base di una delega scritta e mediante la consegna della stessa in busta chiusa. Il processo prevede la identificazione attraverso documenti in corso di validità della persona delegata al ritiro.*

## **2. Definizioni ex art. 4 del D.lgs 196/03**

1. Ai fini del presente codice si intende per:

a) "trattamento", qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati; ai fini del trattamento la raccolta del consenso deve essere sempre condotta in modo esplicito con esclusione del consenso tacito. Tale consenso può essere revocato in qualunque momento dalla persona che lo ha autorizzato.

Per effetto della RE679 è stato introdotto un documento specifico denominato Registro dei Trattamenti, che include i diversi trattamenti dati eseguiti dalla nostra Associazione.

b) "dato personale", qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale;

c) "dati identificativi", i dati personali che permettono l'identificazione diretta dell'interessato;

d) "dati sensibili", i dati personali idonei 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;

- e) "dati giudiziari", i dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del d.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60e 61 del codice di procedura penale;
- f) "titolare", la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza; deve garantire il massimo supporto al DPO.
- g) "responsabile trattamento", la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali;
- g1) "Responsabile della protezione dei dati" denominato DPO, la persona fisica che mantiene informato e assicura il Titolare e il Responsabile della corretta implementazione dei processi come richiesto dal RE 679 del 2016, incluso attribuzione responsabilità, sensibilizzazione e formazione del personale, audit; e' tenuto alla estrema riservatezza e non puo' divulgare informazioni relative a dati Privacy in nessuna occasione.
- h) "incaricati", le persone fisiche autorizzate con documento scritto a compiere operazioni di trattamento dati dal titolare;
- i) "interessato", la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali;
- l) "comunicazione", il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
- m) "diffusione", il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
- n) "dato anonimo", il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile;
- o) "blocco", la conservazione di dati personali con sospensione temporanea di ogni altra operazione del trattamento;
- p) "banca di dati", qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti;
- q) "Garante", l'autorità di cui all'articolo 153, istituita dalla legge 31 dicembre 1996, n. 675.

2. Ai fini del presente codice si intende, altresì, per:

- a) "misure minime", il complesso delle misure tecniche, informatiche, organizzative,

*logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti nell'articolo 31;*

*b) "strumenti elettronici", gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento;*

*c) "autenticazione informatica", l'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità;*

*d) "credenziali di autenticazione", i dati ed i dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l' autenticazione informatica;*

*e) "parola chiave", componente di una credenziale di autenticazione associata ad una persona ed a questa nota, costituita da una sequenza di caratteri o altri dati in forma elettronica;*

*f) "profilo di autorizzazione", l'insieme delle informazioni, univocamente associate ad una persona, che consente di individuare a quali dati essa può accedere, nonché i trattamenti ad essa consentiti;*

*g) "sistema di autorizzazione", l'insieme degli strumenti e delle procedure che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione del richiedente.*



### **3. Elenco dei trattamenti di dati personali**

#### **Contenuti**

*In questa sezione è inserito l'elenco dei trattamenti svolti dal titolare, direttamente o attraverso organizzazioni esterne, con l'indicazione della natura dei dati trattati e dell'ufficio, interno od esterno che operativamente effettua il trattamento. Al proposito si precisa che le operazioni di trattamento avvengono presso la sede della società e, per gli adempimenti di competenza, presso gli studi dei consulenti esterni.*

*I dati oggetto del trattamento riguardano i dati personali e sensibili dei dipendenti e collaboratori (necessari per l'adempimento di specifici obblighi o compiti previsti dalla normativa comunitaria, da leggi, regolamenti e contratti collettivi nazionali di lavoro in particolare ai fini del rispetto della normativa in materia di previdenza ed assistenza sociale e di igiene e sicurezza sul lavoro), i dati personali e sensibili relativi a clienti ed i dati personali dei fornitori, raccolti per adempiere gli obblighi contrattuali, contabili ed amministrativi propri del rapporto commerciale in essere.*

*Tutti i dati sono raccolti solo se strettamente necessari per il rispetto di norme o di impegni contrattuali e sono detenuti per un periodo non superiore a quello indispensabile per l'adempimento di leggi e/o obblighi e/o impegni assunti.*

*Il trattamento dei dati è effettuato sia con l'ausilio di strumenti elettronici che manualmente presso la sede della Società da parte degli incaricati del trattamento. Gli archivi destinati ad ospitare supporti informatici o materiale cartaceo sono debitamente identificati e chiusi a chiave.*

*Per l'elenco completo dei vari trattamenti eseguiti, far riferimento al documento denominato **Registro dei Trattamenti**.*

*Per il trattamento dei dati con l'ausilio di strumenti elettronici sono state adottate le seguenti modalità tecniche di cui al Disciplinare tecnico in materia di misure minime di sicurezza (artt. da 33 a 36 del codice):*

