ErgotherapeutInnen-Verband Schweiz
Association Suisse des Ergothérapeutes
Associazione Svizzera degli Ergoterapisti

Altenbergstrasse 29 | Postfach 686 | CH-3000 Bern 8
T. +41 (0)31 313 88 44
www.ergotherapie.ch | evs-ase@ergotherapie.ch

Promemoria

La protezione dei dati
nell'ambito dell'ergoterapia

Indice

1 Finalità e campo di applicazione

Il presente promemoria si applica ai membri sia dell'Associazione Svizzera degli Ergoterapisti (ASE) sia dell'Associazione Svizzera delle-dei Dietiste-i legalmente riconosciute/i (ASDD). **La seguente tabella fornisce una panoramica introduttiva sugli obblighi fondamentali nell' attuazione sistematica della protezione dei dati,** dopodiché si passa a una descrizione più dettagliata e corredata da esempi dei requisiti da rispettare.

Il contenuto del promemoria è soggetto esclusivamente alla legge svizzera sulla protezione dei dati (LPD)[1]. Qualora un'azienda (di seguito denominata «studio») sia soggetta anche al regolamento europeo sulla protezione dei dati personali (GDPR), ad esempio perché tra le/i clienti figurano persone fisiche provenienti dall'UE/SEE o perché queste ultime sono tracciate/monitorate sul proprio sito web tramite Google Analytics, si applicheranno altresì le corrispondenti disposizioni europee.

Al riguardo, si fa osservare che il promemoria non si estende all'intera legge sulla protezione dei dati, bensì ne espone gli obblighi principali in maniera sintetica. La responsabilità di attuazione degli obblighi è demandata al singolo studio.

1.1 Panoramica dei fondamentali obblighi di conformità alla protezione dei dati

Campo di azione	Attuazione	Esempio	Rimandi
Predisposizione e aggiornamento periodico dei registri delle attività di trattamento	Oltre a fornire una panoramica sul trattamento dei dati dello studio, i registri costituiscono la base per ottemperare agli ulteriori obblighi.L'apposito «Modello_registro_attività di trattamento» è disponibile all'uso.[2]	Quali dati sono registrati per quale finalità e per quanto tempo? I dati sono trasmessi a terzi?	Punto 3.2.1.1
Verifica degli accordi contrattuali con i responsabili del trattamento e analisi dei flussi di dati verso l'estero	Occorre stipulare degli accordi sul trattamento dei dati (DPA) con i responsabili del trattamento (cfr. «Modello_accordo_trattamento dei dati»).[2] La trasmissione di dati all'estero deve essere notificata alle persone interessate. Il trasferimento dei dati personali in un Paese che non dispone di un'adeguata prote-	Se la gestione delle cartelle pazienti prevede l'uso di un software e di un fornitore di servizi che si occupa dell'hosting dei dati, si rende necessario stipulare un accordo contrattuale con quest'ultimo.	Punto 3.2.4

[1] Legge federale sulla protezione dei dati (RS 235.1)

[2] Download del PDF: https://www.ergotherapie.ch/exercice-de-la-profession/bases-legales

