

Centro Phoenix Srl Centro di Psicologia, Neuropsicologia, Riabilitazione e Psicoterapia Via Bassanese n. 72/a ; 36060 Romano d'Ezzelino (VI) Tel/Fax : 0424382527; cell: 3478911893; Sito: https://www.centrophoenix.it; e-mail: segreteria@centrophoenix.it; P.I. 03595710249	Centro Phoenix STP Srl Centro di Psicologia, Neuropsicologia, Riabilitazione e Psicoterapia Via Annibale da Bassano n. 14, 35135 Padova Tel/Fax : 0424382527; cell: 3478911893; Sito: https://www.centrophoenix.it; e-mail: segreteria@centrophoenix.it; P.I. 05666420285
--	---

Romano d'Ezzelino, 19/03/2025

MANUALE DELLE PROCEDURE OPERATIVE GDPR (Regolamento UE 2016/679 e D.Lgs. 101/2018)

NOTA PRELIMINARE: Il presente manuale è stato redatto per il Centro Phoenix Srl e Centro Phoenix STP Srl. Tutte le funzioni e responsabilità sono attribuite al Titolare del Trattamento o a suoi delegati espressamente nominati.

INDICE

1. PROCEDURA GESTIONE RICHIESTE DI ACCESSO AI DATI (Art. 15 GDPR)
2. PROCEDURA RETTIFICA E INTEGRAZIONE DATI (Art. 16 GDPR)
3. PROCEDURA CANCELLAZIONE DATI - DIRITTO ALL'OBLIO (Art. 17 GDPR)
4. PROCEDURA LIMITAZIONE DEL TRATTAMENTO (Art. 18 GDPR)
5. PROCEDURA PORTABILITÀ DEI DATI (Art. 20 GDPR)
6. PROCEDURA OPPOSIZIONE AL TRATTAMENTO (Art. 21 GDPR)
7. PROCEDURA GESTIONE DATA BREACH (Art. 33-34 GDPR)

GLOSSARIO E RUOLI

TITOLARE DEL TRATTAMENTO: Legale rappresentante del Centro Phoenix Srl e Centro Phoenix STP Srl, responsabile ultimo delle decisioni in materia di protezione dei dati personali.

REFERENTE PRIVACY: Persona designata dal Titolare per gestire operativamente le richieste degli interessati e coordinare le attività di compliance (in assenza di DPO).

INTERESSATO: La persona fisica cui si riferiscono i dati personali (paziente, dipendente, collaboratore).

AUTORIZZATI AL TRATTAMENTO: Personale del Centro (psicologi, amministrativi, collaboratori) autorizzati formalmente a trattare dati personali.

TERMINI: - Termine ordinario di risposta: 30 giorni dalla ricezione della richiesta - Proroga possibile: ulteriori 60 giorni in caso di particolare complessità - Notifica data breach al Garante: entro 72 ore dalla scoperta - Comunicazione data breach agli interessati: senza ingiustificato ritardo

PROCEDURA 1: GESTIONE RICHIESTE DI ACCESSO AI DATI (Art. 15 GDPR - Diritto di accesso dell'interessato)

1.1 FINALITÀ E AMBITO DI APPLICAZIONE

Questa procedura disciplina la gestione delle richieste di accesso ai dati personali da parte degli interessati, garantendo il rispetto dell'art. 15 GDPR.

L'interessato ha diritto di ottenere: - Conferma che sia o meno in corso un trattamento dei suoi dati - Accesso ai dati personali - Informazioni sul trattamento (finalità, categorie, destinatari, periodo conservazione, diritti, fonte dei dati) - Copia dei dati personali oggetto di trattamento

1.2 RESPONSABILITÀ

- **REFERENTE PRIVACY:** Ricezione e coordinamento gestione richieste
- **TITOLARE DEL TRATTAMENTO:** Autorizzazione finale e gestione casi complessi
- **PERSONALE AUTORIZZATO:** Supporto nella ricerca e estrazione dati

1.3 MODALITÀ DI PRESENTAZIONE DELLA RICHIESTA

L'interessato può presentare richiesta di accesso mediante: a) Richiesta scritta consegnata a mano presso il Centro b) Richiesta inviata via email a: privacy@centrophoenix.it [adattare] c) Richiesta inviata via PEC a: [inserire PEC] d) Richiesta inviata via raccomandata A/R

REQUISITI DELLA RICHIESTA: - Identificazione dell'interessato (dati anagrafici completi) - Copia documento d'identità valido - Firma (anche digitale per richieste telematiche) - Specificazione del diritto che si intende esercitare

1.4 FLUSSO OPERATIVO

FASE 1: RICEZIONE E PROTOCOLLAZIONE (Giorno 0)

☐ **STEP 1.1 - Ricezione richiesta** - Il Referente Privacy riceve la richiesta - Verifica integrità e leggibilità della documentazione

☐ **STEP 1.2 - Protocolloazione** - Assegnare numero protocollo progressivo: ACC/[ANNO]/[NUMERO] - Registrare nel "Registro Richieste Interessati" (vedi Modulo 1-A): * Data e ora ricezione * Dati identificativi richiedente * Modalità di ricezione * Tipo di richiesta - Calcolare data di scadenza: 30 giorni dalla ricezione - Scadenza: ____/____/____

- STEP 1.3 - Invio ricevuta di ricezione - Inviare entro 24-48 ore ricevuta all'interessato (vedi Modulo 1-B) - Indicare numero protocollo e termine di risposta

FASE 2: VERIFICA IDENTITÀ E LEGITTIMAZIONE (Giorni 1-3)

- STEP 2.1 - Verifica identità richiedente - Controllare documento d'identità allegato - Se documento mancante o non valido: richiedere integrazione - Se richiesta per conto terzi: verificare delega/procura - Se richiedente è genitore/tutore di minore: verificare legittimazione
- STEP 2.2 - Verifica legittimazione - Confermare che il richiedente sia effettivamente interessato - Verificare esistenza di un rapporto con il Centro - In caso di dubbi: richiedere ulteriore documentazione
- STEP 2.3 - Valutazione ammissibilità - Verificare se la richiesta è manifestamente infondata o eccessiva - Verificare se vi sono richieste ripetitive in breve tempo - Se inammissibile: procedere con motivato diniego (vedi Modulo 1-F)

FASE 3: RICERCA E RACCOLTA DATI (Giorni 4-15)

- STEP 3.1 - Identificazione delle fonti Ricercare i dati personali dell'interessato in: - Cartelle cliniche (cartacee e digitali) - Database gestionale pazienti - Archivio contabile e amministrativo - Sistema di prenotazione - Email e corrispondenza - Archivi di backup - Sistemi di videosorveglianza (se applicabile) - Altri archivi o database
- STEP 3.2 - Estrazione dati - Estrarre tutti i dati personali riferiti all'interessato - Includere metadati quando rilevanti - Documentare fonte di ogni dato estratto - Attenzione: escludere dati riferiti a terzi (pazienti, familiari, altri)
- STEP 3.3 - Preparazione documentazione Predisporre documento contenente: a) INFORMAZIONI SUL TRATTAMENTO: - Finalità del trattamento - Categorie di dati trattati - Destinatari o categorie di destinatari - Periodo di conservazione (o criteri per determinarlo) - Diritti dell'interessato (rettifica, cancellazione, limitazione, opposizione, reclamo) - Fonte dei dati (se non raccolti presso l'interessato) - Esistenza di processi decisionali automatizzati (se applicabile) - Garanzie in caso di trasferimento extra-UE (se applicabile)

b) COPIA DEI DATI PERSONALI:

- Elenco completo dei dati in formato chiaro e comprensibile
- Per dati clinici: fornire copia della cartella clinica
- Per corrispondenza: fornire copia email/comunicazioni

FASE 4: VALUTAZIONE ECCEZIONI E LIMITAZIONI (Giorni 16-20)

- STEP 4.1 - Verifica presenza di dati di terzi - Identificare eventuali dati personali di terzi inclusi nei documenti - Se presenti: oscurare/anonimizzare i dati di terzi - Motivare eventuali omissioni nella risposta
- STEP 4.2 - Verifica segreto professionale - Valutare se esistono informazioni coperte da segreto professionale - Consultare il Titolare per valutazione caso per caso - Bilanciare diritto di accesso con altri diritti/libertà
- STEP 4.3 - Verifica oneri sproporzionati - Se la ricerca comporta oneri sproporzionati: valutare se richiedere precisazioni all'interessato su specifici dati - Documentare motivazioni

FASE 5: PREPARAZIONE RISPOSTA (Giorni 21-25)

- STEP 5.1 - Predisposizione lettera di riscontro - Utilizzare Modulo 1-C (Risposta positiva) o Modulo 1-F (Diniego) - Allegare tutta la documentazione raccolta - Indicare chiaramente le informazioni fornite - Specificare eventuali limitazioni e relative motivazioni
- STEP 5.2 - Verifica da parte del Titolare - Sottoporre la risposta al Titolare per approvazione - Apportare eventuali modifiche richieste - Ottenere autorizzazione formale all'invio
- STEP 5.3 - Predisposizione supporti - Prima copia: sempre gratuita - Se supporto cartaceo: predisporre copia stampata - Se supporto elettronico: predisporre file PDF protetto o altro formato - Se richiesto su supporto fisico (USB): predisporre dispositivo

FASE 6: INVIO RISPOSTA (Giorni 26-28)

- STEP 6.1 - Trasmissione risposta Inviare risposta con la stessa modalità della richiesta (salvo diversa indicazione dell'interessato): - Se richiesta cartacea: risposta raccomandata A/R - Se richiesta email: risposta via email - Se richiesta PEC: risposta via PEC - Possibilità di ritiro a mano previo appuntamento
- STEP 6.2 - Archiviazione - Aggiornare "Registro Richieste Interessati" - Archiviare copia della risposta inviata - Archiviare ricevuta di consegna/lettura - Conservare documentazione per almeno 5 anni

FASE 7: CHIUSURA E MONITORAGGIO

- STEP 7.1 - Registrazione chiusura pratica - Annotare data invio risposta - Verificare ricezione da parte dell'interessato - Chiudere la pratica nel registro
- STEP 7.2 - Eventuale follow-up - Se l'interessato richiede chiarimenti: fornirli tempestivamente - Se l'interessato non è soddisfatto: valutare ulteriori azioni - Informare l'interessato del diritto di reclamo al Garante

1.5 TEMPISTICHE E PROROGHE

TERMINE ORDINARIO: 30 giorni dalla ricezione della richiesta

PROROGA ECCEZIONALE: - Possibile per ulteriori 60 giorni se la richiesta è complessa - Comunicare la proroga all'interessato entro 30 giorni dalla richiesta - Indicare i motivi del ritardo

CASI DI PROROGA: - Volume elevato di dati da ricercare - Necessità di oscurare dati di terzi in numerosi documenti - Complessità tecnica nell'estrazione dei dati - Richieste multiple da parte dello stesso interessato

1.6 CASI PARTICOLARI

A) RICHIESTA MANIFESTAMENTE INFONDATA O ECCESSIVA

- Valutare attentamente la natura ripetitiva o pretestuosa
- Possibile rifiuto motivato o richiesta contributo spese ragionevole
- Obbligo di motivazione scritta del rifiuto
- Informare dell'interessato del diritto di reclamo al Garante

B) RICHIESTA DI ACCESSO ALLA CARTELLA CLINICA

- Applicare anche normativa sanitaria specifica
- Possibile presenza dello psicologo durante la consultazione

- Valutare se la conoscenza dei dati possa arrecare grave pregiudizio alla salute del paziente (raro in ambito psicologico, ma previsto dalla normativa)
- Eventuale coinvolgimento di altro professionista sanitario

C) RICHIESTA DA PARTE DI MINORI

- Se minore >14 anni: può presentare richiesta autonomamente
- Se minore <14 anni: deve presentarla il genitore/tutore
- Verificare sempre legittimazione

D) RICHIESTA DA PARTE DI EREDI

- Possibile solo se previsto dalla legge o per tutela diritti ereditari
- Verificare certificato di morte
- Verificare titolo ereditario
- Valutare caso per caso con particolare attenzione al segreto professionale

1.7 MODULISTICA

MODULO 1-A: REGISTRO RICHIESTE DI ACCESSO

[Da integrare nel Registro generale richieste interessati]

Protocollo	Data	Richiedente	Modalità	Scadenza	Evasa il	Esito	Note
ACC/25/001							

MODULO 1-B: RICEVUTA DI RICEZIONE RICHIESTA

CENTRO PHOENIX SRL E CENTRO PHOENIX STP SRL [Indirizzo] [Contatti]

Protocollo n. ACC/[ANNO]/[NUMERO] Data: ____/____/____

Spett.le [Nome Cognome richiedente] [Indirizzo]

Oggetto: Ricevuta ricezione richiesta di accesso ai dati personali - Art. 15 GDPR

Gentile [Sig./Sig.ra] [Cognome],

confermiamo di aver ricevuto in data ____/____/____ la Sua richiesta di accesso ai dati personali ai sensi dell'art. 15 del GDPR.

La richiesta è stata registrata con il numero di protocollo ACC/[ANNO]/[NUMERO].

La informiamo che provvederemo a riscontrare la Sua richiesta entro il termine di 30 giorni dalla ricezione, quindi entro il ____/____/____.

Qualora la richiesta risultasse particolarmente complessa, potremmo prorogare il termine di ulteriori 60 giorni, dandone tempestiva comunicazione con l'indicazione dei motivi del ritardo.

Per qualsiasi informazione o chiarimento, può contattare il nostro Referente Privacy: Email: privacy@centrophoenix.it Tel: [numero]

Cordiali saluti,

Centro Phoenix Srl e Centro Phoenix STP Srl Il Referente Privacy _____

MODULO 1-C: RISPOSTA POSITIVA - FORNITURA DATI

CENTRO PHOENIX SRL E CENTRO PHOENIX STP SRL [Indirizzo] [Contatti]

Protocollo n. ACC/[ANNO]/[NUMERO] Data: ____/____/____

Spett.le [Nome Cognome richiedente] [Indirizzo]

Oggetto: Riscontro richiesta di accesso ai dati personali - Art. 15 GDPR

Gentile [Sig./Sig.ra] [Cognome],

in riscontro alla Sua richiesta di accesso ai dati personali prot. n. ACC/[ANNO]/[NUMERO] del ____/____/____, formulata ai sensi dell'art. 15 del GDPR, Le forniamo le seguenti informazioni e documentazione.

1. CONFERMA DEL TRATTAMENTO Confermiamo che il Centro Phoenix Srl e Centro Phoenix STP Srl tratta dati personali che La riguardano.
2. FINALITÀ DEL TRATTAMENTO I Suoi dati personali sono trattati per le seguenti finalità: ☐ Erogazione prestazioni psicologiche (diagnosi, terapia, riabilitazione) ☐ Adempimenti amministrativi e contabili ☐ Adempimenti fiscali e previdenziali ☐ Gestione del rapporto contrattuale ☐ Ricerca scientifica [se ha prestato consenso] ☐ Marketing [se ha prestato consenso]
3. CATEGORIE DI DATI TRATTATI Trattiamo le seguenti categorie di dati personali che La riguardano: ☐ Dati anagrafici (nome, cognome, data e luogo di nascita, residenza) ☐ Dati di contatto (telefono, email) ☐ Dati relativi alla salute (anamnesi, diagnosi, percorso terapeutico) ☐ Dati economici (fatturazione, pagamenti) ☐ [Altro]: _____
4. DESTINATARI O CATEGORIE DI DESTINATARI I Suoi dati possono essere comunicati a: ☐ Professionisti sanitari coinvolti nel percorso di cura ☐ Società di servizi informatici (gestionale) ☐ Commercialista/consulente del lavoro ☐ Compagnie assicurative (solo se applicabile) ☐ Autorità giudiziarie o amministrative (quando previsto dalla legge)
5. PERIODO DI CONSERVAZIONE I Suoi dati sono conservati per:
 - Dati sanitari: fino a [X] anni dalla conclusione del trattamento, in conformità al Codice Deontologico degli Psicologi
 - Dati amministrativi/fiscali: 10 anni dalla cessazione del rapporto
 - Dati per ricerca: fino a revoca del consenso (in forma anonimizzata)
 - Dati per marketing: fino a revoca del consenso
6. DIRITTI DELL'INTERESSATO Le ricordiamo che Lei ha diritto di:
 - Ottenere la rettifica dei dati inesatti (art. 16 GDPR)
 - Ottenere la cancellazione dei dati (art. 17 GDPR)
 - Ottenere la limitazione del trattamento (art. 18 GDPR)
 - Opporsi al trattamento (art. 21 GDPR)
 - Ricevere i dati in formato strutturato (art. 20 GDPR - portabilità)
 - Revocare il consenso (quando il trattamento si basa sul consenso)
 - Proporre reclamo al Garante per la Protezione dei Dati Personali (www.garanteprivacy.it)

7. ORIGINE DEI DATI I dati sono stati raccolti: ☐ Direttamente presso di Lei (moduli, colloqui) ☐ Da terzi: [specificare se applicabile] _____
8. PROCESSO DECISIONALE AUTOMATIZZATO ☐ NON utilizziamo processi decisionali automatizzati o profilazione ☐ Utilizziamo: [specificare se applicabile] _____
9. TRASFERIMENTI EXTRA-UE ☐ I Suoi dati NON sono trasferiti verso paesi extra-UE ☐ I Suoi dati sono trasferiti verso: [specificare] _____ con le seguenti garanzie: _____
10. COPIA DEI DATI PERSONALI In allegato alla presente, Le forniamo copia dei Suoi dati personali oggetto di trattamento:

ALLEGATI: ☐ Allegato 1: Dati anagrafici e di contatto ☐ Allegato 2: Cartella clinica [può essere fornita in copia o consultabile su appuntamento] ☐ Allegato 3: Documentazione amministrativa/contabile ☐ Allegato 4: Consensi prestati ☐ Allegato 5: Altro _____

NOTE: [Eventuali limitazioni o precisazioni]

INFORMAZIONI SULLA FORNITURA DELLA COPIA: - La presente copia è fornita gratuitamente (prima copia) - Eventuali ulteriori copie potranno essere fornite dietro pagamento di un contributo per i costi amministrativi - Formato: ☐ Cartaceo ☐ Elettronico (PDF)

Per qualsiasi chiarimento o ulteriore richiesta, rimaniamo a disposizione.