#### **Sistema di autenticazione informatica**

*1. Il trattamento di dati personali con strumenti elettronici è consentito solo agli incaricati dotati di credenziali di autenticazione che consentano il superamento di una procedura di autenticazione relativa a uno specifico trattamento.*

*2. Le credenziali di autenticazione consistono in un codice per l'identificazione dell'incaricato associato a una parola chiave riservata conosciuta solamente dal medesimo.*

*3. Ad ogni incaricato è stata assegnata una credenziale per l'autenticazione.*

4. *Con le istruzioni impartite agli incaricati è prescritto di adottare le necessarie cautele per assicurare la segretezza della componente riservata della credenziale e la diligente custodia dei dispositivi in possesso ed uso esclusivo dell'incaricato.*
5. *La parola chiave, quando è prevista dal sistema di autenticazione, è composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito; essa non contiene riferimenti agevolmente riconducibili all'incaricato ed è modificata da quest'ultimo al primo utilizzo e, successivamente, almeno ogni tre mesi. Il Sistema forza il rinnovo ogni 6 mesi.*
6. *Il codice per l'identificazione non può essere assegnato ad altri incaricati, neppure in tempi diversi.*
7. *Le credenziali di autenticazione non utilizzate da almeno sei mesi sono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica.*
8. *Le credenziali sono disattivate anche in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali.*
9. *Sono state impartite istruzioni agli incaricati per non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento.*
10. *Essendo l'accesso ai dati consentito esclusivamente mediante uso della componente riservata della credenziale per l'autenticazione, sono state impartite disposizioni scritte volte a individuare le modalità con le quali il titolare può assicurare la disponibilità di dati o strumenti elettronici in caso di prolungata assenza o impedimento dell'incaricato che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema.*

### **Sistema di autorizzazione**

1. *Sono stati individuati profili di autorizzazione per ciascun incaricato, individuati e configurati anteriormente all'inizio del trattamento. Periodicamente, e comunque almeno annualmente, è verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione.*
2. *E' stata redatta la lista degli incaricati del trattamento e dei relativi profili di autorizzazione.*
3. *I dati personali sono protetti contro il rischio di intrusione e dell'azione di programmi di cui all'art. 615-quinquies del codice penale, mediante l'attivazione di idonei strumenti elettronici (programmi antivirus) aggiornati costantemente (collegamento giornaliero con i siti di riferimento) e verificati settimanalmente.*
4. *Gli aggiornamenti periodici dei programmi per elaboratore (service pack) volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti sono effettuati non appena resi disponibile dalle software house e comunque verificato trimestralmente.*

5. Sono impartite istruzioni organizzative e tecniche che prevedono il salvataggio dei dati con frequenza almeno settimanale.
6. Annualmente il titolare del trattamento redige o aggiorna il documento programmatico sulla sicurezza.

#### **Ulteriori misure adottate per il trattamento di dati sensibili o giudiziari**

1. I dati sensibili o giudiziari sono protetti contro l'accesso abusivo, di cui all'art. 615-ter del codice penale, mediante l'utilizzo di idonei programmi antivirus.
2. Sono state impartite istruzioni organizzative e tecniche per la custodia e l'uso dei supporti rimovibili su cui sono memorizzati i dati al fine di evitare accessi non autorizzati e trattamenti non consentiti.
3. I supporti rimovibili contenenti dati sensibili o giudiziari se non riutilizzati sono distrutti o resi inutilizzabili.
4. Sono adottate idonee misure per garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati e non superiori a sette giorni.
5. Il trattamento dei dati idonei a rivelare lo stato di salute è effettuato in modo tale da consentire il trattamento disgiunto dei dati sensibili dagli altri dati personali che permettono di identificare direttamente gli interessati.

#### **Misure di tutela e garanzia**

1. Il titolare richiede all'installatore/manutentore del sistema informativo una descrizione scritta dell'intervento effettuato che ne attesti la conformità alle disposizioni del presente disciplinare tecnico.
2. Il titolare riferisce, nella relazione accompagnatoria del bilancio d'esercizio dell'avvenuta redazione o aggiornamento del documento programmatico sulla sicurezza.
3. Viene richiesta al responsabile del sistema informatico, annualmente, la relazione di sicurezza dei sistemi informatici con le misure adottate e un piano di miglioramento. Tale documento sarà utilizzato dal DPO per proporre i miglioramenti necessari al Responsabile dei trattamenti.

#### **Trattamenti senza l'ausilio di strumenti elettronici**

1. Agli incaricati sono state impartite istruzioni scritte finalizzate al controllo ed alla custodia, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali. E' stata redatta la lista degli incaricati.