Campo di azione	Attuazione	Esempio	Rimandi
	zione dei dati impone la stipula di contratti aggiuntivi, nonché l'adozione di misure supplementari idonee a garantire l'adeguatezza della protezione dei dati.		
Elaborazione delle richieste delle persone interessate	Le persone interessate hanno il diritto di chiedere • che siano loro fornite le informazioni sui dati che le riguardano, • che i dati falsi siano rettificati, • che i dati inesatti o trattati indebitamente siano cancellati e • che, a determinate condizioni, i dati siano loro consegnati in un formato standard (portabilità dei dati).	Se le/i pazienti chiedono di accedere ai propri dati personali, occorre tra l'altro fornire anche le informazioni su natura e finalità degli stessi.	Punto 3.2.3
Ottemperanza agli obblighi di informazione	Gli studi sono tenuti a informare le persone interessate sul trattamento dei dati personali che le riguardano (raccolta, registrazione, ecc.). In linea generale, l'obbligo di informazione può essere ottemperato mediante dichiarazione sulla protezione dei dati pubblicata sul sito web. È possibile utilizzare il «Modello_dichiarazione sulla protezione dei dati» previo adeguamento alle proprie esigenze.[2]	Le/i pazienti devono essere informate/i del fatto che i loro dati personali saranno trattati ai fini dell'adempimento contrattuale e inoltrati all'assicurazione ai fini della fatturazione.	Punto 3.2.2
Garanzia della sicurezza dei dati e notifica di relative violazioni	In base al livello di rischio che il trattamento dei dati comporta per la persona interessata, si adottano le misure tecniche e organizzative idonee a proteggere l'integrità, la disponibilità e la riservatezza dei dati.	Se i dati personali sono disponibili in forma cartacea è buona norma chiudere a chiave il luogo di conservazione. È altresì opportuno proteggere il computer da accessi non autorizzati utilizzando degli appositi programmi antivirus.	Punto 3.2.5, 3.2.6

Campo di azione	Attuazione	Esempio	Rimandi
	L'eventuale violazione della sicurezza dei dati deve essere segnalata all'IFPDT[3] o alle persone interessate.		
Esecuzione di valutazioni d'impatto sulla protezione dei dati	Il trattamento dei dati previsto deve essere sottoposto a una valutazione del rischio. Un livello di rischio potenzialmente elevato impone di eseguire una valutazione d'impatto sulla protezione prima che esso diventi operativo. [2]	La gestione delle cartelle pazienti obbliga automaticamente a eseguire una valutazione d'impatto sulla protezione dei dati.	Punto 3.2.1.2
Verbalizzazione	Se i dati personali degni di particolare protezione sono trattati su larga scala con mezzi automatizzati, lo studio è tenuto a verbalizzarne almeno la registrazione, la modificazione, la lettura, la comunicazione, la cancellazione e la distruzione.	Uno studio che gestisce le cartelle di tutte/i le/i pazienti è tenuto a verbalizzare nel proprio sistema le eventuali modificazioni, cancellazioni, ecc. di dati. La maggior parte degli attuali sistemi informatici esegue tali operazioni in automatico.	Punto 3.2.1.3
Regolamento per il trattamento dei dati	Il trattamento dei dati sanitari presuppone inoltre la messa a punto di un opportuno regolamento, nel quale è possibile far confluire le diverse informazioni raccolte nel contesto della dichiarazione sulla protezione dei dati.	Le informazioni su finalità del trattamento, su categorie di persone interessate e categorie dei dati personali trattati sono raccolte nel registro delle attività di trattamento; è possibile farvi riferimento nell'apposito regolamento.	Punto3.2.1.4

[3] Incaricato federale della protezione dei dati e della trasparenza

2 Definizioni

Per **protezione dei dati** si intende la protezione della personalità. Non trattandosi in primis di proteggere i dati, bensì la personalità della persona fisica a cui appartengono, è dunque sostanzialmente la sfera privata a essere protetta, ovvero: la protezione dei dati tutela la persona e non i suoi dati!

Per **sicurezza dei dati** si intende la protezione dei dati contro la perdita, la falsificazione, il danneggiamento o la cancellazione mediante l'adozione di specifiche misure organizzative e tecniche. La tipologia e il formato dei dati (analogico o digitale) non sono rilevanti. La sicurezza dei dati è premessa fondamentale della protezione dei dati, sempre che il trattamento concerni dei dati personali.

Per **dati personali** si intendono i dati di persone fisiche (ad es. le/i pazienti, le/i collaboratori/trici). Pertanto, non si tratta della protezione dei dati di uno studio, bensì di informazioni sulla cui base ricostruire l'identità di una determinata persona o che le possono essere attribuite.

I **dati personali degni di particolare protezione**[4] includono, tra gli altri, i dati sanitari.

Trattare si riferisce a qualsiasi utilizzo dei dati personali, segnatamente alle operazioni di registrazione, conservazione, raccolta, cancellazione o modificazione.