Cordiali saluti,

Centro Phoenix Srl e Centro Phoenix STP Srl Il Titolare del Trattamento _____
[Firma e timbro]

MODULO 1-D: RICHIESTA DI CHIARIMENTI/INTEGRAZIONI

CENTRO PHOENIX SRL E CENTRO PHOENIX STP SRL [Indirizzo] [Contatti]

Protocollo n. ACC/[ANNO]/[NUMERO] Data: ____/____/____

Spett.le [Nome Cognome richiedente] [Indirizzo]

Oggetto: Richiesta chiarimenti - Richiesta di accesso ai dati personali

Gentile [Sig./Sig.ra] [Cognome],

in relazione alla Sua richiesta di accesso ai dati personali prot. n. ACC/[ANNO]/[NUMERO] del ____/____/____, al fine di fornirLe un riscontro completo ed accurato, Le chiediamo cortesemente di fornire i seguenti chiarimenti/integrazioni:

☐ Documento d'identità in corso di validità ☐ Delega/procura (in caso di richiesta per conto di terzi) ☐ Specificazione del periodo temporale di interesse ☐ Specificazione delle categorie di dati di interesse ☐ Altro: _____

La preghiamo di fornire la documentazione richiesta entro 7 giorni dalla ricezione della presente.

Il termine per la risposta alla Sua richiesta (30 giorni) decorrerà dalla data di ricevimento della documentazione integrativa.

Cordiali saluti,

Centro Phoenix Srl e Centro Phoenix STP Srl Il Referente Privacy _____

MODULO 1-E: COMUNICAZIONE DI PROROGA

CENTRO PHOENIX SRL E CENTRO PHOENIX STP SRL [Indirizzo] [Contatti]

Protocollo n. ACC/[ANNO]/[NUMERO] Data: ____/____/____

Spett.le [Nome Cognome richiedente] [Indirizzo]

Oggetto: Comunicazione proroga termini - Richiesta di accesso ai dati personali

Gentile [Sig./Sig.ra] [Cognome],

in relazione alla Sua richiesta di accesso ai dati personali prot. n. ACC/[ANNO]/[NUMERO] del ____/____/____, Le comuniciamo che, ai sensi dell'art. 12, comma 3 del GDPR, il termine di risposta è prorogato di ulteriori 60 giorni.

La proroga si rende necessaria per i seguenti motivi: ☐ Complessità della richiesta ☐ Elevato numero di dati da raccogliere e verificare ☐ Necessità di oscurare dati personali di terzi presenti nei documenti ☐ Altro: _____

La nuova data di scadenza per il riscontro è: ____/____/____

Ci scusiamo per il disagio e restiamo a disposizione per qualsiasi chiarimento.

Cordiali saluti,

Centro Phoenix Srl e Centro Phoenix STP Srl Il Referente Privacy _____

MODULO 1-F: DINIEGO TOTALE O PARZIALE

CENTRO PHOENIX SRL E CENTRO PHOENIX STP SRL [Indirizzo] [Contatti]

Protocollo n. ACC/[ANNO]/[NUMERO] Data: ____/____/____

Spett.le [Nome Cognome richiedente] [Indirizzo]

Oggetto: Diniego richiesta di accesso ai dati personali - Art. 15 GDPR

Gentile [Sig./Sig.ra] [Cognome],

in relazione alla Sua richiesta di accesso ai dati personali prot. n. ACC/[ANNO]/[NUMERO] del ____/____/____, con la presente siamo spiacenti di comunicarLe che non è possibile dare seguito alla richiesta per le seguenti motivazioni:

☐ RICHIESTA MANIFESTAMENTE INFONDATA Motivazione:

☐ RICHIESTA MANIFESTAMENTE ECCESSIVA Motivazione: _____

☐ IMPOSSIBILITÀ DI IDENTIFICARE IL RICHIEDENTE Motivazione: _____

☐ ASSENZA DI DATI PERSONALI Confermiamo che non trattiamo dati personali che La riguardano.

☐ ALTRO Motivazione: _____

DIRITTO DI RECLAMO: La informiamo che Lei ha il diritto di proporre reclamo all'Autorità Garante per la Protezione dei Dati Personali, contattabile all'indirizzo: - Sito web: www.garanteprivacy.it - Email: garante@gpdp.it - PEC: protocollo@pec.gpdp.it - Tel: 06.696771 - Indirizzo: Piazza Venezia 11, 00187 Roma

Può inoltre proporre ricorso giurisdizionale.

Cordiali saluti,

Centro Phoenix Srl e Centro Phoenix STP Srl Il Titolare del Trattamento _____
[Firma e timbro]

PROCEDURA 2: RETTIFICA E INTEGRAZIONE DATI (Art. 16 GDPR - Diritto di rettifica)

2.1 FINALITÀ E AMBITO DI APPLICAZIONE

Questa procedura disciplina la gestione delle richieste di rettifica dei dati personali inesatti o di integrazione dei dati incompleti, garantendo il rispetto dell'art. 16 GDPR.

L'interessato ha diritto di ottenere: - Rettifica dei dati personali inesatti - Integrazione dei dati personali incompleti - Aggiornamento dei dati personali

2.2 RESPONSABILITÀ

- REFERENTE PRIVACY: Ricezione e coordinamento gestione richieste
- TITOLARE DEL TRATTAMENTO: Autorizzazione rettifiche significative
- PERSONALE AUTORIZZATO: Esecuzione materiale delle rettifiche nei sistemi

2.3 MODALITÀ DI PRESENTAZIONE DELLA RICHIESTA

Identiche a quelle della Procedura 1 (accesso).

2.4 FLUSSO OPERATIVO

FASE 1: RICEZIONE E PROTOCOLLAZIONE (Giorno 0)

- STEP 1.1 - Ricezione e protocollazione - Assegnare numero protocollo: RETT/[ANNO]/[NUMERO] - Registrare nel “Registro Richieste Interessati” - Calcolare scadenza: 30 giorni dalla ricezione - Inviare ricevuta di ricezione (Modulo 2-A)

FASE 2: VERIFICA IDENTITÀ E ANALISI RICHIESTA (Giorni 1-5)

- STEP 2.1 - Verifica identità - Controllare documento d'identità - Verificare legittimazione del richiedente
- STEP 2.2 - Analisi della richiesta - Identificare i dati che l'interessato ritiene inesatti o incompleti - Comprendere le rettifiche/integrazioni richieste - Valutare se la richiesta è chiara e circostanziata
- STEP 2.3 - Richiesta eventuale documentazione - Se necessario, richiedere documentazione probatoria: * Certificati anagrafici per dati anagrafici * Certificati medici per dati sanitari * Altri documenti comprovanti l'inesattezza - Utilizzare Modulo 2-B per richiedere integrazioni

FASE 3: VERIFICA INESATTEZZA/INCOMPLETEZZA (Giorni 6-12)

- STEP 3.1 - Localizzazione dei dati - Identificare tutti i sistemi/archivi contenenti i dati in questione: * Cartella clinica (cartacea e digitale) * Database gestionale * Sistema contabile * Archivi di backup * Altri archivi
- STEP 3.2 - Verifica della fondatezza - Confrontare i dati attuali con quelli corretti indicati dall'interessato - Verificare eventuali documenti probatori forniti - Consultare eventuali fonti originarie dei dati
- STEP 3.3 - Valutazione Decidere se: a) ACCOGLIERE la richiesta: i dati sono effettivamente inesatti/incompleti b) RESPINGERE la richiesta: i dati sono corretti c) ACCOGLIERE PARZIALMENTE: solo alcuni dati sono inesatti

FASE 4: ESECUZIONE RETTIFICA/INTEGRAZIONE (Giorni 13-20)

- STEP 4.1 - Rettifica nei sistemi principali Se la richiesta è accolta:

Per DATI ANAGRAFICI/CONTATTO: - Aggiornare nel database gestionale - Aggiornare nelle cartelle cliniche - Aggiornare nel sistema contabile - Aggiornare in eventuali altri archivi

Per DATI SANITARI: - Rettificare nella cartella clinica - Mantenere traccia della modifica (chi, quando, perché) - Non cancellare il dato originale, ma annotare la rettifica - Esempio: “In data XX/XX/XXXX il dato [X] è stato rettificato in [Y] su richiesta dell'interessato prot. RETT/[ANNO]/[NUMERO]”

Per DATI ECONOMICI: - Valutare se la rettifica ha impatti su fatture già emesse - Se necessario, emettere nota di credito/debito - Aggiornare i registri contabili

- STEP 4.2 - Tracciabilità delle modifiche - Documentare ogni modifica effettuata - Indicare: data, operatore, dato originale, dato rettificato, motivo - Compilare “Log delle rettifiche” (Modulo 2-E)
- STEP 4.3 - Aggiornamento archivi di backup - Pianificare aggiornamento anche dei backup - Se tecnicamente impossibile: annotare la limitazione

FASE 5: COMUNICAZIONE AI DESTINATARI (Giorni 21-25)

- STEP 5.1 - Identificazione dei destinatari - Individuare tutti i soggetti a cui i dati sono stati comunicati:
* Altri professionisti sanitari * Società di servizi informatici * Commercialista * Compagnie assicurative
* Altri
- STEP 5.2 - Comunicazione della rettifica - Informare ciascun destinatario della rettifica effettuata - Richiedere che procedano a loro volta alla rettifica - Utilizzare Modulo 2-D per la comunicazione - Documentare l'avvenuta comunicazione
- STEP 5.3 - Eccezioni - Non comunicare se impossibile o richiede sforzo sproporzionato - Documentare le ragioni della mancata comunicazione

FASE 6: RISPOSTA ALL'INTERESSATO (Giorni 26-28)

- STEP 6.1 - Predisposizione risposta - Se accolta: Modulo 2-C (Conferma rettifica) - Se respinta: Modulo 2-F (Diniego rettifica) - Indicare le rettifiche effettuate - Elencare i destinatari informati (se richiesto dall'interessato)
- STEP 6.2 - Invio risposta - Inviare entro il termine di 30 giorni - Allegare eventuale documentazione - Archiviare copia
- STEP 6.3 - Registrazione - Aggiornare il "Registro Richieste Interessati" - Archiviare tutta la documentazione

2.5 CASI PARTICOLARI

A) RETTIFICA DI DATI SANITARI

- Particolare attenzione alla tracciabilità
- Mantenere sempre lo storico delle modifiche
- Non cancellare dati clinici originali, ma integrarli/annotarli
- Possibile consultazione con il professionista che ha generato il dato

B) CONTESTAZIONE SULLA RETTIFICA

- Se il Centro contesta la fondatezza della richiesta: documentare i motivi
- Fornire motivazione dettagliata all'interessato
- Informare del diritto di reclamo al Garante

C) RETTIFICA CON IMPATTI FISCALI/CONTABILI

- Consultare il commercialista
- Valutare necessità di rettificare documenti fiscali
- Documentare l'intervento

2.6 MODULISTICA

MODULO 2-A: RICEVUTA RICEZIONE RICHIESTA DI RETTIFICA

[Simile al Modulo 1-B, adattato per rettifica]

MODULO 2-B: RICHIESTA DOCUMENTAZIONE PROBATORIA

CENTRO PHOENIX SRL E CENTRO PHOENIX STP SRL

Protocollo n. RETT/[ANNO]/[NUMERO] Data: ____/____/____

Spett.le [Nome Cognome richiedente]

Oggetto: Richiesta documentazione probatoria - Rettifica dati personali

Gentile [Sig./Sig.ra] [Cognome],

in relazione alla Sua richiesta di rettifica prot. n. RETT/[ANNO]/[NUMERO], al fine di procedere con la verifica e l'eventuale rettifica dei dati, Le chiediamo cortesemente di fornire la seguente documentazione probatoria:

☐ Certificato anagrafico (per rettifica dati anagrafici) ☐ Documento d'identità aggiornato ☐ Certificato medico/referto (per rettifica dati sanitari) ☐ Altro:

La preghiamo di fornire la documentazione entro 7 giorni dalla ricezione della presente.

Cordiali saluti, Il Referente Privacy _____

MODULO 2-C: CONFERMA RETTIFICA EFFETTUATA

CENTRO PHOENIX SRL E CENTRO PHOENIX STP SRL

Protocollo n. RETT/[ANNO]/[NUMERO] Data: ____/____/____

Spett.le [Nome Cognome]

Oggetto: Conferma rettifica/integrazione dati personali - Art. 16 GDPR

Gentile [Sig./Sig.ra] [Cognome],

in riscontro alla Sua richiesta di rettifica/integrazione dei dati personali prot. n. RETT/[ANNO]/[NUMERO] del ____/____/____, Le confermiamo di aver provveduto alle seguenti rettifiche/integrazioni:

DATI RETTIFICATI/INTEGRATI:

1. Dato precedente: _____ Dato rettificato: _____ Data rettifica: ____/____/____
2. Dato precedente: _____ Dato rettificato: _____ Data rettifica: ____/____/____

[Aggiungere ulteriori rettifiche se necessario]

SISTEMI/ARCHIVI AGGIORNATI: ☐ Database gestionale pazienti ☐ Cartella clinica digitale ☐ Cartella clinica cartacea ☐ Sistema contabile ☐ Archivi di backup ☐ Altro: _____

DESTINATARI INFORMATI DELLA RETTIFICA: Abbiamo provveduto a comunicare la rettifica ai seguenti destinatari a cui i dati erano stati precedentemente comunicati: ☐ [Nome destinatario 1] ☐ [Nome destinatario 2] ☐ [Nome destinatario 3] ☐ Non applicabile (dati non comunicati a terzi)

[Se richiesto dall'interessato, fornire l'elenco completo dei destinatari]

Le confermiamo che i Suoi dati sono ora corretti e completi nei nostri sistemi.

Per qualsiasi ulteriore chiarimento, restiamo a disposizione.

Cordiali saluti,

Centro Phoenix Srl e Centro Phoenix STP Srl Il Titolare del Trattamento _____
[Firma e timbro]

MODULO 2-D: COMUNICAZIONE RETTIFICA AI DESTINATARI

CENTRO PHOENIX SRL E CENTRO PHOENIX STP SRL

Data: ____/____/____

Spett.le [Destinatario] [Indirizzo]

Oggetto: Comunicazione rettifica dati personali - Art. 19 GDPR

Egregi Signori,

con la presente Vi comunichiamo che, in seguito a richiesta dell'interessato ai sensi dell'art. 16 GDPR (diritto di rettifica), abbiamo provveduto a rettificare i seguenti dati personali relativi a:

Interessato: [Nome Cognome] Data di nascita: ____/____/____

Dati rettificati: - [Descrizione dato]: da "[valore precedente]" a "[valore rettificato]" - [Descrizione dato]: da "[valore precedente]" a "[valore rettificato]"

Vi preghiamo di prendere atto della rettifica e di procedere all'aggiornamento nei Vostri sistemi/archivi, qualora i dati Vi siano stati comunicati e siano ancora da Voi conservati.

Vi chiediamo cortesemente di confermare l'avvenuto aggiornamento.

Cordiali saluti,

Centro Phoenix Srl e Centro Phoenix STP Srl Il Referente Privacy _____

MODULO 2-E: LOG DELLE RETTIFICHE

REGISTRO RETTIFICHE DATI PERSONALI

Data	Protocollo	Interessato	Dato	Valore	Valore	Operatore	Note
	richiesta	rettificato	precedente	rettificato			
_____	_____	_____	_____	_____	_____	_____	RETT/25/001

MODULO 2-F: DINIEGO RETTIFICA

CENTRO PHOENIX SRL E CENTRO PHOENIX STP SRL

Protocollo n. RETT/[ANNO]/[NUMERO] Data: ____/____/____

Spett.le [Nome Cognome]

Oggetto: Diniego richiesta di rettifica dati personali - Art. 16 GDPR

Gentile [Sig./Sig.ra] [Cognome],

in relazione alla Sua richiesta di rettifica dei dati personali prot. n. RETT/[ANNO]/[NUMERO] del ____/____/____, dopo attenta verifica, non è possibile accogliere la richiesta per le seguenti motivazioni:

☐ I dati in nostro possesso risultano corretti e supportati da documentazione Motivazione:

☐ La richiesta non è sufficientemente circostanziata Motivazione:

☐ Manca documentazione probatoria Motivazione:

☐ Altro: _____

DIRITTO DI RECLAMO: La informiamo che Lei ha il diritto di: - Richiedere al Titolare del trattamento che sia apposta l'indicazione che i dati sono contestati (art. 18 GDPR - limitazione) - Proporre reclamo all'Autorità Garante per la Protezione dei Dati Personali (www.garanteprivacy.it) - Proporre ricorso giurisdizionale

Restiamo a disposizione per ogni chiarimento.

Cordiali saluti,

Centro Phoenix Srl e Centro Phoenix STP Srl Il Titolare del Trattamento _____
[Firma e timbro]

PROCEDURA 3: CANCELLAZIONE DATI - DIRITTO ALL'OBLIO (Art. 17 GDPR - Diritto alla cancellazione)

3.1 FINALITÀ E AMBITO DI APPLICAZIONE

Questa procedura disciplina la gestione delle richieste di cancellazione dei dati personali ("diritto all'oblio"), garantendo il rispetto dell'art. 17 GDPR.