2. *Gli atti e i documenti contenenti dati personali sensibili affidati agli incaricati del trattamento per lo svolgimento dei relativi compiti, sono controllati e custoditi in aree controllate il cui accesso richiede specifiche autorizzazioni.*

3. *L'accesso agli archivi contenenti dati sensibili è possibile solo alle persone autorizzate. Le persone ammesse, a qualunque titolo, dopo l'orario di chiusura, sono identificate, registrate e preventivamente autorizzate.*

### **Informazioni essenziali dei dati riportati nelle tabelle**

*Per ciascun trattamento sono riportate, a titolo esemplificativo, le seguenti informazioni:*

Identificativo del trattamento: *codice che consente l'identificazione univoca di ciascun trattamento.*

Descrizione sintetica: *descrive il trattamento in modo da consentire la comprensione immediata della tabella.*

*Autorizzazioni sanitarie all'effettuazione di terapie ed al trasporto di infermi*

Natura dei dati trattati: *indica se, tra i dati oggetto del trattamento, sono presenti dati sensibili o giudiziari, oltre ad altri dati personali.*

*Sono presenti principalmente dati di natura sanitaria.*

Struttura di riferimento: *indica la struttura aziendale/ufficio all'interno della quale viene realizzato il trattamento.*

*Direzione servizi, segreteria ambulatori e segreteria sociale*

Altre funzioni che concorrono al trattamento: *indica l'esistenza di organizzazioni esterne al Titolare che concorrono al trattamento dei dati in collaborazione con l'attività delle diverse strutture interne.*

*L'indicazione specifica degli addetti e delle Società di consulenza è indicata nella lista degli incaricati di cui all'allegato A.*

Banca dati: *indica l'identificativo della banca dati in cui sono contenuti i dati che sono trattati.*

Ubicazione fisica dei supporti di memorizzazione: *contiene l'indicazione del luogo in cui risiedono fisicamente i dati: dove si trovano l'elaboratore sui cui dischi sono memorizzati, i supporti magnetici utilizzati per le copie di sicurezza nonché gli archivi cartacei.*

Server di rete	Direzione servizi	Dati sensibili Servizi Urgenza e Volontari
Work Station ambulatori	Ambulatorio	Dati sensibili pazienti Ambulatorio
Work Station segreteria	Segreteria	Dati sensibili gestionali e del personale

Tipologia di dispositivi di accesso: *descrive gli strumenti utilizzati dagli incaricati per effettuare il trattamento.*

*Accesso al software tramite password.*

*Tipologia di interconnessione: descrive la rete informatica che collega i dispositivi d'accesso utilizzati dagli incaricati ai dati.*

*Rete interconnessa con doppio server di gestione, con software specifico ad accessi selettivi tramite password.*

**Tabella 1.1 – Elenco dei trattamenti: informazioni di base**

Identificativo del Trattamento	Descrizione sintetica	Natura dei dati trattati		Struttura interna di appartenenza	Altre strutture esterne che concorrono al trattamento	Descrizione e degli strumenti utilizzati
		S	G			
T01	Accettazione pazienti ed emissione fattura	SI	SI	Reparto segreteria e amministrazione	Nessuna	Supporto cartaceo/PC
T02	Monitoraggio dei dati/rendicontazioni e esterna pro ASL	SI	SI	Reparto segreteria e amministrazione	Nessuna	Supporto cartaceo/PC
T03	Amministrazione del personale	SI	SI	Reparto segreteria e amministrazione	Nessuna	Supporto cartaceo/PC
T04	Gestione paghe e contributi	SI	SI	Reparto segreteria e amministrazione	Studio di consulenza	Supporto cartaceo/PC
T05	Gestione Fornitori	NO	SI	Reparto segreteria e amministrazione	Nessuna	Supporto cartaceo/PC
T06	Amministrazione e contabilità	NO	SI	Reparto segreteria e amministrazione	Studio di consulenza	Supporto cartaceo/PC
T07	Salvataggi e ripristino dei dati	SI	SI		Società incaricata	PC
T08	Manutenzione strumenti informatici	SI	SI		Società incaricata	PC
T09	Esecuzione attività diagnostico/riabilit.	SI	SI	Reparto Sanitario	Nessuna	Supporto cartaceo/PC

**Tabella 1.2 – Elenco dei trattamenti: descrizione degli strumenti utilizzati**

Identificativo del trattamento	Eventual e banca dati	Ubicazione fisica dei supporti di memorizzazione	Tipologia dispositivi di accesso	Tipologia interconnessione
T01	Db clienti	Sede amministrativa	PC	nessuna
T02	Db clienti	Sede amministrativa	PC	nessuna
T03	Db personale	Sede amministrativa	PC	nessuna
T04	Db personale	Sede amministrativa e Studio Consulenza 1)	PC	nessuna
T05	Db fornitori	Sede amministrativa	PC	nessuna