Esempio	La registrazione dei dati personali delle/dei pazienti rientra già nel trattamento dei dati, come anche la conservazione delle cartelle pazienti, indipendentemente dal fatto che i dati siano custoditi in forma cartacea o digitale.

La/il **titolare del trattamento** dei dati personali è lo studio che ne decide modalità e finalità.Gli obblighi previsti dalla legislazione sulla protezione dei dati ricadono in gran parte sulla/sul titolare.

Esempio	Lo studio XY risulta essere il titolare del trattamento dei dati delle/dei pazienti.

La/il **responsabile del trattamento** è la persona prestante servizio che elabora i dati personali per conto e su istruzioni della/del titolare.

Esempio	Lo studio XY si avvale di una persona che gestisce il programma software per XY, che registra i dati per conto dello studio e che, in caso di problemi, può accedere all'intero sistema e ai dati personali ivi contenuti. Tale persona prestante servizio è detta responsabile del trattamento.

[4] Art. 3 lett. c LPD o art. 5 lett. c revLPD.

Per **violazione della sicurezza dei dati** si intende ogni violazione della sicurezza che comporti la perdita, la cancellazione, la distruzione, la modificazione dei dati personali, nonché l'accesso o la comunicazione degli stessi a persone non autorizzate.

3 Attuazione sistematica della protezione dei dati

3.1 Principi del trattamento dei dati personali

Principio 1: I dati possono essere trattati soltanto conformemente al **principio di proporzionalità**, vale a dire solo se veramente necessario e solo se ritenuto indispensabile all'adempimento dell'accordo di trattamento.

Esempio	Qualora le/i pazienti possano prenotare le visite online, è consentito consultare soltanto i dati personali necessari ai fini del trattamento terapico o della relativa successiva fatturazione, escluso qualsiasi ulteriore dato non attinente al caso in questione.

Principio 2: È vietato raccogliere segretamente dati relativi alla/al paziente.

Esempio	La persona interessata deve essere debitamente informata sulla presenza di un impianto di videosorveglianza nell'ingresso dello studio, ad esempio tramite pittogramma.

Principio 3: I dati possono essere raccolti e poi trattati solo per la stessa precisa finalità, ossia non improvvisamente per una finalità diversa da quella per la quale erano stati acquisiti.

Esempio	I dati delle/dei candidate/i non possono, dopo una rinuncia, essere riutilizzati ai fini di una nuova assunzione senza previo consenso delle/degli stesse/i.[5]

Principio 4: Una volta che i dati personali non saranno più necessari, si provvederà alla loro cancellazione o distruzione.

Nota	Fintanto che sussiste l'obbligo di conservazione, i relativi dati vanno custoditi. Se una persona non è più cliente da tempo, non è più consentito inviarle del materiale pubblicitario.

[5] Esempio tratto da: https://www.daten-schutz.ch/datenschutz-prinzipien (ultimo accesso il 15.02.2022)

3.2 Gli obblighi fondamentali

3.2.1 Obblighi di documentazione

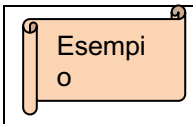
3.2.1.1 Registro delle attività di trattamento

Lo studio è tenuto a documentare il trattamento dei dati e, a tal fine, a predisporre un registro scritto contenente le informazioni essenziali di tutti i trattamenti (registro del trattamento dei dati), che deve essere periodicamente controllato, nonché adeguato nel caso di modificazioni. È possibile utilizzare al riguardo il «Modello_registro_attività di trattamento»[2]. (Attenzione: inserire l'elenco delle misure tecniche e organizzative in una cartella separata). I registri sono degli strumenti di documentazione interna. Tuttavia, se richiesti dall'autorità di vigilanza (IFPDT), devono essere consegnati.

In veste di responsabile del trattamento dei dati è possibile tenere un registro abbreviato, ad esempio quando uno studio si fa carico della fatturazione di un altro studio (ad es. una società affiliata). Anche in questa circostanza il modello di tabella Excel prevede una apposita cartella.