L'interessato ha diritto di ottenere la cancellazione dei dati personali quando: a) I dati non sono più necessari rispetto alle finalità b) L'interessato revoca il consenso e non sussiste altro fondamento giuridico c) L'interessato si oppone al trattamento e non sussiste un motivo legittimo prevalente d) I dati sono stati trattati illecitamente e) I dati devono essere cancellati per adempiere un obbligo legale f) I dati sono stati raccolti da minori per servizi della società dell'informazione

IMPORTANTE: Il diritto alla cancellazione NON è assoluto ed incontra limiti significativi, soprattutto in ambito sanitario.

3.2 RESPONSABILITÀ

- REFERENTE PRIVACY: Ricezione e coordinamento
- TITOLARE DEL TRATTAMENTO: Decisione finale (obbligo coinvolgimento per la delicatezza della materia)
- PERSONALE AUTORIZZATO: Esecuzione materiale cancellazioni autorizzate

3.3 MODALITÀ DI PRESENTAZIONE DELLA RICHIESTA

Identiche a quelle della Procedura 1 (accesso).

3.4 FLUSSO OPERATIVO

FASE 1: RICEZIONE E PROTOCOLLAZIONE (Giorno 0)

- STEP 1.1 - Ricezione e protocollazione - Assegnare numero protocollo: CANC/[ANNO]/[NUMERO] - Registrare nel “Registro Richieste Interessati” - Calcolare scadenza: 30 giorni dalla ricezione - Inviare ricevuta di ricezione (Modulo 3-A)
- STEP 1.2 - Alert immediato al Titolare - Informare immediatamente il Titolare del trattamento - Le richieste di cancellazione richiedono valutazione attenta

FASE 2: VERIFICA IDENTITÀ E ANALISI RICHIESTA (Giorni 1-5)

- STEP 2.1 - Verifica identità - Controllare documento d'identità - Verificare legittimazione
- STEP 2.2 - Analisi della motivazione - Comprendere il motivo della richiesta di cancellazione - Identificare su quale presupposto si fonda (lettere a-f dell'art. 17)

FASE 3: VERIFICA PRESUPPOSTI PER LA CANCELLAZIONE (Giorni 6-15) *** FASE CRITICA - COINVOLGERE SEMPRE IL TITOLARE ***

- STEP 3.1 - Mappatura dei dati - Identificare tutti i dati personali dell'interessato - Localizzare tutti i sistemi/archivi che li contengono
- STEP 3.2 - Verifica presupposti POSITIVI (pro-cancellazione)

Verificare se sussiste almeno uno dei seguenti presupposti:

- a) DATI NON PIÙ NECESSARI I dati non sono più necessari rispetto alle finalità per cui sono stati raccolti o trattati. Esempio: paziente che ha concluso il percorso terapeutico da oltre [X] anni e non vi sono obblighi di conservazione.
- b) REVOCA DEL CONSENSO L'interessato revoca il consenso su cui si basa il trattamento e non esiste altro fondamento giuridico. ATTENZIONE: In ambito sanitario, il trattamento per finalità di cura NON si basa sul consenso ma su obbligo legale/interesse vitale. Applicabile a: dati per ricerca scientifica, marketing.
- c) OPPOSIZIONE AL TRATTAMENTO L'interessato si oppone al trattamento (art. 21) e non sussiste un motivo legittimo prevalente.
- d) TRATTAMENTO ILLECITO I dati sono stati trattati illecitamente.

□ e) **OBBLIGO LEGALE DI CANCELLAZIONE** I dati devono essere cancellati per adempiere un obbligo legale.

□ f) **DATI DI MINORI** I dati sono stati raccolti da minori per servizi della società dell'informazione (es. app, social).

□ **STEP 3.3 - Verifica ECCEZIONI (contro-cancellazione)**

***** ATTENZIONE: IN AMBITO SANITARIO LE ECCEZIONI SONO PREVALENTI *****

Il diritto alla cancellazione **NON** si applica quando il trattamento è necessario per:

□ a) **ESERCIZIO DIRITTO DI LIBERTÀ DI ESPRESSIONE E INFORMAZIONE** Raramente applicabile in ambito sanitario.

□ b) **ADEMPIMENTO OBBLIGO LEGALE / COMPITO DI INTERESSE PUBBLICO *** ECCEZIONE FONDAMENTALE IN AMBITO SANITARIO ***** - Obbligo di conservazione cartella clinica (Codice Deontologico Psicologi: raccomanda conservazione per almeno 5 anni, alcuni interpretano fino a 10-20 anni) - Obblighi contabili/fiscali (10 anni) - Obblighi previdenziali - Altri obblighi di legge settoriali

□ c) **MOTIVI DI INTERESSE PUBBLICO IN SANITÀ *** ECCEZIONE FONDAMENTALE IN AMBITO SANITARIO ***** - Finalità di medicina preventiva - Diagnosi e assistenza sanitaria - Gestione dei sistemi sanitari - Interesse pubblico nel settore della sanità pubblica

□ d) **FINALITÀ DI ARCHIVIAZIONE NEL PUBBLICO INTERESSE, RICERCA SCIENTIFICA, STATISTICA** Se la cancellazione rischia di rendere impossibile o pregiudicare gravemente il conseguimento degli obiettivi.

□ e) **ACCERTAMENTO, ESERCIZIO O DIFESA DI UN DIRITTO IN SEDE GIUDIZIARIA** - Contenzioso in corso con il paziente - Potenziale contenzioso (conservazione a fini difensivi) - Procedimenti penali, civili, amministrativi

□ **STEP 3.4 - Bilanciamento e decisione**

PRINCIPIO: In ambito psicologico-sanitario, il diritto alla cancellazione è **FORTEMENTE LIMITATO** dagli obblighi professionali e di legge.

VALUTAZIONE DA EFFETTUARE (con il Titolare):

1) Verificare se esistono **OBBLIGHI DI CONSERVAZIONE**:

- Codice Deontologico Psicologi (art. 15): conservazione documentazione
- Obblighi fiscali/contabili: 10 anni
- Altri obblighi settoriali

SE SÌ → **DINIEGO MOTIVATO** (impossibile cancellare)

2) Se **NON** esistono obblighi di conservazione attuali:

- Verificare se il periodo minimo consigliato è trascorso
- Verificare assenza di contenziosi in corso o potenziali
- Verificare che la cancellazione non pregiudichi diritti del Centro

SE OK → CANCELLAZIONE POSSIBILE SE NON OK → DINIEGO MOTIVATO o LIMITAZIONE (art. 18)

3) Considerare richieste PARZIALI:

- Cancellazione dati per finalità specifiche (es. marketing)
- Mantenimento dati per finalità con base giuridica (es. cura, contabilità)

FASE 4: DECISIONE ED EVENTUALE ESECUZIONE (Giorni 16-25)

□ STEP 4.1 - Decisione formale del Titolare - Il Titolare decide se accogliere, respingere o accogliere parzialmente - Documentare motivazioni della decisione - Compilare “Verbale di valutazione richiesta cancellazione” (Modulo 3-E)

□ STEP 4.2 - Se ACCOLTA (totalmente o parzialmente):

A) CANCELLAZIONE LOGICA vs CANCELLAZIONE FISICA

CANCELLAZIONE LOGICA (preferibile in ambito sanitario):

- I dati non sono eliminati fisicamente ma resi inaccessibili
- I dati sono “oscurati” o “bloccati”
- Possibile recupero in caso di necessità legale/giudiziaria
- Tracciabilità dell’operazione

CANCELLAZIONE FISICA:

- I dati sono eliminati definitivamente e irrecuperabilmente
- Possibile solo se assenza assoluta di obblighi conservazione
- Attenzione ai backup

B) ESECUZIONE CANCELLAZIONE

□ Identificare tutti i sistemi/archivi contenenti i dati

□ CARTELLA CLINICA DIGITALE:

- Cancellare/oscurare i dati secondo modalità decisa
- Annotare: “Dati cancellati su richiesta interessato prot. CANC/[ANNO]/[NUMERO] del [DATA]”
- Mantenere traccia dell’operazione

□ CARTELLA CLINICA CARTACEA:

- Apporre timbro/annotazione: “Cancellato su richiesta interessato”
- Trasferire in archivio separato con accesso limitato (se cancellazione logica)
- Oppure distruggere fisicamente con metodi sicuri (se cancellazione fisica autorizzata)

□ DATABASE GESTIONALE:

- Cancellare/anonimizzare i dati anagrafici
- Mantenere solo identificativo anonimo se necessario per statistiche

□ SISTEMA CONTABILE:

- Valutare attentamente: obblighi fiscali di 10 anni
- Possibile solo anonimizzazione (rimozione dati anagrafici dettagliati)
- EMAIL E CORRISPONDENZA:
 - Cancellare email contenenti dati del paziente
 - Eliminare file allegati
- BACKUP:
 - Cancellare dai backup più recenti
 - Documentare se impossibile cancellare da backup datati (giustificazione tecnica)
 - Garantire che dati nei vecchi backup non siano accessibili

C) TRACCIABILITÀ

- Documentare tutte le cancellazioni effettuate
 - Compilare “Log cancellazioni” (Modulo 3-F)
 - Conservare la documentazione relativa alla richiesta e al processo decisionale
- STEP 4.3 - Se RESPINTA: - Predisporre motivazione dettagliata (Modulo 3-D) - Indicare le specifiche eccezioni applicabili (art. 17, par. 3 GDPR)

FASE 5: COMUNICAZIONE AI DESTINATARI (Giorni 26-28)

- STEP 5.1 - Se la cancellazione è stata effettuata: - Identificare tutti i destinatari a cui i dati erano stati comunicati - Informare ciascun destinatario della cancellazione - Richiedere che procedano a loro volta alla cancellazione - Documentare l’avvenuta comunicazione
- STEP 5.2 - Eccezioni alla comunicazione: - Se impossibile - Se richiede sforzo sproporzionato - Documentare le ragioni

FASE 6: RISPOSTA ALL’INTERESSATO (Giorni 27-30)

- STEP 6.1 - Predisposizione risposta - Se accolta: Modulo 3-B (Conferma cancellazione) - Se accolta parzialmente: Modulo 3-C (Cancellazione parziale) - Se respinta: Modulo 3-D (Diniego cancellazione)
- STEP 6.2 - Invio risposta - Inviare risposta motivata - Se diniego: fornire motivazione dettagliata e riferimenti normativi - Informare del diritto di reclamo al Garante
- STEP 6.3 - Archiviazione - Archiviare tutta la documentazione del processo decisionale - Conservare per almeno 5 anni

3.5 CASI PARTICOLARI - AMBITO SANITARIO

A) RICHIESTA DI CANCELLAZIONE CARTELLA CLINICA

*** CASO FREQUENTE E DELICATO ***

PRINCIPIO: La cartella clinica è documento sanitario che il professionista ha l’OBBLIGO di conservare.

RISPOSTA TIPICA: DINIEGO MOTIVATO

Motivazioni da indicare:

- Art. 17, par. 3, lett. b) GDPR: necessità per adempimento obbligo legale
- Art. 17, par. 3, lett. c) GDPR: motivi di interesse pubblico in sanità
- Codice Deontologico Psicologi (art. 15): obbligo conservazione documentazione
- Art. 17, par. 3, lett. e) GDPR: necessità per accertamento/difesa diritti in sede giudiziaria (potenziale contenzioso)
- Obblighi assicurativi (polizza RC professionale richiede conservazione documentazione)

ECCEZIONE: Possibile cancellazione solo se:

- Trascorso tempo molto lungo (es. >20 anni) E
- Nessun obbligo di conservazione residuo E
- Nessun contenzioso in corso o prevedibile E
- Autorizzazione del Titolare

ALTERNATIVA: Proporre LIMITAZIONE del trattamento (art. 18 GDPR) invece di cancellazione - vedi Procedura 4.

B) RICHIESTA DI CANCELLAZIONE PER REVOCA CONSENSO RICERCA SCIENTIFICA

POSSIBILE ACCOGLIMENTO se:

- Il trattamento per ricerca si basava sul consenso E
- I dati non sono già stati anonimizzati E
- La cancellazione non pregiudica gravemente la ricerca

Procedura:

- Cancellare i dati dalla banca dati di ricerca
- Anonimizzare se già inclusi in dataset di ricerca
- Comunicare agli eventuali partner di ricerca

C) RICHIESTA DI CANCELLAZIONE DATI AMMINISTRATIVI/ECONOMICI

DINIEGO se entro periodo di conservazione obbligatoria (10 anni fiscali)

ACCOGLIMENTO se:

- Trascorsi termini di conservazione fiscale E
- Nessun contenzioso in essere

ALTERNATIVA: Cancellare dati eccedenti (es. indirizzi email, note) ma mantenere dati essenziali per adempimenti.

D) RICHIESTA DA PARTE DI EREDI

VALUTARE CASO PER CASO:

- Gli eredi hanno diritti limitati sui dati del defunto
- Bilanciare diritti eredi con riservatezza del defunto
- Considerare volontà del defunto se espressa in vita
- In caso di dubbio: consultare Garante Privacy

3.6 TEMPI DI CONSERVAZIONE RACCOMANDATI - AMBITO PSICOLOGICO

Per orientare le decisioni sulle richieste di cancellazione:

DATI CLINICI (Cartella clinica): - Minimo: 5 anni dalla conclusione trattamento (prassi professionale)
- Consigliato: 10 anni (possibile contenzioso civile - prescrizione ordinaria) - Esteso: fino a 20 anni in casi particolari (minori, patologie rilevanti)

DATI AMMINISTRATIVI/FISCALI: - Obbligatorio: 10 anni (normativa fiscale)

DATI PER RICERCA: - Fino a revoca consenso (possibile anonimizzazione invece di cancellazione)

DATI PER MARKETING: - Fino a revoca consenso o opposizione

3.7 MODULISTICA

MODULO 3-A: RICEVUTA RICEZIONE RICHIESTA DI CANCELLAZIONE

[Simile al Modulo 1-B, adattato per cancellazione]

MODULO 3-B: CONFERMA CANCELLAZIONE

CENTRO PHOENIX SRL E CENTRO PHOENIX STP SRL

Protocollo n. CANC/[ANNO]/[NUMERO] Data: ____/____/____

Spett.le [Nome Cognome]

Oggetto: Conferma cancellazione dati personali - Art. 17 GDPR

Gentile [Sig./Sig.ra] [Cognome],

in riscontro alla Sua richiesta di cancellazione dei dati personali prot. n. CANC/[ANNO]/[NUMERO] del ____/____/____, Le confermiamo di aver provveduto alla cancellazione dei Suoi dati personali.

DATI CANCELLATI: ☐ Dati anagrafici e di contatto ☐ Dati per finalità di marketing ☐ Dati per finalità di ricerca scientifica ☐ Altri dati:

SISTEMI/ARCHIVI DA CUI SONO STATI CANCELLATI: ☐ Database gestionale ☐ Sistema di email/newsletter ☐ Banca dati ricerca scientifica ☐ Altro:

MODALITÀ DI CANCELLAZIONE: ☐ Cancellazione definitiva e irreversibile ☐ Cancellazione logica (dati resi inaccessibili ma recuperabili per obblighi legali)

Data cancellazione: ____/____/____

DESTINATARI INFORMATI: Abbiamo informato i seguenti destinatari della cancellazione: ☐ [Nome destinatario 1] ☐ [Nome destinatario 2] ☐ Non applicabile

DATI CONSERVATI: I seguenti dati NON sono stati cancellati in quanto soggetti a obblighi di conservazione: ☐ Cartella clinica (obbligo professionale e legale - conservazione fino al

____/____/____) ☐ Dati contabili/fiscali (obbligo legale - conservazione fino al ____/____/____) ☐
Altro: _____

Motivazione: _____

La informiamo che i dati non cancellati (se presenti) saranno conservati esclusivamente per le finalità previste dalla legge e saranno cancellati al termine del periodo di conservazione obbligatorio.

Cordiali saluti,

Centro Phoenix Srl e Centro Phoenix STP Srl Il Titolare del Trattamento _____
[Firma e timbro]

MODULO 3-C: CONFERMA CANCELLAZIONE PARZIALE

[Simile al Modulo 3-B, con sezione ampliata su “DATI CONSERVATI” e relative motivazioni dettagliate]

MODULO 3-D: DINIEGO CANCELLAZIONE

CENTRO PHOENIX SRL E CENTRO PHOENIX STP SRL

Protocollo n. CANC/[ANNO]/[NUMERO] Data: ____/____/____

Spett.le [Nome Cognome]

Oggetto: Diniego richiesta di cancellazione dati personali - Art. 17 GDPR

Gentile [Sig./Sig.ra] [Cognome],

in relazione alla Sua richiesta di cancellazione dei dati personali prot. n. CANC/[ANNO]/[NUMERO] del ____/____/____, dopo attenta valutazione, non è possibile accogliere la richiesta per le seguenti motivazioni giuridiche:

MOTIVAZIONI DEL DINIEGO (Art. 17, par. 3 GDPR):

☐ a) ADEMPIMENTO DI UN OBBLIGO LEGALE (Art. 17, par. 3, lett. b)

Il trattamento è necessario per adempiere un obbligo legale:

☐ Obbligo di conservazione documentazione sanitaria: - Codice Deontologico degli Psicologi (art. 15): conservazione documentazione professionale - Periodo di conservazione ancora in corso: fino al ____/____/____ - Motivazione: [dettagliare]

☐ Obblighi fiscali e contabili: - Art. 2220 Codice Civile e normativa fiscale: conservazione documentazione contabile per 10 anni - Periodo di conservazione ancora in corso: fino al ____/____/____

☐ Altri obblighi di legge: - Specificare: _____

☐ b) MOTIVI DI INTERESSE PUBBLICO IN SANITÀ (Art. 17, par. 3, lett. c)

Il trattamento è necessario per motivi di interesse pubblico nel settore della sanità pubblica: - Finalità di medicina preventiva - Diagnosi e assistenza sanitaria - Gestione dei servizi sanitari

Motivazione: La cartella clinica costituisce documentazione essenziale per garantire la continuità assistenziale e la tracciabilità del percorso terapeutico. La sua conservazione è nell'interesse pubblico della tutela della salute.