T06	Db contabilità	Sede amministrativa e Studio Consulenza 2)	PC	nessuna
T07	Db backup	Sede amministrativa	PC	nessuna
T08	Tutti i Db	Sede amministrativa	PC	nessuna
T09	Db clienti	Sede amministrativa	PC	nessuna

#### **4. Distribuzione dei compiti e delle responsabilità**

##### **Contenuti**

In questa sezione è tracciata la mappa che associa ad ogni ufficio i trattamenti da questo effettuati, descrivendo sinteticamente l'organizzazione della struttura e le relative responsabilità. Sono stati individuati, con apposito atto di nomina, Il Responsabile della sicurezza dei dati personali, il Responsabile del trattamento dati personali gli incaricati del trattamento, i responsabili esterni e l'amministratore di sistema.

##### **Informazioni essenziali**

- Struttura di riferimento: contiene lo stesso identificativo utilizzato nella sezione precedente.

- Responsabile: indica il nome del responsabile della struttura.

- Trattamenti operati dalla struttura: contiene l'elenco dei trattamenti per i quali la funzione aziendale ha la responsabilità primaria.

- Compiti della struttura: contiene una descrizione sintetica dei compiti assegnati alla funzione.

**Tabella 2.1 Strutture preposte ai trattamenti**

<b>Struttura</b>	<b>Responsabile/i</b>	<b>Trattamenti operati dalla struttura</b>	<b>Compiti della struttura</b>
Reparto Medico Segreteria e amministrazione	Si rimanda all'allegato A organigramma della privacy – elenco degli incaricati	Rapporti con i clienti, medici e strutture invianti. Operazioni di segreteria ed accettazione amministrativa ed operativa del clienti. Salvataggio e ripristino dati	Acquisizione e caricamento dei dati, consultazione, comunicazione a terzi, all'interessato o suo delegato
Reparto Segreteria e amministrazione	Si rimanda all'allegato A organigramma della privacy – elenco degli incaricati	Tenuta della contabilità, Monitoraggio dati e rendicontazione esterna, Gestione operativa del personale, Rapporti con i fornitori	Acquisizione e caricamento dei dati, consultazione, comunicazione a terzi, manut. ordinaria dei SW, gestione dei Db

Reparto Sanitario	Si rimanda all'allegato A organigramma della privacy - elenco degli incaricati	Effettuazione delle prestazioni sanitarie, Refertazione attività diagnostica, Rapporti con i clienti, medici e strutture invianti	Acquisizione e caricamento dei dati, consultazione, comunicazione a terzi.
Studio di consulenza	Si rimanda all'allegato A organigramma della privacy	Elaborazione paghe e contributi del personale	Acquisizione e caricamento dei dati, consultazione, comunicazione a terzi
Studio di consulenza	Si rimanda all'allegato A organigramma della privacy	Elaborazione reportistica contabile, fiscale, amministrativa e societaria	Acquisizione e caricamento dei dati, consultazione, comunicazione a terzi
Società incaricata esterna	Si rimanda all'allegato A organigramma della privacy	Operazioni di manutenzione ed aggiornamento dei sistemi informatici	Analisi, correzione, aggiornamento e manutenzione dei Db, SW e HW
Società incaricata esterna	Si rimanda all'allegato A organigramma della privacy	Operazioni di manutenzione ed aggiornamento dei sistemi informatici	Analisi, correzione, aggiornamento e manutenzione SW dei Db

## **5. Analisi dei rischi sui dati**

### **Contenuti**

*In questa sezione sono individuati i principali eventi potenzialmente dannosi per la sicurezza dei dati, le possibili conseguenze e le contromisure adottate.*

*Il trattamento dei dati avviene principalmente nella sede della Società e presso gli Studi dei consulenti per gli adempimenti di loro competenza. Le zone dei locali nei quali avviene il trattamento dei dati non sono aperte al pubblico essendo riservati unicamente agli incaricati del trattamento.*

*Durante l'orario di apertura, i documenti di natura sensibile sono conservati in archivi costantemente presidiati da personale incaricato e non accessibili al pubblico.*

*Fuori dagli orari di lavoro, tutte le porte di accesso sono chiuse a chiave.*

*Il personale è stato idoneamente formato sulle precauzioni da seguire per garantire la sicurezza del trattamento dei dati sensibili.*

*Le attrezzature elettroniche utilizzate per il trattamento sono regolarmente mantenute dalla Ditta incaricata e periodicamente aggiornate sia a livello di software (service pack) sia a livello di programma antivirus.*

*Il personale incaricato del trattamento è stato debitamente formato in ordine alle regole comportamentali ed ai protocolli operativi da seguire per garantire la riservatezza dei dati. Sono state assegnate le password e le user ID per gli utilizzi del sistema informatico ed è stato nominato il responsabile della raccolta della PW e User ID.*



### **Informazioni essenziali**

Elenco degli eventi: contiene l'elenco degli eventi che possono generare dei danni e quindi che comportano dei rischi per la sicurezza dei dati personali. L'elenco identifica quindi l'universo degli eventi che si ritengono rilevanti per l'analisi dei 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. In questo modo consente di formulare un indicatore qualitativo di gravità omogeneo per i diversi eventi che deve essere esplicitato.