3.2.1.2 Valutazione d'impatto sulla protezione dei dati e definizione dei valori soglia

Prima di procedere al trattamento dei dati occorre, in taluni casi, eseguire una valutazione d'impatto sulla protezione dei dati (DPIA), nella fattispecie per il trattamento su larga scala dei dati sanitari in quanto presentano un livello di rischio elevato per le/i pazienti. («Modello_valutazione d'impatto sulla protezione dei dati»[2]). Lo studio deve esaminare l'esempio e adattarlo alle proprie caratteristiche.



La gestione della cartella pazienti impone di eseguire una DPIA.¨

Nel quadro della valutazione d'impatto sulla protezione dei dati («Modello_ valutazione d'impatto sulla protezione dei dati»[2]) si procede come di seguito:

1. descrizione sistematica del trattamento dei dati previsto
2. valutazione dei rischi (ad es. il rischio di crash informatico o il rischio di hackeraggio con conseguente vendita dei dati)
3. messa a punto di misure volte a ridurre tali rischi.

Se nonostante l'adozione di misure adeguate il livello di rischio rimane elevato occorre rivolgersi all'autorità di vigilanza (IFPDT).[6]

Nel caso di attività di trattamento che non impongono l'obbligo di DPIA, occorre innanzitutto valutarne la necessità in base a una definizione dei valori soglia. («Modello-definizione dei valori soglia»[2]). Ciò non dovrebbe avvenire per la maggior parte delle attività di trattamento dello studio, fatti salvi i trattamenti straordinari.

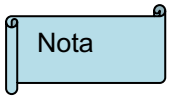
[6] Se dalla **DPIA** emerge ancora un rischio elevato, occorre verbalizzare almeno le seguenti operazioni: registrazione, modificazione, lettura, comunicazione, cancellazione o distruzione (art. 3 cpv. 1 P-OLPD). I **verbali** devono essere conservati almeno un anno separatamente dal sistema in cui sono trattati i dati personali.

3.2.1.3 Verbalizzazione

Se i dati personali degni di particolare protezione sono trattati su larga scala con mezzi automatizzati, lo studio è tenuto a verbalizzarne almeno la registrazione, la modificazione, la lettura, la comunicazione, la cancellazione e la distruzione. La verbalizzazione è richiesta in particolare quando a posteriori non sarà altrimenti possibile determinare se il trattamento sia stato effettuato in base alle finalità per le quali i dati sono stati ottenuti o comunicati.

Il verbale deve fornire informazioni sull'identità della persona che si è occupata del trattamento, su natura, data e ora di quest'ultimo, nonché, all'occorrenza, sull'identità delle/dei destinatarie/i dei dati.

I verbali devono essere conservati almeno un anno separatamente dal sistema in cui sono trattati i dati personali.



Per verbalizzazione si intende un processo automatizzato che in gran parte degli attuali sistemi avviene ormai in automatico.

3.2.1.4 Messa a punto di un regolamento per il trattamento dei dati

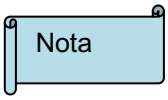
Il trattamento dei dati sanitari presuppone la messa a punto di un regolamento sul trattamento dei dati, nel quale è possibile far confluire le diverse informazioni raccolte nel contesto della dichiarazione sulla protezione dei dati. Il regolamento sul trattamento deve contenere i seguenti dati:

- informazioni sulla finalità del trattamento;
- informazioni sulle categorie di persone interessate e sulle categorie dei dati personali trattati;
- informazioni sul periodo di conservazione dei dati personali o sui criteri che lo determinano;
- informazioni sull'organizzazione interna;
- informazioni sulla provenienza e sulla modalità di raccolta dei dati personali;
- informazioni sulle misure tecniche e organizzative idonee a garantire la sicurezza dei dati;
- informazioni sui diritti di accesso, come anche sulla natura ed entità degli accessi;
- informazioni sulle misure adottate in merito alla minimizzazione dei dati;
- informazioni sulle procedure di trattamento dei dati, segnatamente quelle di registrazione, rettifica, comunicazione, conservazione, archiviazione, pseudonimizzazione, anonimizzazione, cancellazione o distruzione;
- informazioni sulla procedura per l'esercizio del diritto di informazione e del diritto di fornire o trasferire dei dati.