☐ c) ACCERTAMENTO, ESERCIZIO O DIFESA DI DIRITTI IN SEDE GIUDIZIARIA (Art. 17, par. 3, lett. e)

Il trattamento è necessario per: ☐ Contenzioso in corso: [specificare] ☐ Potenziale contenzioso: La documentazione è necessaria per l'eventuale difesa del Centro in sede giudiziaria (prescrizione decennale per responsabilità professionale) ☐ Obbligo assicurativo: Polizza RC professionale richiede conservazione documentazione

☐ d) FINALITÀ DI ARCHIVIAZIONE DI INTERESSE PUBBLICO, RICERCA SCIENTIFICA (Art. 17, par. 3, lett. d)

La cancellazione renderebbe impossibile o pregiudicherebbe gravemente il conseguimento degli obiettivi del trattamento per finalità di ricerca. [Raramente applicabile - solo se dati già anonimizzati e integrati in dataset]

PERIODO DI CONSERVAZIONE RESIDUO: I Suoi dati saranno conservati fino al: ____/____/____
Al termine di tale periodo, procederemo alla cancellazione salvo sussistano ulteriori obblighi di conservazione.

ALTERNATIVE POSSIBILI: Le segnaliamo che, in alternativa alla cancellazione, potrebbe esercitare il diritto di: ☐ LIMITAZIONE del trattamento (Art. 18 GDPR): i dati vengono conservati ma non utilizzati (salvo per obblighi legali e difesa diritti) ☐ OPPOSIZIONE al trattamento per specifiche finalità (Art. 21 GDPR)

DIRITTO DI RECLAMO: La informiamo che Lei ha il diritto di proporre reclamo all'Autorità Garante per la Protezione dei Dati Personali: - Sito web: www.garanteprivacy.it - Email: garante@gpdp.it - PEC: protocollo@pec.gpdp.it - Tel: 06.696771 - Indirizzo: Piazza Venezia 11, 00187 Roma

Può inoltre proporre ricorso giurisdizionale.

Restiamo a disposizione per ogni chiarimento.

Cordiali saluti,

Centro Phoenix Srl e Centro Phoenix STP Srl Il Titolare del Trattamento _____
[Firma e timbro]

MODULO 3-E: VERBALE DI VALUTAZIONE RICHIESTA CANCELLAZIONE

VERBALE DI VALUTAZIONE - RICHIESTA CANCELLAZIONE DATI

Protocollo richiesta: CANC/[ANNO]/[NUMERO] Data richiesta: ____/____/____ Interessato: _____

Data valutazione: ____/____/____ Presenti: - Titolare del trattamento: _____
- Referente Privacy: _____
[Altri partecipanti]: _____

1. SINTESI DELLA RICHIESTA:

2. DATI OGGETTO DELLA RICHIESTA: ☐ Cartella clinica ☐ Dati amministrativi/contabili ☐
Dati per ricerca scientifica ☐ Dati per marketing ☐ Altro:

3. PRESUPPOSTI PER LA CANCELLAZIONE (Art. 17, par. 1): ☐ Sì ☐ No Dati non più necessari
☐ Sì ☐ No Revoca del consenso ☐ Sì ☐ No Opposizione al trattamento ☐ Sì ☐ No Trattamento
illecito ☐ Sì ☐ No Obbligo legale di cancellazione

4. ECCEZIONI ALLA CANCELLAZIONE (Art. 17, par. 3): ☐ Sì ☐ No Adempimento obbligo
legale Specificare: _____ ☐ Sì ☐ No Motivi
di interesse pubblico in sanità ☐ Sì ☐ No Accertamento/difesa diritti in sede giudiziaria ☐ Sì ☐ No
Finalità di ricerca scientifica

5. OBBLIGHI DI CONSERVAZIONE: ☐ Sì ☐ No Codice Deontologico Psicologi Periodo residuo:
fino al ____/____/____ ☐ Sì ☐ No Obblighi fiscali/contabili Periodo residuo: fino al
____/____/____ ☐ Sì ☐ No Altri obblighi:

6. CONTENZIOSO: ☐ Sì ☐ No Contenzioso in corso ☐ Sì ☐ No Potenziale contenzioso prevedibile

7. VALUTAZIONE TECNICA: Possibilità tecnica di cancellazione: ☐ Sì ☐ No ☐ Parziale Note:

8. DECISIONE: ☐ ACCOLTA - Cancellazione totale ☐ ACCOLTA PARZIALMENTE -
Specificare: _____ ☐ RESPINTA

Motivazione della decisione:

9. MODALITÀ DI CANCELLAZIONE (se accolta): ☐ Cancellazione fisica (definitiva) ☐
Cancellazione logica (dati resi inaccessibili)

Sistemi da cui cancellare: ☐ Cartella clinica digitale ☐ Cartella clinica cartacea ☐ Database gestionale ☐
Sistema contabile ☐ Email ☐ Backup ☐ Altro:

10. COMUNICAZIONE AI DESTINATARI: ☐ Sì ☐ No Necessaria Se sì, destinatari da informare:

Il Titolare del Trattamento Il Referente Privacy _____

MODULO 3-F: LOG CANCELLAZIONI

REGISTRO CANCELLAZIONI DATI PERSONALI

Data	Protocollo	Interessato	Dati	Sistemi	Modalità	Operatore	Note
	richiesta	cancellati	coinvolti	cancellazione			
CANC/25/001		☐ Fisica		☐ Logica			

PROCEDURA 4: LIMITAZIONE DEL TRATTAMENTO (Art. 18 GDPR - Diritto di limitazione)

4.1 FINALITÀ E AMBITO DI APPLICAZIONE

Questa procedura disciplina la gestione delle richieste di limitazione del trattamento dei dati personali, garantendo il rispetto dell'art. 18 GDPR.

COSA SIGNIFICA "LIMITAZIONE": I dati vengono conservati ma non possono essere trattati (utilizzati) salvo eccezioni specifiche.

L'interessato ha diritto di ottenere la limitazione del trattamento quando: a) Contesta l'esattezza dei dati (per il periodo necessario alla verifica) b) Il trattamento è illecito ma l'interessato si oppone alla cancellazione c) I dati non sono più necessari al Titolare ma servono all'interessato per l'accertamento/difesa di diritti in sede giudiziaria d) L'interessato si è opposto al trattamento (in attesa della verifica se i motivi legittimi del Titolare prevalgono)

EFFETTI DELLA LIMITAZIONE: - I dati sono conservati - I dati NON possono essere trattati (utilizzati) salvo: * Consenso dell'interessato * Accertamento, esercizio o difesa di un diritto in sede giudiziaria * Tutela dei diritti di un'altra persona * Motivi di interesse pubblico rilevante UE o Stato membro

4.2 RESPONSABILITÀ

- REFERENTE PRIVACY: Ricezione e coordinamento
- TITOLARE DEL TRATTAMENTO: Valutazione e autorizzazione limitazione
- PERSONALE AUTORIZZATO: Applicazione tecnica della limitazione

4.3 MODALITÀ DI PRESENTAZIONE DELLA RICHIESTA

Identiche a quelle della Procedura 1 (accesso).

4.4 FLUSSO OPERATIVO

FASE 1: RICEZIONE E PROTOCOLLAZIONE (Giorno 0)

□ STEP 1.1 - Ricezione e protocollazione - Assegnare numero protocollo: LIM/[ANNO]/[NUMERO] - Registrare nel “Registro Richieste Interessati” - Calcolare scadenza: 30 giorni dalla ricezione - Inviare ricevuta di ricezione (Modulo 4-A)

FASE 2: VERIFICA IDENTITÀ E ANALISI RICHIESTA (Giorni 1-5)

□ STEP 2.1 - Verifica identità - Controllare documento d'identità - Verificare legittimazione

□ STEP 2.2 - Identificazione del presupposto Comprendere su quale base si fonda la richiesta:

□ a) CONTESTAZIONE ESATTEZZA DATI L'interessato contesta l'esattezza di alcuni dati → Limitazione temporanea in attesa di verifica → Collegare eventualmente a procedura di rettifica (Procedura 2)

□ b) TRATTAMENTO ILLECITO + OPPOSIZIONE A CANCELLAZIONE L'interessato ritiene che il trattamento sia illecito ma preferisce la limitazione alla cancellazione

□ c) DATI NON PIÙ NECESSARI AL TITOLARE MA NECESSARI ALL'INTERESSATO I dati non servono più al Titolare ma l'interessato ne ha bisogno per difendersi in giudizio Esempio: contenzioso tra paziente e Centro

□ d) OPPOSIZIONE AL TRATTAMENTO IN ATTESA DI VERIFICA L'interessato si è opposto al trattamento e si attende la verifica se i motivi legittimi del Titolare prevalgono

FASE 3: VALUTAZIONE DELLA RICHIESTA (Giorni 6-15)

□ STEP 3.1 - Mappatura dei dati interessati - Identificare i dati oggetto della richiesta di limitazione - Localizzare tutti i sistemi/archivi che li contengono

□ STEP 3.2 - Valutazione fondatezza

PER CASO a) - CONTESTAZIONE ESATTEZZA: - Avviare verifica dell'esattezza (vedi Procedura 2 - Rettifica) - La limitazione è OBBLIGATORIA per il periodo della verifica - Durata stimata verifica: _____ giorni

PER CASO b) - TRATTAMENTO ILLECITO: - Verificare se effettivamente il trattamento è/era illecito - Se illecito: ACCOGLIERE la richiesta - Se lecito: RESPINGERE motivando

PER CASO c) - NECESSITÀ DELL'INTERESSATO PER DIFESA IN GIUDIZIO: - Verificare se sussiste effettivamente un procedimento giudiziario - Verificare se i dati sono ancora necessari al Titolare - Se necessari all'interessato per difesa: ACCOGLIERE

PER CASO d) - OPPOSIZIONE AL TRATTAMENTO: - Valutare se esistono motivi legittimi cogenti del Titolare - La limitazione è OBBLIGATORIA in attesa della verifica - Vedi anche Procedura 6 (Opposizione)

□ STEP 3.3 - Decisione - Determinare se accogliere o respingere - Se accolta: determinare durata della limitazione - Compilare “Verbale di valutazione limitazione” (Modulo 4-E)

FASE 4: APPLICAZIONE DELLA LIMITAZIONE (Giorni 16-22)

□ STEP 4.1 - Implementazione tecnica

OBIETTIVO: Garantire che i dati siano conservati ma non utilizzati

METODI DI IMPLEMENTAZIONE:

A) MARCATURA/ETICHETTATURA

- Applicare flag “LIMITATO” nel database
- Annotare nella cartella clinica cartacea: “TRATTAMENTO LIMITATO - Richiesta prot. LIM/[ANNO]/[NUMERO]”
- Data inizio limitazione: ____/____/____

B) SEGREGAZIONE

- Trasferire i dati in archivio separato ad accesso ristretto
- Limitare autorizzazioni di accesso al minimo indispensabile

C) BLOCCO FUNZIONALE

- Disabilitare funzionalità di modifica/utilizzo nei sistemi informatici
- Mantenere solo funzioni di consultazione (se autorizzata)

☐ STEP 4.2 - Applicazione nei singoli sistemi

☐ CARTELLA CLINICA DIGITALE: - Apporre indicatore “TRATTAMENTO LIMITATO” - Bloccare modifiche (salvo per rettifica in caso a)) - Limitare accesso

☐ CARTELLA CLINICA CARTACEA: - Apporre timbro/etichetta visibile: “TRATTAMENTO LIMITATO” - Trasferire in archivio ad accesso ristretto

☐ DATABASE GESTIONALE: - Impostare flag di limitazione - Disabilitare utilizzo per finalità operative (es. no invio comunicazioni)

☐ SISTEMA DI NEWSLETTER/MARKETING: - Rimuovere dalle liste attive - Mantenere in archivio “sospesi”

☐ BACKUP: - Annotare la limitazione (se tecnicamente possibile)

☐ STEP 4.3 - Informazione al personale - Informare tutti gli autorizzati al trattamento della limitazione - Specificare che i dati NON possono essere utilizzati salvo eccezioni - Documentare l'informazione fornita

☐ STEP 4.4 - Tracciabilità - Documentare tutte le azioni intraprese - Compilare “Log limitazioni” (Modulo 4-F)

FASE 5: COMUNICAZIONE AI DESTINATARI (Giorni 23-25)

☐ STEP 5.1 - Identificazione destinatari - Individuare tutti i soggetti a cui i dati sono stati comunicati

☐ STEP 5.2 - Comunicazione della limitazione - Informare ciascun destinatario della limitazione applicata - Richiedere che applichino a loro volta la limitazione - Utilizzare Modulo 4-D - Documentare l'avvenuta comunicazione

☐ STEP 5.3 - Eccezioni - Non comunicare se impossibile o sforzo sproporzionato - Documentare ragioni

FASE 6: RISPOSTA ALL'INTERESSATO (Giorni 26-28)

☐ STEP 6.1 - Predisposizione risposta - Se accolta: Modulo 4-B (Conferma limitazione) - Se respinta: Modulo 4-C (Diniego limitazione) - Specificare durata della limitazione - Indicare le condizioni per la revoca

☐ STEP 6.2 - Invio risposta - Inviare entro termine di 30 giorni - Archiviare copia

FASE 7: GESTIONE DELLA LIMITAZIONE NEL TEMPO

☐ STEP 7.1 - Monitoraggio periodico - Verificare periodicamente se permangono i presupposti per la limitazione - Valutare conclusione verifica (caso a) o (caso d)) - Valutare se dati ancora necessari all'interessato (caso c))

☐ STEP 7.2 - Revoca della limitazione

La limitazione viene REVOCATA quando: - Cessano i motivi che l'hanno determinata - L'interessato revoca la richiesta - Conclusione della verifica (casi a) e d)) - Conclusione procedimento giudiziario (caso c))

OBBLIGO: Informare l'interessato PRIMA di revocare la limitazione (art. 18, par. 3 GDPR)

Procedura di revoca: ☐ Predisporre comunicazione preventiva all'interessato (Modulo 4-G) ☐ Attendere [X giorni] per dare tempo all'interessato di reagire ☐ Rimuovere i blocchi/flag di limitazione dai sistemi ☐ Ripristinare normale trattamento ☐ Documentare la revoca nel Log

4.5 UTILIZZO DEI DATI LIMITATI - ECCEZIONI

Anche durante la limitazione, i dati POSSONO essere trattati nei seguenti casi:

☐ a) CONSENSO DELL'INTERESSATO L'interessato autorizza espressamente un'operazione di trattamento Esempio: richiede copia della cartella → Richiedere consenso scritto e specifico

☐ b) ACCERTAMENTO, ESERCIZIO O DIFESA DI DIRITTI IN SEDE GIUDIZIARIA Il Titolare deve utilizzare i dati per difendersi in giudizio → Documentare la necessità → Limitare l'utilizzo allo stretto necessario

☐ c) TUTELA DEI DIRITTI DI UN'ALTRA PERSONA Raramente applicabile → Valutare caso per caso

☐ d) MOTIVI DI INTERESSE PUBBLICO RILEVANTE Esempio: indagini delle autorità sanitarie → Valutare con il Titolare → Documentare ampiamente

IMPORTANTE: Ogni utilizzo durante la limitazione deve essere: - Documentato - Motivato con riferimento a una delle eccezioni sopra - Comunicato all'interessato

4.6 DIFFERENZA TRA LIMITAZIONE E CANCELLAZIONE

LIMITAZIONE (Art. 18): - I dati SONO conservati - I dati NON sono utilizzati (salvo eccezioni) - Soluzione temporanea o permanente - Preferibile quando esistono obblighi di conservazione

CANCELLAZIONE (Art. 17): - I dati NON sono più conservati - I dati sono eliminati - Soluzione definitiva - Possibile solo se nessun obbligo di conservazione

IN AMBITO SANITARIO: Spesso la LIMITAZIONE è l'unica soluzione praticabile quando il paziente non vuole che i suoi dati siano utilizzati ma sussistono obblighi di conservazione della cartella clinica.

4.7 MODULISTICA

MODULO 4-A: RICEVUTA RICEZIONE RICHIESTA DI LIMITAZIONE

[Simile ai precedenti, adattato]

MODULO 4-B: CONFERMA LIMITAZIONE

CENTRO PHOENIX SRL E CENTRO PHOENIX STP SRL

Protocollo n. LIM/[ANNO]/[NUMERO] Data: ____/____/____

Spett.le [Nome Cognome]

Oggetto: Conferma limitazione del trattamento dei dati personali - Art. 18 GDPR

Gentile [Sig./Sig.ra] [Cognome],

in riscontro alla Sua richiesta di limitazione del trattamento prot. n. LIM/[ANNO]/[NUMERO] del ____/____/____, Le confermiamo di aver applicato la limitazione del trattamento dei Suoi dati personali.