Rif. misure d'azione: contiene il riferimento alla contromisura adottata, descritta con la tabella 4.1.

**Tabella 3.1 - Analisi dei rischi**

Rischio/Evento	Impatto sulla sicurezza dei dati		Possibilità di accadimento
	Descrizione	Gravità stimata	Riferim. misure d'azione
<b>Comportamenti degli operatori - COD.A</b>	1. Uso di credenziali di autenticazione altrui	Trattamenti operati in modo abusivo: perdita della rintracciabilità del trattamento	Bassa Bassa Ma01-1
	2. Carenza di consapevolezza, disattenzione o incuria	Comunicazione involontaria dei dati a non aventi diritto Abbandono momentaneo dei PC con programmi attivi, Inosservanza dei protocolli comportamentali	Media Bassa Ma01-2
	3. Comportamenti sleali o fraudolenti	Comunicazione e/o diffusione volontaria a terzi di dati personali e/o aziendali.	Alta Bassa Ma01-3
	4. Errore materiale	Consegna, comunicazione di dati personali e/o sensibili e della relativa documentazione a persona errata. Errore nella gestione informatica e cartacea del trattamento del dato personale	Alta Bassa Ma01-4
<b>Termini agli strumenti - COD.B</b>	1. Azione di virus informatici o di codici malefici	Perdita di affidabilità e sicurezza dei sistemi informatici: vulnerabilità degli stessi e dei dati in essi contenuti Perdita di dati	Alta Bassa Ma02-1

	2. Spamming o altre tecniche di sabotaggio	Perdita di affidabilità e sicurezza dei sistemi informatici	Media	Bassa ----- Ma02-2
	3. Malfunzionamento, indisponibilità o degrado degli strumenti	Perdita di affidabilità e sicurezza dei sistemi informatici Perdita della base dati Indisponibilità dei dati Impossibilità di operare	Media	Bassa ----- Ma02-3
	4. Accessi esterni non autorizzati	Perdita di sicurezza dei sistemi informatici: vulnerabilità degli stessi e dei dati in essi contenuti	Alta	Bassa ----- Ma02-4
	5 Intercettazione di informazioni in rete	Perdita di affidabilità e sicurezza dei sistemi informatici: vulnerabilità degli stessi e dei dati in essi contenuti	Alta	Bassa ----- Ma02-5
<b>Rischio/Evento</b>		<b>Impatto sulla sicurezza dei dati</b>		<b>Possibilità di accadimento</b> ----- <b>Riferim. misure d'azione</b>
		<b>Descrizione</b>	<b>Gravità stimata</b>	
<b>relativi al contesto - COD.C</b>	1. Accessi non autorizzati a locali/reparti ad accesso ristretto	Conoscenza e/o sottrazione di dati da parte di terzi	Bassa	Bassa ----- Ma03-1
	2. Asportazione e furto di strumenti contenenti dati	Impossibilità di operare Perdita di riservatezza	Bassa	Bassa ----- Ma03-2
	3. Eventi distruttivi, naturali o artificiali, dolosi, accidentali o dovuti ad incuria	Incendio, allagamenti, eventi naturali	Media	Bassa -----
	4. Guasto ai sistemi complementari (impianto elettrico, climatizzazione, ...)	Perdita dei dati in lavorazione	Bassa	Bassa ----- Ma03-4
	5. Errori umani nella gestione della sicurezza fisica	Conoscenza e/o sottrazione di dati da parte di terzi Distruzione di dati per eventi colposi	Bassa	Bassa ----- Ma01-1

## 6. Misure in essere e da adottare

### Contenuti

In questa sezione sono riportate, in forma sintetica, le misure in essere e da adottare a contrasto dei rischi individuati dall'analisi effettuata.

**Informazioni essenziali**

Misure: la descrizione sintetica della misura di sicurezza adottata.

Rischio contrastato: indica il riferimento all'elemento dell'analisi dei rischi che ha motivato l'adozione della misura in oggetto.

Data base/trattamento interessato: riporta l'identificativo dei data base o dell'archivio informatizzato e dei trattamenti interessati per ciascuna delle misure adottate.

Data di effettività: indica la data a partire dalla quale la misura è operativa o se già operativa una dicitura standard ('in essere').