PRESUPPOSTO DELLA LIMITAZIONE: ☐ Contestazione esattezza dati (in attesa di verifica) ☐ Trattamento illecito con opposizione a cancellazione ☐ Dati non più necessari al Titolare ma necessari a Lei per difesa in giudizio ☐ Opposizione al trattamento (in attesa di verifica)

DATI OGGETTO DI LIMITAZIONE: ☐ Tutti i Suoi dati personali ☐ Solo i seguenti dati:

MODALITÀ DI LIMITAZIONE APPLICATA: I Suoi dati sono stati: ☐ Marcati con indicatore "TRATTAMENTO LIMITATO" nei nostri sistemi ☐ Trasferiti in archivio separato ad accesso ristretto ☐ Bloccati per impedirne l'utilizzo operativo

Data applicazione limitazione: ____/____/____

SISTEMI IN CUI È STATA APPLICATA LA LIMITAZIONE: ☐ Cartella clinica (digitale e cartacea) ☐ Database gestionale ☐ Sistema di marketing/comunicazioni ☐ Altro:

EFFETTI DELLA LIMITAZIONE: I Suoi dati saranno: ✓ CONSERVATI (non cancellati) ✓ NON UTILIZZATI per le normali finalità di trattamento

I Suoi dati potranno essere utilizzati SOLO nei seguenti casi: - Con il Suo consenso esplicito - Per l'accertamento, esercizio o difesa di diritti in sede giudiziaria - Per la tutela dei diritti di un'altra persona fisica o giuridica - Per motivi di interesse pubblico rilevante

DURATA DELLA LIMITAZIONE: ☐ Temporanea - fino a: ____/____/____ Motivo: _____ ☐ Temporanea - fino a conclusione di: _____ ☐ Permanente - fino a Sua diversa richiesta

DESTINATARI INFORMATI: Abbiamo informato i seguenti destinatari della limitazione: ☐ [Nome destinatario 1] ☐ [Nome destinatario 2] ☐ Non applicabile

COMUNICAZIONE PREVENTIVA PRIMA DELLA REVOCA: La informiamo che, qualora venissero meno i presupposti della limitazione, La informeremo PREVENTIVAMENTE prima di revocare la limitazione e ripristinare il normale trattamento dei dati.

SUOI DIRITTI: Lei mantiene tutti gli altri diritti previsti dal GDPR: - Diritto di accesso (art. 15) - Diritto di rettifica (art. 16) - Diritto di cancellazione (art. 17) - Diritto di opposizione (art. 21) - Diritto di reclamo al Garante Privacy

Per qualsiasi chiarimento, restiamo a disposizione.

Cordiali saluti,

Centro Phoenix Srl e Centro Phoenix STP Srl Il Titolare del Trattamento _____
[Firma e timbro]

MODULO 4-C: DINIEGO LIMITAZIONE

[Simile agli altri dinieghi, con motivazioni specifiche]

MODULO 4-D: COMUNICAZIONE LIMITAZIONE AI DESTINATARI

CENTRO PHOENIX SRL E CENTRO PHOENIX STP SRL

Data: ____/____/____

Spett.le [Destinatario]

Oggetto: Comunicazione limitazione del trattamento - Art. 19 GDPR

Egregi Signori,

con la presente Vi comunichiamo che, in seguito a richiesta dell'interessato ai sensi dell'art. 18 GDPR, abbiamo applicato la limitazione del trattamento ai dati personali relativi a:

Interessato: [Nome Cognome] Data di nascita: ____/____/____

Dati oggetto di limitazione: [specificare]

Vi preghiamo di: 1. Prendere atto della limitazione 2. Applicare a Vostra volta la limitazione nei Vostri sistemi 3. NON utilizzare i dati (salvo consenso dell'interessato o altre eccezioni previste dall'art. 18, par. 2 GDPR) 4. Confermare l'avvenuta applicazione della limitazione

La limitazione è stata applicata in data: ____/____/____

Vi informeremo tempestivamente in caso di revoca della limitazione.

Cordiali saluti,

Centro Phoenix Srl e Centro Phoenix STP Srl Il Referente Privacy _____

MODULO 4-E: VERBALE VALUTAZIONE LIMITAZIONE

VERBALE DI VALUTAZIONE - RICHIESTA LIMITAZIONE

Protocollo: LIM/[ANNO]/[NUMERO] Data richiesta: ____/____/____ Interessato: _____
Data valutazione: ____/____/____

Presenti: - Titolare: _____ - Referente Privacy: _____

1. PRESUPPOSTO DELLA RICHIESTA (Art. 18, par. 1): ☐ a) Contestazione esattezza dati ☐ b) Trattamento illecito + opposizione a cancellazione ☐ c) Dati non più necessari ma utili per difesa interessato ☐ d) Opposizione al trattamento (in attesa verifica)
2. VALUTAZIONE: Fondatezza richiesta: ☐ Sì ☐ No ☐ Parzialmente Motivazione: _____

3. DECISIONE: ☐ ACCOLTA ☐ RESPINTA Motivazione: _____

4. SE ACCOLTA - DURATA LIMITAZIONE: ☐ Temporanea - fino a: ____/____/____ o fino a _____
☐ Permanente
5. MODALITÀ APPLICAZIONE: ☐ Marcatura ☐ Segregazione ☐ Blocco funzionale

Il Titolare Il Referente Privacy _____

MODULO 4-F: LOG LIMITAZIONI

REGISTRO LIMITAZIONI TRATTAMENTO

Data	Prot.	Interessato	Presupposto	Dati	Durata	Revoca	Note
(a/b/c/d)		limitati		limitazione		il	
_____	_____	_____	_____	_____	_____	_____	LIM/25/001

MODULO 4-G: COMUNICAZIONE PREVENTIVA REVOCA LIMITAZIONE

CENTRO PHOENIX SRL E CENTRO PHOENIX STP SRL

Data: ____/____/____

Spett.le [Nome Cognome]

Oggetto: Comunicazione preventiva revoca limitazione trattamento - Art. 18 GDPR

Gentile [Sig./Sig.ra] [Cognome],

con la presente La informiamo che, in relazione alla limitazione del trattamento applicata ai Suoi dati personali (prot. LIM/[ANNO]/[NUMERO]), sono venuti meno i presupposti che avevano determinato la limitazione.

MOTIVO DELLA REVOCA: ☐ Conclusa verifica esattezza dati (caso a)) ☐ Conclusa verifica opposizione (caso d)) ☐ Concluso procedimento giudiziario (caso c)) ☐ Su Sua richiesta ☐ Altro:

Pertanto, ai sensi dell'art. 18, paragrafo 3 del GDPR, La informiamo PREVENTIVAMENTE che, decorsi [X] giorni dalla presente comunicazione, procederemo a revocare la limitazione e a ripristinare il normale trattamento dei dati.

Se desidera opporsi alla revoca o ha osservazioni in merito, La preghiamo di contattarci entro il termine sopra indicato.

Cordiali saluti,

Centro Phoenix Srl e Centro Phoenix STP Srl Il Titolare del Trattamento _____

PROCEDURA 5: PORTABILITÀ DEI DATI (Art. 20 GDPR - Diritto alla portabilità)

5.1 FINALITÀ E AMBITO DI APPLICAZIONE

Questa procedura disciplina la gestione delle richieste di portabilità dei dati personali, garantendo il rispetto dell'art. 20 GDPR.

COSA SIGNIFICA "PORTABILITÀ": L'interessato ha diritto di: a) Ricevere i propri dati personali in formato strutturato, di uso comune e leggibile da dispositivo automatico b) Trasmettere tali dati a un altro titolare del trattamento

AMBITO DI APPLICAZIONE - LIMITATO: Il diritto alla portabilità si applica SOLO quando: 1. Il trattamento si basa su: - CONSENSO (art. 6, par. 1, lett. a) o art. 9, par. 2, lett. a)) - CONTRATTO (art. 6, par. 1, lett. b)) E 2. Il trattamento è effettuato con mezzi AUTOMATIZZATI (non cartacei)

IMPORTANTE PER L'AMBITO SANITARIO: Il diritto alla portabilità ha applicazione MOLTO LIMITATA in ambito sanitario perché la maggior parte dei trattamenti NON si basa su consenso o contratto, ma su: - Obbligo di legge (conservazione cartella clinica) - Interesse pubblico in sanità - Interessi vitali

5.2 RESPONSABILITÀ

- REFERENTE PRIVACY: Ricezione e coordinamento
- TITOLARE DEL TRATTAMENTO: Valutazione applicabilità
- PERSONALE TECNICO: Estrazione dati in formato strutturato

5.3 MODALITÀ DI PRESENTAZIONE DELLA RICHIESTA

Identiche a quelle della Procedura 1 (accesso).

5.4 FLUSSO OPERATIVO

FASE 1: RICEZIONE E PROTOCOLLAZIONE (Giorno 0)

- ☐ STEP 1.1 - Ricezione e protocollazione - Assegnare numero protocollo: PORT/[ANNO]/[NUMERO]
- Registrare nel “Registro Richieste Interessati” - Calcolare scadenza: 30 giorni - Inviare ricevuta (Modulo 5-A)

FASE 2: VERIFICA APPLICABILITÀ DEL DIRITTO (Giorni 1-10) *** FASE CRITICA ***

- ☐ STEP 2.1 - Verifica identità - Controllare documento d'identità - Verificare legittimazione
- ☐ STEP 2.2 - Mappatura dei dati richiesti - Identificare i dati personali oggetto della richiesta - Distinguere per finalità di trattamento
- ☐ STEP 2.3 - Verifica presupposti di applicabilità

Per OGNI categoria di dati, verificare:

REQUISITO 1: BASE GIURIDICA DEL TRATTAMENTO

Il trattamento si basa su: ☐ Sì ☐ No CONSENSO (art. 6, par. 1, lett. a) o art. 9, par. 2, lett. a)) ☐ Sì ☐ No CONTRATTO (art. 6, par. 1, lett. b))

Se NO ad entrambi → Portabilità NON applicabile

REQUISITO 2: TRATTAMENTO AUTOMATIZZATO

- ☐ Sì ☐ No I dati sono trattati con mezzi automatizzati (digitali)

Se NO → Portabilità NON applicabile (dati solo cartacei esclusi)

- ☐ STEP 2.4 - Valutazione per categorie di dati

- A) DATI SANITARI (Cartella clinica): Base giuridica: ☐ Obbligo di legge (art. 6, par. 1, lett. c)) ☐ Interesse pubblico in sanità (art. 9, par. 2, lett. h)) → Portabilità NON applicabile

ALTERNATIVA: Fornire copia tramite diritto di accesso (Procedura 1)

- B) DATI AMMINISTRATIVI/CONTABILI: Base giuridica: ☐ Obbligo di legge ☐ Contratto → Se contratto: Portabilità applicabile → Se obbligo legale: Portabilità NON applicabile

- C) DATI PER RICERCA SCIENTIFICA: Base giuridica: ☐ Consenso → Portabilità applicabile (se dati in formato digitale)

- D) DATI PER MARKETING: Base giuridica: ☐ Consenso → Portabilità applicabile

- ☐ STEP 2.5 - Decisione preliminare

Determinare: ☐ Portabilità applicabile a tutti i dati richiesti ☐ Portabilità applicabile solo ad alcuni dati ☐ Portabilità NON applicabile

Se NON applicabile → Predisporre diniego motivato (Modulo 5-D)

Se applicabile → Procedere con estrazione

FASE 3: ESTRAZIONE DATI IN FORMATO STRUTTURATO (Giorni 11-20)

- ☐ STEP 3.1 - Determinazione formato

Richiedere all'interessato (se non già specificato): ☐ Formato preferito per la fornitura dei dati

Formati comunemente usati: ☐ CSV (Comma-Separated Values) ☐ JSON (JavaScript Object Notation)
☐ XML (eXtensible Markup Language) ☐ PDF strutturato ☐ Excel (XLSX)

Caratteristiche richieste: - Formato STRUTTURATO (non semplice immagine o PDF scansionato) - Di uso COMUNE - Leggibile da DISPOSITIVO AUTOMATICO - INTEROPERABILE (utilizzabile da altri sistemi)

☐ STEP 3.2 - Estrazione dei dati

Per OGNI categoria di dati portabili:

☐ Estrarre dal database/sistema informatico ☐ Organizzare in formato strutturato ☐ Includere: * Tutti i dati personali forniti dall'interessato * Dati generati dall'interessato (es. risposte a questionari) * ESCLUDERE: dati inferiti/derivati (es. valutazioni cliniche elaborate)

☐ Verificare completezza ed accuratezza

☐ STEP 3.3 - Preparazione file

☐ Creare file nel formato concordato ☐ Strutturare con campi chiaramente identificabili ☐ Includere legenda/documentazione se necessario ☐ Verificare leggibilità del file

☐ STEP 3.4 - Esclusione dati di terzi

☐ Verificare che il file NON contenga dati personali di terzi ☐ Se presenti: rimuovere o anonimizzare

FASE 4: TRASMISSIONE DATI (Giorni 21-28)

☐ STEP 4.1 - Modalità di trasmissione

OPZIONE A: FORNITURA DIRETTA ALL'INTERESSATO

Modalità sicure: ☐ Download da area riservata protetta da password ☐ Invio via email crittografata ☐
Supporto fisico (USB) consegnato a mano ☐ Altro:

OPZIONE B: TRASMISSIONE DIRETTA A ALTRO TITOLARE

Solo se: ☐ L'interessato lo richiede espressamente ☐ Tecnicamente fattibile ☐ Il nuovo titolare è identificato e accetta la ricezione

Procedura: ☐ Verificare identità del nuovo titolare ☐ Stabilire modalità tecniche di trasmissione ☐
Trasmettere i dati in modo sicuro ☐ Richiedere conferma di ricezione ☐ Documentare la trasmissione

☐ STEP 4.2 - Sicurezza della trasmissione

☐ Utilizzare sempre canali sicuri e crittografati ☐ Se file di grandi dimensioni: utilizzare servizi di file transfer sicuri ☐ Proteggere il file con password (comunicare password separatamente) ☐ Tracciare l'invio/consegna

☐ STEP 4.3 - Documentazione

- Documentare modalità e data di trasmissione □ Conservare ricevuta di consegna/conferma ricezione □ Aggiornare registro

FASE 5: RISPOSTA ALL'INTERESSATO (Giorni 27-30)

- STEP 5.1 - Predisposizione risposta - Se applicabile: Modulo 5-B (Fornitura dati portabili) - Se non applicabile: Modulo 5-D (Diniego portabilità)
- STEP 5.2 - Invio risposta - Allegare file con i dati (o fornire istruzioni per download) - Fornire documentazione sul formato utilizzato - Archiviare

5.5 LIMITAZIONI E PRECISAZIONI

A) DATI FORNITI vs DATI GENERATI DAL TITOLARE

PORTABILI:

- Dati forniti attivamente dall'interessato
- Dati generati dall'interessato

NON PORTABILI:

- Dati inferiti o derivati dal Titolare
- Elaborazioni e valutazioni del professionista Esempio: in psicologia, le diagnosi e le valutazioni cliniche elaborate dallo psicologo NON sono portabili, ma sono accessibili tramite diritto di accesso.

B) DIRITTI DI TERZI

La portabilità NON deve ledere diritti e libertà di terzi:

- Segreto professionale di altri professionisti
- Diritti di proprietà intellettuale
- Dati personali di altri pazienti/persone

C) GRATUITÀ

La prima copia è GRATUITA Copie ulteriori: possibile contributo per costi amministrativi

D) DIFFERENZA CON DIRITTO DI ACCESSO

PORTABILITÀ (Art. 20):

- Solo dati basati su consenso/contratto
- Solo dati automatizzati
- Formato strutturato e interoperabile
- Possibile trasmissione diretta a altro titolare

ACCESSO (Art. 15):

- Tutti i dati, qualunque sia la base giuridica
- Anche dati cartacei
- Formato leggibile (anche PDF)
- Fornitura solo all'interessato

5.6 CASI PRATICI - AMBITO PSICOLOGICO

CASO 1: Paziente chiede portabilità cartella clinica per trasferirsi a altro psicologo

VALUTAZIONE: - Base giuridica trattamento dati clinici: interesse pubblico in sanità, NON consenso
- Portabilità NON applicabile

SOLUZIONE: - Diniego portabilità (Modulo 5-D) - ALTERNATIVA: Fornire copia cartella clinica tramite diritto di accesso (Procedura 1) - Formato: PDF o copia cartacea (sufficiente per trasferimento cure)

CASO 2: Paziente che aveva dato consenso per ricerca scientifica chiede portabilità dati di ricerca

VALUTAZIONE: - Base giuridica: consenso - Dati digitalizzati - Portabilità applicabile

SOLUZIONE: - Estrarre dati di ricerca (questionari, test, risposte) - Fornire in formato CSV o JSON - Escludere elaborazioni/valutazioni dei ricercatori

CASO 3: Paziente chiede portabilità dati anagrafici e di contatto

VALUTAZIONE: - Base giuridica: contratto o consenso (a seconda del caso) - Dati digitalizzati - Portabilità applicabile

SOLUZIONE: - Estrarre dati anagrafici e contatti dal database - Fornire in formato CSV o JSON - Trasmettere in modo sicuro

5.7 MODULISTICA

MODULO 5-A: RICEVUTA RICEZIONE RICHIESTA PORTABILITÀ

[Simile ai precedenti]

MODULO 5-B: FORNITURA DATI PORTABILI

CENTRO PHOENIX SRL E CENTRO PHOENIX STP SRL

Protocollo n. PORT/[ANNO]/[NUMERO] Data: ____/____/____

Spett.le [Nome Cognome]

Oggetto: Fornitura dati in formato portabile - Art. 20 GDPR

Gentile [Sig./Sig.ra] [Cognome],

in riscontro alla Sua richiesta di portabilità dei dati prot. n. PORT/[ANNO]/[NUMERO] del ____/____/____, Le forniamo i Suoi dati personali in formato strutturato, di uso comune e leggibile da dispositivo automatico.

DATI FORNITI: Abbiamo incluso i seguenti dati personali: ☐ Dati anagrafici e di contatto ☐ Dati relativi a [specificare finalità basata su consenso/contratto] ☐ Altro:

FORMATO DEI DATI: ☐ CSV (Comma-Separated Values) ☐ JSON (JavaScript Object Notation) ☐ XML (eXtensible Markup Language) ☐ Excel (XLSX) ☐ Altro:

MODALITÀ DI FORNITURA: ☐ File allegato alla presente (protetto da password) Password: [comunicata separatamente] ☐ Download da area riservata: [link e credenziali] ☐ Supporto fisico (USB) consegnato a mano ☐ Trasmissione diretta a: [altro titolare] - [conferma trasmissione]

CONTENUTO DEL FILE: Il file contiene i seguenti campi/informazioni: [Elenco dei campi o allegare legenda]

ISTRUZIONI PER L'USO: [Fornire istruzioni per aprire/utilizzare il file, se necessario]

DATI NON INCLUSI: I seguenti dati NON sono inclusi nel file in quanto non rientrano nell'ambito del diritto alla portabilità (art. 20 GDPR):

☐ Dati sanitari (cartella clinica) - Base giuridica: interesse pubblico in sanità, non consenso → Disponibili tramite diritto di accesso (art. 15 GDPR)

☐ Dati amministrativi/contabili - Base giuridica: obbligo di legge → Disponibili tramite diritto di accesso (art. 15 GDPR)

☐ Valutazioni e diagnosi elaborate dal professionista (dati inferiti)

☐ Altro: _____

TRASMISSIONE A ALTRO TITOLARE: ☐ NON richiesta ☐ Effettuata in data ____/____/____ a: [nome titolare]

RACCOMANDAZIONI: - Conservare i dati in modo sicuro - Non condividere la password con terzi - Verificare l'integrità del file dopo il download

Per qualsiasi difficoltà tecnica o chiarimento, restiamo a disposizione.

Cordiali saluti,

Centro Phoenix Srl e Centro Phoenix STP Srl Il Titolare del Trattamento _____
[Firma e timbro]

MODULO 5-C: RICHIESTA SPECIFICAZIONI

CENTRO PHOENIX SRL E CENTRO PHOENIX STP SRL

Protocollo n. PORT/[ANNO]/[NUMERO] Data: ____/____/____

Spett.le [Nome Cognome]

Oggetto: Richiesta specificazioni - Portabilità dati

Gentile [Sig./Sig.ra] [Cognome],

in relazione alla Sua richiesta di portabilità dei dati prot. n. PORT/[ANNO]/[NUMERO], per poterLe fornire i dati nel formato più adeguato alle Sue esigenze, Le chiediamo cortesemente di specificare:

- ☐ Formato preferito: ☐ CSV ☐ JSON ☐ XML ☐ Excel ☐ Altro: _____
- ☐ Modalità di trasmissione preferita: ☐ Email ☐ Download da area riservata ☐ Supporto fisico ☐ Altro: _____
- ☐ Trasmissione diretta a altro titolare: ☐ No, desidero ricevere io i dati ☐ Sì, trasmettere a: Nome titolare: _____ Contatto: _____

La preghiamo di fornire le specificazioni entro 7 giorni.

Cordiali saluti, Il Referente Privacy _____

MODULO 5-D: DINIEGO PORTABILITÀ

CENTRO PHOENIX SRL E CENTRO PHOENIX STP SRL

Protocollo n. PORT/[ANNO]/[NUMERO] Data: ____/____/____

Spett.le [Nome Cognome]

Oggetto: Diniego richiesta di portabilità dati - Art. 20 GDPR

Gentile [Sig./Sig.ra] [Cognome],

in relazione alla Sua richiesta di portabilità dei dati prot. n. PORT/[ANNO]/[NUMERO] del ____/____/____, dopo attenta valutazione, siamo spiacenti di informarLa che il diritto alla portabilità NON è applicabile ai dati richiesti.

MOTIVAZIONI:

Il diritto alla portabilità (art. 20 GDPR) si applica SOLO quando il trattamento: a) Si basa su CONSENSO o CONTRATTO, E b) È effettuato con mezzi AUTOMATIZZATI

Nel Suo caso:

☐ DATI SANITARI (Cartella clinica)

Base giuridica del trattamento: ☒ Interesse pubblico nel settore della sanità pubblica (art. 9, par. 2, lett. h) GDPR) ☒ Obbligo di legge (conservazione cartella clinica) ☐ NON consenso

Conclusione: Il diritto alla portabilità NON si applica ai dati sanitari.

ALTERNATIVA DISPONIBILE: Lei può esercitare il DIRITTO DI ACCESSO (art. 15 GDPR) per ottenere copia della Sua cartella clinica in formato leggibile (PDF o cartaceo).

Se desidera trasferire le Sue cure a un altro professionista, saremo lieti di fornirLe copia completa della documentazione clinica tramite il diritto di accesso.

☐ DATI AMMINISTRATIVI/CONTABILI

Base giuridica del trattamento: ☒ Obbligo di legge (adempimenti fiscali e contabili) ☐ NON consenso o contratto

Conclusione: Il diritto alla portabilità NON si applica.

□ ALTRO: _____

DIRITTI ALTERNATIVI CHE PUÒ ESERCITARE:

✓ DIRITTO DI ACCESSO (Art. 15 GDPR) Può ottenere copia di tutti i Suoi dati personali, inclusa la cartella clinica, in formato leggibile.

✓ DIRITTO DI RETTIFICA (Art. 16 GDPR) Può richiedere la correzione di dati inesatti.

✓ DIRITTO DI CANCELLAZIONE (Art. 17 GDPR) Può richiedere la cancellazione dei dati (nei limiti previsti dalla legge).

COME PROCEDERE:

Se desidera esercitare il diritto di accesso per ottenere copia della Sua cartella clinica o di altri dati, La invitiamo a presentare apposita richiesta che evaderemo entro 30 giorni.

DIRITTO DI RECLAMO:

La informiamo che Lei ha il diritto di proporre reclamo all'Autorità Garante per la Protezione dei Dati Personali (www.garanteprivacy.it).

Restiamo a disposizione per ogni chiarimento.

Cordiali saluti,

Centro Phoenix Srl e Centro Phoenix STP Srl Il Titolare del Trattamento _____
[Firma e timbro]

PROCEDURA 6: OPPOSIZIONE AL TRATTAMENTO (Art. 21 GDPR - Diritto di opposizione)

6.1 FINALITÀ E AMBITO DI APPLICAZIONE

Questa procedura disciplina la gestione delle richieste di opposizione al trattamento dei dati personali, garantendo il rispetto dell'art. 21 GDPR.

L'interessato ha diritto di opporsi al trattamento dei propri dati personali quando: - Il trattamento si basa su INTERESSE LEGITTIMO del titolare (art. 6, par. 1, lett. f)) - Il trattamento si basa su COMPITO DI INTERESSE PUBBLICO o ESERCIZIO DI PUBBLICI POTERI (art. 6, par. 1, lett. e)) - Il trattamento è per MARKETING DIRETTO

OPPOSIZIONE RELATIVA vs ASSOLUTA:

OPPOSIZIONE RELATIVA (art. 21, par. 1): - L'interessato può opporsi per motivi connessi alla sua situazione particolare - Il Titolare può continuare il trattamento se dimostra motivi legittimi cogenti - Valutazione caso per caso

OPPOSIZIONE ASSOLUTA (art. 21, par. 2): - Opposizione al marketing diretto - Il Titolare DEVE cessare il trattamento - Nessuna possibilità di bilanciamento

6.2 APPLICABILITÀ IN AMBITO SANITARIO

IN AMBITO PSICOLOGICO-SANITARIO, il diritto di opposizione ha applicazione MOLTO LIMITATA perché:

- I dati sanitari sono trattati per INTERESSE PUBBLICO IN SANITÀ (art. 9, par. 2, lett. h)), NON per interesse legittimo
- Il trattamento è necessario per l'erogazione delle prestazioni sanitarie
- Non è possibile opporsi al trattamento necessario per la cura

DOVE SI APPLICA: - Marketing e comunicazioni promozionali (opposizione assoluta) - Ricerca scientifica in casi particolari (valutazione caso per caso) - Eventuali altri trattamenti non strettamente necessari per la cura

6.3 RESPONSABILITÀ

- REFERENTE PRIVACY: Ricezione e coordinamento
- TITOLARE DEL TRATTAMENTO: Valutazione e decisione (sempre coinvolto)
- PERSONALE AUTORIZZATO: Esecuzione cessazione trattamento

6.4 FLUSSO OPERATIVO

FASE 1: RICEZIONE E PROTOCOLLAZIONE (Giorno 0)

□ STEP 1.1 - Ricezione e protocollazione - Assegnare numero protocollo: OPP/[ANNO]/[NUMERO] - Registrare nel "Registro Richieste Interessati" - Calcolare scadenza: 30 giorni (ma opposizione marketing: immediata) - Inviare ricevuta (Modulo 6-A) - ALERT al Titolare (richiesta delicata)

FASE 2: VERIFICA IDENTITÀ E CLASSIFICAZIONE (Giorni 1-5)

□ STEP 2.1 - Verifica identità - Controllare documento d'identità - Verificare legittimazione

□ STEP 2.2 - Classificazione tipo di opposizione

Identificare a cosa l'interessato si oppone:

□ TIPO A: OPPOSIZIONE A MARKETING DIRETTO (Art. 21, par. 2) → Opposizione ASSOLUTA → ACCOGLIMENTO IMMEDIATO OBBLIGATORIO → Procedere con Fase 3-A

□ TIPO B: OPPOSIZIONE A TRATTAMENTO BASATO SU INTERESSE LEGITTIMO (Art. 21, par. 1) → Opposizione RELATIVA → Necessaria valutazione bilanciamento interessi → Procedere con Fase 3-B

□ TIPO C: OPPOSIZIONE A TRATTAMENTO PER INTERESSE PUBBLICO → Opposizione RELATIVA → Necessaria valutazione motivi legittimi cogenti → Procedere con Fase 3-B

FASE 3-A: GESTIONE OPPOSIZIONE AL MARKETING (immediata)

□ STEP 3-A.1 - Accoglimento immediato

L'opposizione al marketing è un diritto ASSOLUTO. Il Titolare NON può rifiutare o bilanciare interessi.

AZIONI IMMEDIATE (entro 24-48 ore):

- ☐ Rimuovere l'interessato da tutte le liste di marketing: - Newsletter via email - SMS promozionali - Chiamate telefoniche - Invii postali - Qualsiasi altra comunicazione promozionale
- ☐ Annotare l'opposizione nei sistemi: - Database: flag "OPT-OUT MARKETING" - Note: "Opposizione marketing prot. OPP/[ANNO]/[NUMERO] del [DATA]"
- ☐ Garantire che l'interessato NON riceva più comunicazioni marketing
- ☐ STEP 3-A.2 - Conferma immediata all'interessato - Inviare conferma entro 48 ore (Modulo 6-B) - Non attendere i 30 giorni
- ☐ STEP 3-A.3 - Comunicazione ai responsabili - Informare eventuali responsabili del trattamento che gestiscono marketing - Richiedere cessazione immediata
- ☐ STEP 3-A.4 - Documentazione - Registrare nel Log opposizioni (Modulo 6-F) - Chiudere la pratica

FASE 3-B: GESTIONE OPPOSIZIONE RELATIVA (Giorni 6-25) *** PER OPPOSIZIONI BASATE SU INTERESSE LEGITTIMO O INTERESSE PUBBLICO ***

- ☐ STEP 3-B.1 - Identificazione del trattamento oggetto di opposizione

Identificare con precisione: - Quale trattamento è oggetto di opposizione - Quale base giuridica (interesse legittimo o interesse pubblico) - Quali dati sono coinvolti - Quali finalità

- ☐ STEP 3-B.2 - Verifica base giuridica

IMPORTANTE: L'opposizione si applica SOLO se il trattamento si basa su: - Interesse legittimo del titolare (art. 6, par. 1, lett. f)), OPPURE - Compito di interesse pubblico (art. 6, par. 1, lett. e))

SE il trattamento si basa su: - Consenso → Non è opposizione ma REVOCA DEL CONSENSO (gestire di conseguenza) - Contratto → Non applicabile (trattamento necessario per esecuzione contratto) - Obbligo di legge → Non applicabile (trattamento obbligatorio per legge) - Interessi vitali → Non applicabile (trattamento necessario per salvare vite)

IN AMBITO SANITARIO: - Dati sanitari per cure: interesse pubblico in sanità → RARAMENTE applicabile l'opposizione (trattamento necessario) - Dati per ricerca: potenzialmente applicabile (valutare caso per caso)

- ☐ STEP 3-B.3 - Analisi dei motivi dell'interessato

L'interessato deve indicare i motivi dell'opposizione connessi alla sua situazione particolare.

- ☐ Verificare se l'interessato ha indicato motivazioni specifiche ☐ Se mancano: richiedere chiarimenti (Modulo 6-C) ☐ Valutare la serietà e rilevanza dei motivi addotti

- ☐ STEP 3-B.4 - Bilanciamento degli interessi

PRINCIPIO: Il Titolare può continuare il trattamento SOLO se dimostra l'esistenza di motivi legittimi COGENTI che prevalgono sugli interessi, diritti e libertà dell'interessato.

VALUTAZIONE (con il Titolare):

A) MOTIVI DEL TITOLARE PER CONTINUARE IL TRATTAMENTO:

- ☐ Necessità per l'erogazione delle prestazioni sanitarie (se applicabile: prevale quasi sempre)
- ☐ Adempimento obblighi di legge/regolamentari (se applicabile: prevale)
- ☐ Tutela di interessi vitali dell'interessato o di terzi (se applicabile: prevale)
- ☐ Accertamento, esercizio o difesa di diritti in sede giudiziaria (es. potenziale contenzioso con il paziente) (se applicabile: prevale)
- ☐ Interesse legittimo rilevante del Titolare (valutare rilevanza e cogenza)
- ☐ Altro: _____

B) MOTIVI DELL'INTERESSATO PER OPPORSI:

[Riportare i motivi indicati dall'interessato]

C) BILANCIAMENTO:

I motivi del Titolare sono COGENTI e prevalgono? ☐ SÌ → Diniego opposizione (Modulo 6-E)
Motivazione: _____

- ☐ NO → Accoglimento opposizione (Modulo 6-D) Il trattamento deve cessare

☐ STEP 3-B.5 - Verbale di valutazione - Documentare la valutazione (Modulo 6-G) - Raccogliere firma del Titolare - Conservare agli atti

FASE 4: ESECUZIONE CESSAZIONE TRATTAMENTO (Se opposizione accolta)

- ☐ STEP 4.1 - Identificazione azioni necessarie

Determinare cosa significa "cessare il trattamento" nel caso specifico:

- ☐ Cessare utilizzo per specifiche finalità (es. ricerca) ☐ Applicare limitazione del trattamento (vedi Procedura 4) ☐ Cancellare i dati (se non vi sono obblighi di conservazione) (vedi Procedura 3) ☐ Altro: _____

- ☐ STEP 4.2 - Implementazione

☐ Aggiornare i sistemi informatici ☐ Annotare l'opposizione negli archivi cartacei ☐ Informare il personale autorizzato ☐ Applicare blocchi/limitazioni tecniche ☐ Documentare le azioni intraprese

☐ STEP 4.3 - Comunicazione ai destinatari - Informare eventuali destinatari/responsabili - Richiedere cessazione del trattamento - Documentare

FASE 5: RISPOSTA ALL'INTERESSATO (Giorni 26-30)

☐ STEP 5.1 - Predisposizione risposta - Se marketing: Modulo 6-B (conferma immediata) - Se opposizione relativa accolta: Modulo 6-D - Se opposizione relativa respinta: Modulo 6-E

☐ STEP 5.2 - Invio risposta - Inviare entro termine - Motivare adeguatamente (specie se diniego) - Archiviare

6.5 CASI PARTICOLARI - AMBITO PSICOLOGICO

CASO 1: Paziente si oppone al trattamento dei dati sanitari per finalità di cura

VALUTAZIONE: - Base giuridica: interesse pubblico in sanità - Trattamento necessario per erogazione prestazioni - Opposizione: difficilmente accoglibile

RISPOSTA: - Spiegare che il trattamento è necessario per la cura - Se il paziente non vuole che i suoi dati siano trattati, non è possibile proseguire il rapporto terapeutico - DINIEGO OPPOSIZIONE (ma proporre conclusione rapporto se paziente insiste)

CASO 2: Paziente si oppone all'utilizzo dei dati per ricerca scientifica

VALUTAZIONE: - Se ricerca basata su consenso: è REVOCA DEL CONSENSO, non opposizione - Se ricerca basata su interesse pubblico: possibile opposizione - Bilanciare: interesse della ricerca vs. diritti del paziente

RISPOSTA: - Valutare se la ricerca può proseguire senza i dati del paziente - Se possibile: ACCOGLIERE opposizione - Anonimizzare i dati se già inclusi in dataset - Se impossibile: valutare diniego motivato

CASO 3: Paziente si oppone a invio newsletter/comunicazioni promozionali

VALUTAZIONE: - Marketing diretto - Opposizione ASSOLUTA

RISPOSTA: - ACCOGLIMENTO IMMEDIATO - Rimuovere da liste marketing - Confermare entro 48 ore

6.6 MODULISTICA

MODULO 6-A: RICEVUTA RICEZIONE OPPOSIZIONE

[Simile ai precedenti]

MODULO 6-B: CONFERMA OPPOSIZIONE MARKETING (immediata)

CENTRO PHOENIX SRL E CENTRO PHOENIX STP SRL

Protocollo n. OPP/[ANNO]/[NUMERO] Data: ____/____/____

Spett.le [Nome Cognome]

Oggetto: Conferma opposizione al trattamento per marketing diretto - Art. 21 GDPR

Gentile [Sig./Sig.ra] [Cognome],

confermiamo di aver ricevuto la Sua opposizione al trattamento dei dati personali per finalità di marketing diretto.