Periodicità e responsabilità dei controlli: contiene l'indicazione della periodicità con cui sono verificate la funzionalità e l'efficienza della misura adottata e della struttura operativa che ne ha la responsabilità.

**Tab. 4.1 – Confidenziale - Disponibile presso la sede****7. Criteri e modalità di ripristino dei dati****Contenuti**

In questa sezione sono descritti i criteri e le procedure adottate per il salvataggio dei dati e per il loro ripristino in caso di danneggiamento o di inaffidabilità della base dati.

**Informazioni essenziali**

Data base: contiene l'identificativo del data base o dell'archivio interessato.

Dati sensibili o giudiziari contenuti: contiene l'elenco dei dati sensibili o giudiziari contenuti nel database o archivio.

Criteri individuati per il salvataggio (procedure operative in essere): contiene una descrizione della tipologia di salvataggio e della frequenza con cui viene effettuato.

Ubicazione di conservazione delle copie: contiene l'indicazione del luogo fisico in cui sono custodite le copie dei dati salvate.

Struttura operativa incaricata del salvataggio: contiene il riferimento alla struttura operativa incaricata di effettuare il salvataggio e di controllarne l'esito.

**Tab. 5.1 Confidenziale – Disponibile in sede.**

*Data base/archivio: contiene l'identificativo del data base o dell'archivio interessato.*

*Scheda operativa: contiene il riferimento alla scheda operativa che descrive la procedura di ripristino.*

*Pianificazione delle prove di ripristino: contiene l'indicazione delle date in cui si prevede di effettuare dei test di efficacia delle procedure di salvataggio/ripristino dei dati adottate.*

*E' stato individuato l'incaricato dell'effettuazione delle copie di back up e delle eventuali operazioni di ripristino che effettua le operazioni conformemente a quanto descritto nei manuali di istruzione del dispositivo di back up e nell'allegato L ai quali si rimanda per maggior dettaglio.*

*Il tempo di ripristino dei dati è definito in n. 3 giorni dal verificarsi dell'evento dannoso.*

*I supporti informatici utilizzati per l'effettuazione delle copie sono conservati in apposito archivio identificato chiuso a chiave. Prima della loro eventuale ri-utilizzazione o distruzione si provvede a cancellarne il contenuto. Le copie sono effettuate settimanalmente ed i relativi supporti vengono identificati con la data e catalogati in ordine cronologico. Al termine di ogni operazione di copia viene verificato il buon esito dell'operazione.*

**Tab. 5.2 Confidenziale - disponibile in sede**

## **8. Pianificazione degli interventi formativi previsti**

### **Contenuti**

*Per gli incaricati del trattamento è predisposto un programma di formazione al momento dell'ingresso in servizio, che partendo dalla consegna e dalla spiegazione dei contenuti del "Codice di comportamento degli incaricati" viene successivamente erogato in caso di cambiamenti di mansioni o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali.*

*I contenuti della formazione sono:*

- *I profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività ed in particolare le misure minime di sicurezza;*
- *Le indicazioni/conclusioni emerse dell'analisi del rischio effettuata annualmente in occasione della stesura del D.P.S.;*
- *Le contromisure organizzative e tecnologiche già adottate e/o in previsione di esserlo;*

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 destinati e/o le tipologie di incaricati interessati.

Numero di incaricati interessati: contiene il numero di addetti interessati dal corso.

Numero di incaricati già formati/da formare nell'anno: contiene l'indicazione del numero di addetti già formati negli anni precedenti e quelli di cui si prevede la formazione nell'anno in corso.

**Tab. 6.1**

<b>Corso di formazione</b>	<b>Descrizione sintetica</b>	<b>Classi di incarico interessate</b>	<b>Numero di incaricati interessati</b>
1. Applicazione del nuovo testo unico sulla privacy	Formazione di base sulla legge e sulle responsabilità degli incaricati	Tutte	Tutti
2. Verifica ed aggiornamento dell'applicazione del testo unico sulla privacy	Verifica ed aggiornamento delle procedure adottate per il corretto trattamento dei dati	Tutte	Tutti

## **9. Trattamenti affidati all'esterno**

### **Contenuti**

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

*Il trattamento affidato a strutture esterne è limitato ai dati riferiti:*

- alla retribuzione del personale (ed obblighi previdenziali, assistenziali e contributivi connessi);
- agli adempimenti in campo societario, amministrativo e fiscale;
- alla manutenzione del sistema informatico;

### **Informazioni essenziali**

Attività esternalizzata: contiene l'identificativo dell'attività che è stata oggetto di delega a terzi.

Descrizione sintetica: contiene una descrizione sintetica dell'attività.

Dati personali, sensibili o giudiziari interessati: contiene l'elenco dei dati personali, sensibili o giudiziari oggetto di trattamento per la realizzazione dell'attività delegata.