Abbiamo provveduto IMMEDIATAMENTE a: ☐ Rimuovere il Suo indirizzo email dalle liste per l'invio di newsletter ☐ Rimuovere il Suo numero di telefono dalle liste per comunicazioni promozionali ☐

Annotare la Sua opposizione nei nostri sistemi ☐ Altro:

NON riceverà più comunicazioni promozionali da parte nostra.

NOTA IMPORTANTE: Continuerà a ricevere comunicazioni relative al servizio (es. conferme di appuntamento, fatture, comunicazioni necessarie per l'erogazione delle prestazioni), in quanto tali comunicazioni NON sono marketing ma sono necessarie per la gestione del rapporto.

Cordiali saluti,

Centro Phoenix Srl e Centro Phoenix STP Srl Il Referente Privacy _____

MODULO 6-C: RICHIESTA CHIARIMENTI MOTIVAZIONI

CENTRO PHOENIX SRL E CENTRO PHOENIX STP SRL

Protocollo n. OPP/[ANNO]/[NUMERO] Data: ____/____/____

Spett.le [Nome Cognome]

Oggetto: Richiesta chiarimenti - Opposizione al trattamento

Gentile [Sig./Sig.ra] [Cognome],

in relazione alla Sua richiesta di opposizione al trattamento prot. n. OPP/[ANNO]/[NUMERO], per poter valutare adeguatamente la richiesta, Le chiediamo cortesemente di specificare:

☐ I motivi specifici connessi alla Sua situazione particolare che giustificano l'opposizione ☐ Quali dati/trattamenti specifici sono oggetto dell'opposizione ☐ Altro:

Il diritto di opposizione (art. 21 GDPR) richiede che Lei indichi i motivi della Sua richiesta connessi alla Sua situazione particolare, in modo da consentirci di effettuare il bilanciamento degli interessi.

La preghiamo di fornire i chiarimenti entro 7 giorni.

Cordiali saluti, Il Referente Privacy _____

MODULO 6-D: ACCOGLIMENTO OPPOSIZIONE

CENTRO PHOENIX SRL E CENTRO PHOENIX STP SRL

Protocollo n. OPP/[ANNO]/[NUMERO] Data: ____/____/____

Spett.le [Nome Cognome]

Oggetto: Accoglimento opposizione al trattamento - Art. 21 GDPR

Gentile [Sig./Sig.ra] [Cognome],

in riscontro alla Sua richiesta di opposizione al trattamento prot. n. OPP/[ANNO]/[NUMERO] del ____/____/____, dopo attenta valutazione, Le confermiamo di aver accolto la Sua richiesta.

TRATTAMENTO OGGETTO DI OPPOSIZIONE: [Specificare quale trattamento/finalità]

MOTIVI DELL'ACCOGLIMENTO: Dopo aver bilanciato i Suoi diritti e interessi con i nostri motivi legittimi, abbiamo ritenuto di accogliere la Sua opposizione per i seguenti motivi:

AZIONI INTRAPRESE: Abbiamo provveduto a: ☐ Cessare il trattamento per la finalità di: _____ ☐ Applicare limitazione del trattamento (i dati sono conservati ma non utilizzati) ☐ Cancellare i dati (se non sussistono obblighi di conservazione) ☐ Altro:

Data cessazione trattamento: ____/____/____

DATI CONSERVATI: I seguenti dati sono comunque conservati per altre finalità con diversa base giuridica: ☐ Dati sanitari per finalità di cura (interesse pubblico in sanità) ☐ Dati amministrativi per obblighi di legge ☐ Altro:

DESTINATARI INFORMATI: Abbiamo informato i seguenti destinatari della cessazione del trattamento: [Elenco se applicabile]

Cordiali saluti,

Centro Phoenix Srl e Centro Phoenix STP Srl Il Titolare del Trattamento _____
[Firma e timbro]

MODULO 6-E: DINIEGO OPPOSIZIONE

CENTRO PHOENIX SRL E CENTRO PHOENIX STP SRL

Protocollo n. OPP/[ANNO]/[NUMERO] Data: ____/____/____

Spett.le [Nome Cognome]

Oggetto: Diniego opposizione al trattamento - Art. 21 GDPR

Gentile [Sig./Sig.ra] [Cognome],

in relazione alla Sua richiesta di opposizione al trattamento prot. n. OPP/[ANNO]/[NUMERO] del ____/____/____, dopo attenta valutazione e bilanciamento degli interessi, siamo spiacenti di informarLa che non è possibile accogliere la Sua opposizione.

MOTIVAZIONI DEL DINIEGO:

Ai sensi dell'art. 21, paragrafo 1 del GDPR, il Titolare può continuare il trattamento se dimostra l'esistenza di motivi legittimi COGENTI per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato.

Nel Suo caso, sussistono i seguenti motivi legittimi cogenti:

☐ NECESSITÀ PER L'EROGAZIONE DELLE PRESTAZIONI SANITARIE

Il trattamento dei Suoi dati sanitari è necessario per: - Erogare le prestazioni psicologiche richieste - Garantire la continuità assistenziale - Adempiere agli obblighi professionali

Base giuridica: Interesse pubblico nel settore della sanità pubblica (art. 9, par. 2, lett. h) GDPR)

Il trattamento è quindi necessario e non può essere interrotto senza compromettere l'erogazione delle prestazioni.

Motivazione: La cartella clinica e la documentazione sanitaria sono indispensabili per garantire la qualità e la sicurezza delle cure. L'opposizione al loro trattamento renderebbe impossibile proseguire il rapporto terapeutico.

☐ ADEMPIMENTO OBBLIGHI DI LEGGE

Il trattamento è necessario per adempiere obblighi di legge: - Conservazione documentazione sanitaria (Codice Deontologico Psicologi) - Obblighi fiscali e contabili - [Altri obblighi]

Motivazione: _____

☐ ACCERTAMENTO, ESERCIZIO O DIFESA DI DIRITTI IN SEDE GIUDIZIARIA

Il trattamento è necessario per la tutela dei diritti del Centro in caso di contenzioso.

Motivazione: _____

☐ ALTRO

Motivazione: _____

BILANCIAMENTO DEGLI INTERESSI:

Abbiamo attentamente valutato i motivi da Lei addotti per l'opposizione: [Riportare motivi dell'interessato]

Tuttavia, riteniamo che i motivi legittimi del Titolare sopra esposti siano COGENTI e prevalgano sui Suoi interessi, in quanto:

ALTERNATIVE:

Se non desidera che i Suoi dati siano ulteriormente trattati, Le suggeriamo le seguenti alternative: ☐ Conclusione del rapporto terapeutico (con conservazione dati per obblighi legali) ☐ Limitazione del trattamento (art. 18 GDPR) - i dati sono conservati ma non utilizzati ☐ Altro:

DIRITTO DI RECLAMO:

La informiamo che Lei ha il diritto di proporre reclamo all'Autorità Garante per la Protezione dei Dati Personali (www.garanteprivacy.it).

Può inoltre proporre ricorso giurisdizionale.

Restiamo a disposizione per ogni chiarimento.

Cordiali saluti,

Centro Phoenix Srl e Centro Phoenix STP Srl Il Titolare del Trattamento _____
[Firma e timbro]

MODULO 6-F: LOG OPPOSIZIONI

REGISTRO OPPOSIZIONI AL TRATTAMENTO

Data	Prot.	Interessato	Tipo	Trattamento	Esito	Data	Note
opposizione		oggetto		cessazione			
_____	_____	_____	_____	_____	_____	OPP/25/001	☐
Marketing	☐ Accolto	☐ Relativa	☐ Respinto				

MODULO 6-G: VERBALE VALUTAZIONE OPPOSIZIONE

VERBALE DI VALUTAZIONE - OPPOSIZIONE AL TRATTAMENTO

Protocollo: OPP/[ANNO]/[NUMERO] Data richiesta: ____/____/____ Interessato: _____
Data valutazione: ____/____/____

Presenti: - Titolare: _____ - Referente Privacy: _____

1. TIPO DI OPPOSIZIONE: ☐ Marketing diretto (art. 21, par. 2) → Accoglimento automatico ☐ Opposizione relativa (art. 21, par. 1) → Valutazione necessaria

2. TRATTAMENTO OGGETTO DI OPPOSIZIONE: Finalità: _____
giuridica: _____ Base
coinvolti: _____ Dati

3. MOTIVI DELL'INTERESSATO: _____

4. MOTIVI LEGITTIMI COGENTI DEL TITOLARE: ☐ Sì ☐ No Necessità per erogazione prestazioni sanitarie ☐ Sì ☐ No Adempimento obblighi di legge ☐ Sì ☐ No Accertamento/difesa diritti in giudizio ☐ Sì ☐ No Altro: _____

Dettaglio: _____

5. BILANCIAMENTO: I motivi del Titolare sono COGENTI e prevalgono? ☐ SÌ → Diniego opposizione ☐ NO → Accoglimento opposizione

Motivazione del bilanciamento: _____

6. DECISIONE: ☐ ACCOLTA ☐ RESPINTA

Azioni

da

intraprendere:

Il Titolare Il Referente Privacy _____

PROCEDURA 7: GESTIONE DATA BREACH (VIOLAZIONE DATI PERSONALI) (Art. 33-34 GDPR - Notifica violazione e comunicazione all'interessato)

7.1 FINALITÀ E AMBITO DI APPLICAZIONE

Questa procedura disciplina la gestione delle violazioni di dati personali (data breach), garantendo il rispetto degli artt. 33 e 34 del GDPR.

DEFINIZIONE DI DATA BREACH: Violazione di sicurezza che comporta accidentalmente o in modo illecito: - La DISTRUZIONE dei dati - La PERDITA dei dati - La MODIFICA non autorizzata dei dati - La DIVULGAZIONE non autorizzata dei dati - L'ACCESSO non autorizzato ai dati

TIPOLOGIE DI VIOLAZIONE: 1. VIOLAZIONE DELLA RISERVATEZZA: accesso/divulgazione non autorizzati 2. VIOLAZIONE DELL'INTEGRITÀ: modifica/alterazione non autorizzata 3. VIOLAZIONE DELLA DISPONIBILITÀ: perdita/distruzione/impossibilità di accesso

OBBLIGHI TEMPORALI CRITICI: - NOTIFICA AL GARANTE: entro 72 ORE dalla scoperta della violazione (se rischio per diritti e libertà) - COMUNICAZIONE AGLI INTERESSATI: senza ingiustificato ritardo (se rischio ELEVATO per diritti e libertà)

7.2 RESPONSABILITÀ

- REFERENTE DATA BREACH: Primo punto di contatto, coordinamento
- TITOLARE DEL TRATTAMENTO: Decisione finale su notifica/comunicazione
- TUTTO IL PERSONALE: Obbligo di segnalare tempestivamente ogni sospetta violazione

7.3 ESEMPI DI DATA BREACH IN AMBITO PSICOLOGICO

VIOLAZIONI DELLA RISERVATEZZA: - Email con dati clinici inviata a destinatario sbagliato - Cartelle cliniche lasciate incustodite e visualizzate da persone non autorizzate - Accesso non autorizzato al sistema gestionale pazienti - Furto di laptop contenente dati non crittografati - Smarrimento di chiavetta USB con cartelle cliniche - Attacco hacker con esfiltrazione di dati - Invio di newsletter con indirizzi email in chiaro (tutti visibili)

VIOLAZIONI DELL'INTEGRITÀ: - Modifica non autorizzata di cartelle cliniche - Alterazione di dati anagrafici nel database - Ransomware che cripta e/o modifica i file

VIOLAZIONI DELLA DISPONIBILITÀ: - Cancellazione accidentale di database pazienti senza backup - Ransomware che rende inaccessibili i dati - Guasto server con perdita dati - Distruzione di archivio cartaceo per incendio/allagamento - Cancellazione involontaria di email con dati clinici

7.4 FLUSSO OPERATIVO

FASE 1: RILEVAMENTO E SEGNALAZIONE IMMEDIATA (Ora 0)

☐ STEP 1.1 - Rilevamento della violazione

La violazione può essere rilevata da: ☐ Personale interno ☐ Sistema automatico di allarme ☐ Segnalazione di un paziente ☐ Responsabile del trattamento esterno (es. fornitore IT) ☐ Autorità (es. Polizia Postale) ☐ Altro: _____

☐ STEP 1.2 - Segnalazione immediata

CHIUNQUE rilevi una violazione o una sospetta violazione DEVE: ☐ Segnalare IMMEDIATAMENTE al Referente Data Breach ☐ Utilizzare il “Modulo di Segnalazione Iniziale” (Modulo 7-A) ☐ Fornire tutte le informazioni disponibili: - Data e ora della violazione (o della scoperta) - Natura della violazione - Dati coinvolti - Persone coinvolte - Come è stata scoperta

MODALITÀ DI SEGNALAZIONE RAPIDA: - Telefono: [numero Referente] - Email: databreach@centrophoenix.it [adattare] - Di persona

TEMPISTICA: IMMEDIATAMENTE (entro minuti/poche ore)

☐ STEP 1.3 - Registrazione iniziale - Il Referente Data Breach registra la segnalazione - Assegna numero protocollo: BREACH/[ANNO]/[NUMERO] - Registra nel “Registro Violazioni” (Modulo 7-H) - Annota data e ora precisi della scoperta (conta per le 72 ore!)

FASE 2: CONTENIMENTO E VALUTAZIONE INIZIALE (Ore 0-6)

☐ STEP 2.1 - Misure immediate di contenimento

PRIORITÀ: Contenere la violazione e limitare i danni

AZIONI IMMEDIATE (a seconda del caso):

Per ACCESSO NON AUTORIZZATO: ☐ Disattivare account compromessi ☐ Cambiare password ☐ Bloccare accessi sospetti ☐ Isolare sistema compromesso dalla rete

Per INVIO ERRATO DI EMAIL/DOCUMENTI: ☐ Richiedere cancellazione al destinatario sbagliato ☐ Se possibile, richiamare email (funzione Outlook) ☐ Documentare il destinatario errato

Per FURTO/SMARRIMENTO DISPOSITIVI: ☐ Se dispositivo geolocalizzabile: tentare localizzazione ☐ Se possibile: cancellazione remota dati ☐ Bloccare accesso da remoto ☐ Denunciare alle autorità competenti

Per RANSOMWARE/MALWARE: ☐ Isolare immediatamente dispositivi infetti ☐ Scollegare dalla rete ☐ NON pagare riscatti senza consulto ☐ Contattare esperti di sicurezza informatica ☐ Verificare se backup disponibili

Per PERDITA DATI/CANCELLAZIONE: ☐ Tentare recupero da backup ☐ Interrompere operazioni su dispositivo (se cancellazione) ☐ Contattare tecnico IT per recupero dati

Per DATI CARTACEI: ☐ Recuperare documenti se possibile ☐ Limitare accesso all'area dove è avvenuta la violazione ☐ Identificare eventuali testimoni

☐ STEP 2.2 - Raccolta informazioni dettagliate

Documentare con precisione (Modulo 7-B “Scheda di Valutazione”):

- A) NATURA DELLA VIOLAZIONE: ☐ Tipo: Riservatezza / Integrità / Disponibilità ☐ Descrizione dettagliata dell'incidente ☐ Come è avvenuta (causa) ☐ È stata causata da: umano / tecnico / naturale / malintenzionato
- B) TEMPISTICA: ☐ Data e ora della violazione (stima se non certa) ☐ Data e ora della scoperta (certa) ☐ Violazione ancora in corso? Sì / No ☐ Se conclusa: quando si è conclusa
- C) DATI COINVOLTI: ☐ Tipologia di dati:
- Dati anagrafici
 - Dati di contatto
 - Dati sanitari/clinici
 - Dati economici
 - Altri dati sensibili ☐ Numero di interessati coinvolti (stima se necessario) ☐ Categorie di interessati (pazienti / dipendenti / altro)
- D) SISTEMI/ARCHIVI COINVOLTI: ☐ Database digitale ☐ Email ☐ Cartelle cliniche cartacee ☐ Backup ☐ Dispositivi mobili ☐ Altro: _____
- E) CAUSE: ☐ Errore umano (specificare) ☐ Guasto tecnico (specificare) ☐ Attacco esterno (specificare) ☐ Furto/smarrimento ☐ Causa naturale (incendio, allagamento, etc.) ☐ Altra causa: _____

☐ STEP 2.3 - Costituzione team di gestione

Convocare immediatamente: ☐ Titolare del trattamento ☐ Referente Data Breach ☐ Referente Privacy ☐ Responsabile IT (se coinvolti sistemi informatici) ☐ Legale (se violazione grave) ☐ Altri: _____

Briefing iniziale: condividere informazioni raccolte

FASE 3: VALUTAZIONE DEL RISCHIO (Ore 6-24) * FASE CRITICA PER DECISIONE NOTIFICA *****

☐ STEP 3.1 - Valutazione del rischio per diritti e libertà degli interessati

OBIETTIVO: Determinare se la violazione presenta: - **RISCHIO BASSO:** nessun rischio o rischio improbabile → NO notifica - **RISCHIO MEDIO:** rischio possibile → SÌ notifica al Garante - **RISCHIO ELEVATO:** rischio probabile e significativo → SÌ notifica + comunicazione agli interessati

CRITERI DI VALUTAZIONE (Modulo 7-C “Matrice Valutazione Rischio”):

- A) NATURA DEI DATI VIOLATI: Attribuire punteggio:
- Dati anagrafici base: 1 punto
 - Dati di contatto: 1 punto
 - Dati economici: 2 punti
 - Dati sanitari/clinici: 3 punti (ALTO IMPATTO)

- Dati su minori: +1 punto
- Dati su soggetti vulnerabili: +1 punto
- B) GRAVITÀ DELLE CONSEGUENZE POTENZIALI: ☐ Danno economico (frode, furto identità): 2 punti ☐ Danno reputazionale: 2 punti ☐ Violazione riservatezza dati sanitari: 3 punti (ALTO IMPATTO) ☐ Discriminazione: 3 punti ☐ Perdita controllo dati personali: 2 punti ☐ Danno fisico: 3 punti ☐ Danno psicologico: 3 punti (in ambito psicologico: ALTO IMPATTO)
- C) NUMERO DI INTERESSATI COINVOLTI:
 - 1-10 interessati: 1 punto
 - 11-100 interessati: 2 punti
 - 100 interessati: 3 punti
- D) FACILITÀ DI IDENTIFICAZIONE DEGLI INTERESSATI:
 - Dati non identificabili/anonimi: 0 punti
 - Identificazione difficile: 1 punto
 - Identificazione diretta: 2 punti
- E) MISURE DI SICUREZZA PREESISTENTI:
 - Crittografia/pseudonimizzazione: -2 punti
 - Password robuste: -1 punto
 - Accesso limitato: -1 punto
- F) MISURE DI MITIGAZIONE POST-VIOLAZIONE:
 - Contenimento rapido: -1 punto
 - Recupero dati: -1 punto
 - Cancellazione presso destinatario: -2 punti

CALCOLO RISCHIO: Totale punti: _____

- 0-3 punti: RISCHIO BASSO → NO notifica necessaria
- 4-7 punti: RISCHIO MEDIO → SÌ notifica al Garante
- 8+ punti: RISCHIO ELEVATO → SÌ notifica al Garante + comunicazione agli interessati

☐ STEP 3.2 - Valutazione specifica per dati sanitari

*** IN AMBITO PSICOLOGICO: ATTENZIONE MASSIMA ***

I dati sanitari/clinici sono particolarmente sensibili. Una violazione di dati psicologici può causare: - Grave danno reputazionale all'interessato - Discriminazione - Danno psicologico (stress, ansia, vergogna) - Impatti sulle relazioni personali/lavorative

PRESUNZIONE: Violazione di dati clinici psicologici → RISCHIO ELEVATO

ECCEZIONI (rischio ridotto): ☐ Dati crittografati/pseudonimizzati (chiave non compromessa) ☐ Violazione contenuta immediatamente con certezza nessun accesso terzi ☐ Dati già pubblici (raro in ambito clinico)

☐ STEP 3.3 - Decisione preliminare

In base alla valutazione del rischio, decidere:

☐ OPZIONE A: RISCHIO BASSO → NON notificare al Garante → Documentare nel Registro Violazioni → Procedere con misure correttive interne → Fine procedura emergenza (ma documentare tutto)

☐ OPZIONE B: RISCHIO MEDIO/ELEVATO → NOTIFICARE al Garante entro 72 ore → Se rischio ELEVATO: anche comunicare agli interessati → Procedere con FASE 4 e 5

FASE 4: NOTIFICA AL GARANTE (Entro 72 ore dalla scoperta) *** SE RISCHIO $\geq$ MEDIO ***

☐ STEP 4.1 - Verifica termine 72 ore

Data/ora scoperta violazione: ____/____/____ ore ____ Termine 72 ore: ____/____/____ ore

SE il termine sta per scadere e non si hanno tutte le informazioni: → Inviare notifica PARZIALE entro 72 ore (indicare che seguiranno integrazioni) → Inviare integrazioni appena disponibili informazioni complete

☐ STEP 4.2 - Preparazione notifica al Garante

Utilizzare il sistema online del Garante Privacy: <https://servizi.gdpd.it>

OPPURE (in caso di malfunzionamento): PEC: protocollo@pec.gdpd.it

CONTENUTO OBBLIGATORIO DELLA NOTIFICA (Art. 33, par. 3 GDPR):

☐ a) NATURA DELLA VIOLAZIONE - Descrizione dettagliata dell'incidente - Come è avvenuta - Tipo di violazione (riservatezza/integrità/disponibilità)

☐ b) CONTATTI - Nome e contatti del Referente Privacy/Data Breach (o Titolare)

☐ c) CONSEGUENZE PROBABILI - Descrizione delle probabili conseguenze della violazione - Valutazione del rischio

☐ d) CATEGORIE E NUMERO APPROSSIMATIVO DI INTERESSATI - Numero di interessati coinvolti (es. "circa 50 pazienti") - Categorie (es. "pazienti in terapia nel periodo X")

☐ e) CATEGORIE E NUMERO APPROSSIMATIVO DI REGISTRAZIONI - Numero di record di dati personali (es. "50 cartelle cliniche") - Categorie di dati (es. "dati anagrafici, dati clinici, diagnosi")

☐ f) MISURE ADOTTATE O PROPOSTE - Misure di contenimento già attuate - Misure per mitigare le conseguenze - Misure per prevenire future violazioni

Compilare il Modulo 7-D "Notifica al Garante"

☐ STEP 4.3 - Approvazione e invio notifica - Far approvare la notifica dal Titolare - Inviare tramite portale online Garante (preferibile) - Conservare ricevuta/protocollo di invio - Annotare nel Registro Violazioni

☐ STEP 4.4 - Se notifica oltre 72 ore - Se impossibile rispettare le 72 ore: documentare i motivi - Inviare comunque notifica (anche tardiva) - Indicare nella notifica i motivi del ritardo

FASE 5: COMUNICAZIONE AGLI INTERESSATI (Senza ingiustificato ritardo) *** SE RISCHIO ELEVATO ***

☐ STEP 5.1 - Valutazione necessità comunicazione

Comunicare agli interessati SE e SOLO SE: ☐ Il rischio è ELEVATO per diritti e libertà

ECCEZIONI (NO comunicazione anche se rischio elevato): ☐ a) Misure tecniche/organizzative di protezione applicate prima della violazione (es. crittografia con chiave non compromessa) ☐ b) Misure successive che assicurano che rischio elevato non si concretizzi ☐ c) Comunicazione richiederebbe sforzo sproporzionato → comunicazione pubblica o misura simile

☐ STEP 5.2 - Preparazione comunicazione

CONTENUTO OBBLIGATORIO (Art. 34, par. 2 GDPR):

- ☐ a) NATURA DELLA VIOLAZIONE - Descrizione in linguaggio semplice e chiaro - Cosa è successo
- ☐ b) CONTATTI - Nome e contatti del Referente Privacy (o Titolare) - Possibilità di ottenere maggiori informazioni
- ☐ c) CONSEGUENZE PROBABILI - Spiegare quali potrebbero essere le conseguenze - Rassicurare se rischio limitato
- ☐ d) MISURE ADOTTATE - Cosa ha fatto il Centro per contenere la violazione - Cosa ha fatto per mitigare i danni - Raccomandazioni per l'interessato (es. cambiare password, monitorare estratti conto, etc.)

Utilizzare Modulo 7-E “Comunicazione agli Interessati”

LINGUAGGIO: - Chiaro e semplice - Evitare tecnicismi - Essere trasparenti e onesti - NON minimizzare la gravità ma neanche allarmismo eccessivo - Focalizzare su cosa fare

☐ STEP 5.3 - Modalità di comunicazione

- ☐ COMUNICAZIONE INDIVIDUALE (preferibile se possibile): - Email personale - Lettera raccomandata - Telefonata + conferma scritta - Consegna a mano
- ☐ COMUNICAZIONE PUBBLICA (se sforzo sproporzionato): - Pubblicazione sul sito web - Annuncio stampa - Altro mezzo per raggiungere pubblicamente gli interessati

TEMPISTICA: Senza ingiustificato ritardo (idealmente 24-48 ore dopo la notifica al Garante)

- ☐ STEP 5.4 - Invio comunicazioni - Inviare comunicazioni a tutti gli interessati coinvolti - Documentare l'invio - Gestire eventuali richieste di chiarimento - Aggiornare Registro Violazioni

FASE 6: INDAGINE APPROFONDITA E MISURE CORRETTIVE (Giorni successivi)

☐ STEP 6.1 - Indagine dettagliata sulle cause

Condurre analisi approfondita: ☐ Ricostruire esattamente come è avvenuta la violazione ☐ Identificare vulnerabilità sfruttate ☐ Identificare responsabilità (senza caccia alle streghe ma per migliorare) ☐ Documentare tutto

Compilare “Report di Indagine” (Modulo 7-F)

☐ STEP 6.2 - Misure correttive immediate

Implementare misure per prevenire ripetizione:

MISURE TECNICHE: ☐ Aggiornare software/sistemi ☐ Implementare/rafforzare crittografia ☐ Migliorare controlli di accesso ☐ Implementare autenticazione a due fattori ☐ Migliorare sistema di backup ☐ Altro: _____

MISURE ORGANIZZATIVE: ☐ Formazione aggiuntiva personale ☐ Aggiornamento procedure ☐ Revisione autorizzazioni di accesso ☐ Implementazione controlli aggiuntivi ☐ Altro: _____

MISURE FISICHE: ☐ Migliorare sicurezza fisica locali ☐ Implementare sistemi di controllo accessi ☐ Altro: _____

☐ STEP 6.3 - Piano di azione correttiva - Redigere piano formale con azioni, responsabili, scadenze - Monitorare implementazione - Verificare efficacia

☐ STEP 6.4 - Eventuale coinvolgimento autorità - Se violazione derivante da reato: denunciare autorità competenti - Collaborare con Polizia Postale se necessario - Documentare

FASE 7: DOCUMENTAZIONE E CHIUSURA (Completamento)

☐ STEP 7.1 - Completamento documentazione

Assicurarsi che sia stato compilato e archiviato: ☐ Modulo 7-A: Segnalazione Iniziale ☐ Modulo 7-B: Scheda di Valutazione ☐ Modulo 7-C: Matrice Valutazione Rischio ☐ Modulo 7-D: Notifica al Garante (se inviata) ☐ Modulo 7-E: Comunicazione Interessati (se inviata) ☐ Modulo 7-F: Report di Indagine ☐ Modulo 7-G: Piano di Azione Correttiva ☐ Modulo 7-H: Registro Violazioni (aggiornato)

☐ STEP 7.2 - Chiusura formale - Riunione finale del team - Verificare completamento tutte le azioni - Chiudere la pratica nel Registro - Archiviare tutta la documentazione (conservare almeno 5 anni)

☐ STEP 7.3 - Lessons learned - Condividere con il team le lezioni apprese - Aggiornare procedure se necessario - Programmare audit di verifica efficacia misure

7.5 REGISTRO DELLE VIOLAZIONI

OBBLIGO: Il Titolare deve tenere un REGISTRO di TUTTE le violazioni (art. 33, par. 5 GDPR), anche quelle NON notificate al Garante.

Il Registro deve contenere: - Fatti relativi alla violazione - Effetti della violazione - Misure adottate

Il Registro deve essere disponibile per eventuali verifiche del Garante.

Utilizzare Modulo 7-H.

7.6 CASI PARTICOLARI

CASO 1: Email con cartella clinica inviata a destinatario sbagliato

AZIONE: ☐ Contenimento: Richiedere immediatamente cancellazione al destinatario ☐ Valutazione: Rischio ELEVATO (dati clinici, violazione riservatezza) ☐ Notifica Garante: SÌ (entro 72 ore) ☐ Comunicazione interessato: SÌ (senza ritardo) ☐ Misure correttive: Formazione su uso email, procedura double-check destinatari

CASO 2: Furto laptop con database pazienti NON crittografato

AZIONE: ☐ Contenimento: Denuncia, tentativo cancellazione remota, cambio password ☐ Valutazione: Rischio ELEVATO (dati clinici accessibili) ☐ Notifica Garante: SÌ (entro 72 ore) ☐ Comunicazione interessati: SÌ (tutti i pazienti nel database) ☐ Misure correttive: Crittografia obbligatoria, policy dispositivi mobili

CASO 3: Furto laptop con database pazienti CRITTOGRAFATO

AZIONE: ☐ Contenimento: Denuncia, verifica che chiave crittografia non compromessa ☐ Valutazione: Rischio BASSO (dati non accessibili senza chiave) ☐ Notifica Garante: NO (se certezza che crittografia non violabile) ☐ Comunicazione interessati: NO ☐ Registro: SÌ (documentare comunque)

CASO 4: Ransomware che cripta e rende inaccessibili cartelle cliniche

AZIONE: ☐ Contenimento: Isolamento sistemi, NO pagamento riscatto immediato, esperti sicurezza ☐ Valutazione: Rischio MEDIO-ELEVATO (disponibilità compromessa, possibile esfiltrazione) ☐ Notifica Garante: SÌ (entro 72 ore) ☐ Comunicazione interessati: Valutare se dati esfiltrati (se sì: SÌ) ☐ Recupero: Tentare ripristino da backup ☐ Misure correttive: Rafforzare sicurezza, formazione, backup offline

CASO 5: Cancellazione accidentale database senza backup recuperabile

AZIONE: ☐ Contenimento: Tentare recupero dati con esperti ☐ Valutazione: Rischio ELEVATO (perdita permanente dati, disponibilità) ☐ Notifica Garante: SÌ (entro 72 ore) ☐ Comunicazione interessati: SÌ (perdita permanente dati) ☐ Misure correttive: Sistema backup robusto, procedure contro cancellazioni accidentali

CASO 6: Cartelle cliniche lasciate incustodite in sala d'attesa, visualizzate da altri pazienti

AZIONE: ☐ Contenimento: Recuperare immediatamente cartelle, identificare testimoni ☐ Valutazione: Rischio MEDIO-ELEVATO (riservatezza, dati clinici) ☐ Notifica Garante: SÌ (entro 72 ore) ☐ Comunicazione interessati: SÌ (pazienti le cui cartelle erano visibili) ☐ Misure correttive: Procedure custodia documenti, formazione personale

7.7 PREVENZIONE - MISURE PER RIDURRE RISCHIO DATA BREACH

MISURE TECNICHE: ☐ Crittografia dati sensibili (sia a riposo che in transito) ☐ Backup regolari (testati periodicamente) ☐ Antivirus e firewall aggiornati ☐ Autenticazione forte (password complesse, 2FA) ☐ Controllo accessi granulare ☐ Log degli accessi ☐ Aggiornamenti software tempestivi ☐ Email crittografate per dati sensibili

MISURE ORGANIZZATIVE: ☐ Formazione continua del personale ☐ Procedure chiare e scritte ☐ Clear desk policy ☐ Gestione corretta dei dispositivi mobili ☐ Controllo accessi fisici ai locali ☐ Distruzione sicura documenti e dispositivi ☐ Test periodici di sicurezza ☐ Piano di disaster recovery

MISURE COMPORTAMENTALI: ☐ Attenzione nell'uso email (verificare destinatari) ☐ Non lasciare documenti incustoditi ☐ Logout da sistemi quando ci si allontana ☐ Non condividere password ☐ Segnalare tempestivamente anomalie

7.8 MODULISTICA

[A causa della lunghezza, fornisco la struttura dei moduli principali]

MODULO 7-A: SEGNALAZIONE INIZIALE VIOLAZIONE

- Data/ora scoperta
- Chi ha scoperto
- Descrizione sommaria
- Dati coinvolti (stima iniziale)
- Azioni immediate intraprese

MODULO 7-B: SCHEDA DI VALUTAZIONE DETTAGLIATA

- Ricostruzione dettagliata dell'incidente
- Natura della violazione
- Cause
- Sistemi coinvolti
- Dati coinvolti (dettagliato)
- Numero interessati
- Tempistica
- Misure di contenimento

MODULO 7-C: MATRICE VALUTAZIONE RISCHIO

- Criteri di valutazione (natura dati, conseguenze, numero interessati, etc.)
- Punteggi
- Calcolo rischio: BASSO/MEDIO/ELEVATO
- Decisione: notificare sì/no, comunicare sì/no

MODULO 7-D: NOTIFICA AL GARANTE

- Tutti i campi obbligatori dell'art. 33 GDPR
- Formato compatibile con sistema online Garante

MODULO 7-E: COMUNICAZIONE AGLI INTERESSATI

- Descrizione violazione (linguaggio semplice)
- Contatti
- Conseguenze possibili
- Misure adottate
- Raccomandazioni per l'interessato

MODULO 7-F: REPORT DI INDAGINE

- Analisi approfondita cause
- Responsabilità
- Vulnerabilità identificate

- Tempistica ricostruita

MODULO 7-G: PIANO DI AZIONE CORRETTIVA

- Misure correttive da implementare
- Responsabili
- Scadenze
- Monitoraggio

MODULO 7-H: REGISTRO VIOLAZIONI (da Modello già fornito in documento principale)

CONCLUSIONE DEL MANUALE DELLE PROCEDURE

Il presente manuale fornisce al Centro Phoenix Srl e Centro Phoenix STP Srl procedure operative dettagliate per la gestione di tutte le principali casistiche previste dal GDPR.

RACCOMANDAZIONI FINALI:

1. **FORMAZIONE:** Formare tutto il personale sulle procedure, in particolare sulla segnalazione data breach
2. **TEST:** Effettuare simulazioni periodiche, specialmente di data breach
3. **AGGIORNAMENTO:** Rivedere e aggiornare le procedure almeno annualmente
4. **DOCUMENTAZIONE:** Conservare tutta la documentazione relativa all'applicazione delle procedure
5. **MIGLIORAMENTO CONTINUO:** Utilizzare ogni richiesta/incidente come opportunità di apprendimento
6. **CONSULTAZIONE:** In caso di dubbi, consultare esperti legali specializzati in privacy

Romano d'Ezzelino, 19/03/2025

Il Titolare del Trattamento dei dati Centro Phoenix Srl

Il Titolare del Trattamento dei dati Centro Phoenix STP Srl

Il Responsabile del Trattamento dei dati Centro Phoenix Srl e Centro Phoenix STP Srl