Soggetto esterno: riporta l'identificativo della società o del consulente a cui è stato affidato l'incarico.

Descrizione impegni assunti: perché sia garantito un adeguato trattamento dei dati è necessario che la società che viene delegata al trattamento si assuma alcuni impegni su base contrattuale. Essi sono riconducibili ai seguenti:

1. Il titolare accetta di adottare le istruzioni specifiche eventualmente ricevute per il trattamento dei dati personali o di integrarle nelle procedure già in essere.
2. Il titolare si impegna a relazionare annualmente sulle misure di sicurezza adottate e di allertare immediatamente il proprio committente in caso di situazioni anomale o di emergenze
3. Il titolare riconosce il diritto del committente a verificare periodicamente l'applicazione delle norme di sicurezza adottate.

In questa casella sono riportati gli impegni contrattualmente assunti nel caso specifico.

Date delle verifiche: contiene l'indicazione del numero e delle date delle verifiche previste.

**Tab. 7.1**

<b>Attività esternalizzata</b>	<b>Descrizione sintetica</b>	<b>Dati sensibili o giudiziari</b>	<b>Soggetto esterno</b>	<b>Descrizione impegni assunti</b>	<b>Date delle verifiche</b>
Elaborazione paghe e contributi del personale	Elaborazione buste paga, presenze, assenze etc.	Dati personali e sensibili dei dipendenti	Studio di consulenza	Sottoscrizione e impegni	In caso di anomalie

Elaborazione reportistica fiscale, amministrativa e societaria	Predisposizione del bilancio e dei documenti fiscali previsti dalla legge	Dati personali e sensibili dei dipendenti; dati personali dei soci, dei fornitori e dei clienti	Studio di consulenza	Sottoscrizioni e impegni	In caso di anomalie
Manutenzione sistema informatico	Operazioni di manutenzione, aggiornamento dei sistemi informatici	Dati personali e sensibili contenuti nei data base aziendali	Società incaricata esterna	Sottoscrizioni e impegni	In caso di anomalie e comunque semestralmente
Manutenzione sistema informatico	Operazioni di manutenzione, aggiornamento software	Dati personali e sensibili contenuti nei data base aziendali	Ditta incaricata esterna	Sottoscrizioni e impegni	In caso di anomalie e annualmente

## **10. Cifratura dei dati o separazione dei dati identificativi**

### **Contenuti**

*In questa sezione sono rappresentate le modalità di protezione adottate per i dati sensibili.*

*Al fine di garantire sempre la massima riservatezza dei dati sensibili, sono state comunque adottate particolari modalità operative che consentono di separare i dati identificativi del cliente con i relativi dati sensibili, utilizzando supporti cartacei diversi.*

*Il Cliente riceverà:*

- *per gli aspetti amministrativi della prestazione il documento fiscale che richiamerà genericamente il servizio sanitario fruito ed i dati identificativi del cliente e risponde ai vigenti obblighi amministrativo-fiscali;*
- *per gli aspetti sanitari una busta chiusa contenente la documentazione sanitaria od il referto (dati sensibili).*

*Si realizza così una duplicità dei documenti (ognuno dei quali contenente una determinata categoria di dati), gestibili separatamente, prodotti da diversi incaricati e soggetti alle regole di gestione che garantiscono la massima riservatezza dei dati contenuti.*

**TRATTAMENTI CON STRUMENTI ELETTRONICI**

<b><i>Lista degli adempimenti</i></b>	<b><i>Si/No</i></b>	<b><i>Riferimento documentale</i></b>
1. Sistema di autenticazione informatica.		
a) Tutte le applicazioni hanno una procedura di autenticazione	SI	Istruzioni per l'accesso agli strumenti informatici Istruzioni sulla custodia e gestione della password
b) Procedura per l'affidamento delle credenziali agli incaricati		Istruzioni per l'accesso agli strumenti informatici Istruzioni sulla custodia e gestione della password
i) Istruzioni sulle modalità di conservazione della parola chiave	SI	Istruzioni per l'accesso agli strumenti informatici Istruzioni sulla custodia e gestione della password
ii) Istruzioni sulla composizione della parola chiave	SI	Istruzioni per l'accesso agli strumenti informatici Istruzioni sulla custodia e gestione della password
iii) Istruzioni sull'aggiornamento della parola chiave	SI	Istruzioni per l'accesso agli strumenti informatici Istruzioni sulla custodia e gestione della password
c) Procedure di controllo sulle credenziali:		
i) Unicità del codice per l'identificazione (non riassegnato)	SI	Istruzioni per l'accesso agli strumenti informatici Istruzioni sulla custodia e gestione della password
ii) Disattivazione delle credenziali non utilizzate da sei mesi	SI	Istruzioni per l'accesso agli strumenti informatici Istruzioni sulla custodia e gestione della password
iii) Disattivazione per perdita del diritto all'accesso	SI	Istruzioni per l'accesso agli strumenti informatici Istruzioni sulla custodia e gestione della password
d) PC incustoditi durante il trattamento		
i) Attivazione salvaschermo con parola chiave	SI	Istruzioni per l'accesso agli strumenti informatici Istruzioni sulla custodia e gestione della password
ii) Istruzione agli incaricati	SI	Istruzioni per l'accesso agli strumenti informatici Istruzioni sulla custodia e gestione della password



e) Dispositivi ad uso personale		
i) Disposizioni scritte per l'accesso agli strumenti in caso di impedimento dell'incaricato	SI	Istruzioni per l'accesso agli strumenti informatici Istruzioni sulla custodia e gestione della password
ii) Individuazione dell'incaricato del trattamento delle chiavi	SI	Organigramma della privacy - elenco degli incaricati
iii) Modalità di trattamento delle chiavi	SI	Istruzioni per l'accesso agli strumenti informatici Istruzioni sulla custodia e gestione della password
iv) Tempi per la comunicazione in caso di accesso	SI	Istruzioni per l'accesso agli strumenti informatici Istruzioni sulla custodia e gestione della password

<b>Lista degli adempimenti</b>	<b>Si/No</b>	<b>Note</b>
2. Sistema di autorizzazione		
a) Individuazione degli ambiti in cui è applicato	SI	Allegato A Organigramma della privacy - elenco degli incaricati
b) Definizione dei profili per classi omogenee	SI	Allegato A Organigramma della privacy - elenco degli incaricati
c) Procedura annuale per la verifica della sussistenza delle condizioni	SI	Istruzioni per l'accesso agli strumenti informatici Istruzioni sulla custodia e gestione della password
d) Lista degli incaricati per classi omogenee	SI	Allegato A Organigramma della privacy - elenco degli incaricati

<b>Lista degli adempimenti</b>	<b>Si/No</b>	<b>Note</b>
3. Altre misure di sicurezza		
a) Adozione antivirus		
i) Procedura di aggiornamento periodico	SI	Descrizione sistema informatico e procedure di back up e ripristino dati
ii) Individuazione dell'incaricato	SI	Allegato A Organigramma della privacy - elenco degli incaricati
iii) Controllo della periodicità	SI	settimanale
b) Aggiornamento dei programmi		
i) Procedura per	SI	Relazione sicurezza Sistemista e valutazione del DPO

l'aggiornamento degli strumenti		
ii)	Individuazione dell'incaricato	SI Allegato A Organigramma della privacy – elenco degli incaricati
iii)	Controllo della periodicità	SI Sistemista sistema informatico
c) Salvataggio dei dati		
i)	Individuazione dell'incaricato	SI Allegato A Organigramma della privacy – elenco degli incaricati
ii) Definizione delle procedure tecniche		
(1)	orari di esecuzione	SI Sistemista
(2)	attivazione delle procedure	SI Descrizione sistema informatico
(3)	verifica del buon esito	SI Descrizione sistema informatico
(4)	criteri di catalogazione delle copie	SI Descrizione sistema informatico
(5)	criteri di ri-utilizzo dei supporti	SI Sistemista informatico
iii) Definizione delle procedure organizzative		
1.	luogo di conservazione delle copie	SI Descrizione sistema informatico
2.	modalità di trasferimento	SI Descrizione sistema informatico

### TRATTAMENTI SENZA L'AUSILIO DI STRUMENTI ELETTRONICI

<b>Adempimenti relativi a tutte le categorie dati personali</b>		
<b><i>Lista degli adempimenti</i></b>	<b><i>Si/No</i></b>	<b><i>Note</i></b>
1. Istruzioni agli incaricati in caso di trattamento di dati personali	SI	Istruzioni sulla custodia e gestione della documentaz. Cartacea
Istruzioni agli incaricati per il controllo e la custodia	SI	istruzioni sulla custodia e gestione della documentaz. Cartacea
Lista degli incaricati per classi omogenee di incarico	SI	Allegato A Organigramma della privacy – elenco degli incaricati
Lista degli incaricati su base individuale	SI	Allegato A Organigramma della privacy – elenco degli incaricati

*Il presente documento sarà aggiornato in caso di variazioni/modifiche legislative, organizzative ed operative che possano interessare le misure adottate, atte a garantire la riservatezza dei dati e, comunque ogni anno.*

*Gli allegati sono disponibili su richiesta presso la sede PA Croce Bianca Savona.*

*Savona, 19 sett 2018*

*Il Titolare del Trattamento dati  
Presidente PA Croce Bianca Savona  
Giovanni Carlevarino*