3.2.2 Obbligo di informazione

Lo studio è tenuto a informare le persone interessate sul trattamento dei dati che le riguardano (quindi sulla raccolta, registrazione, ecc.).

In linea generale, l'obbligo di informazione può essere ottemperato mediante dichiarazione sulla protezione dei dati pubblicata sul sito web oppure in forma cartacea durante il primo contatto con la/il paziente.



Si consideri che l'ottemperanza all'obbligo di informazione vale anche nei confronti delle collaboratrici e dei collaboratori dello studio. Pertanto, si consiglia di predisporre una dichiarazione sulla protezione dei dati a parte, da consegnare alle collaboratrici e ai collaboratori oppure da mettere a disposizione, ad esempio, in intranet.

L'allegato (separato) del presente promemoria contiene un modello di dichiarazione sulla protezione dei dati (vedi punto 5) che lo studio deve adattare alle proprie caratteristiche.

È importante che alla fine si forniscano le informazioni sulla totalità dei dati trattati, ovvero sui trattamenti inerenti il campo di attività effettivo (trattamento dei dati delle/dei pazienti), i trattamenti all'interno delle pagine web (cookie, ecc.), nonché quelli delle collaboratrici e dei collaboratori.

3.2.3 Garanzia dei diritti degli interessati

Le persone interessate (ad es. le/i pazienti o eventuali collaboratrici e collaboratori) hanno il diritto di ottenere informazioni sul trattamento dei loro dati personali, oltre che di richiederne la cancellazione o la rettifica qualora fossero errati o incompleti. Tali diritti sono chiamati collettivamente «diritti degli interessati».

Se la/il paziente chiede la cancellazione di determinati dati che la/lo riguardano, occorre prima accertarsi che ciò sia consentito. Ad esempio, riguardo ai dati contenuti nella cartella pazienti esiste l'obbligo legale di conservarli e, dunque, non possono essere cancellati. Per contro, si procede alla cancellazione se si tratta di una vecchia valutazione di una collaboratrice o di un collaboratore ormai non più rilevante.

La persona che inoltra una richiesta di accesso alle informazioni deve prima essere identificata, ossia occorre prima accertarsi (ad es. tramite copia dell'ID) che la/il richiedente sia davvero la/il paziente. La richiesta di accesso alle informazioni esige una risposta senza indugio, in ogni caso entro 30 giorni dal ricevimento della stessa. Questa scadenza è prevista anche per tutti gli atri diritti degli interessati. In linea di massima, le informazioni sono comunicate in forma scritta (è consentita la forma digitale qualora sia garantita la sicurezza della e-mail che, comunque, è meglio trasmettere in forma crittografata).Previo consenso della/del paziente, l'informazione può essere fornita anche verbalmente. Inoltre, è possibile consentire alle/ai pazienti di consultare i dati in loco.

Esempio

La/il paziente presenta una richiesta scritta di accesso ai dati. Lo studio è tenuto a rispondere entro 30 giorni per iscritto (o verbalmente previo consenso della/del paziente) informandola/o sul trattamento dei suoi dati personali, indipendentemente dal fatto che essi siano disponibili in forma cartacea o digitale. Devono essere fornite le seguenti informazioni:

- Indirizzo di contatto dello studio: studio XY, via, NPA/luogo, numero di telefono
- Finalità del trattamento: «I vostri dati personali sono trattati ai fini dell'adempimento contrattuale».
- Periodo di conservazione: «Finché siete nostre/i pazienti continuiamo a trattare i vostri dati. Alla scadenza del termine legale di conservazione, i dati saranno debitamente cancellati».
- Provenienza dei dati personali: «Trattiamo i dati personali forniti da voi stessi e dal medico prescrittore».
- Destinatarie/i dei dati personali: «Oltre che al medico prescrittore, i vostri dati personali saranno comunicati all'assicurazione ai fini della fatturazione».

Di principio, la risposta alla domanda di accesso ai dati deve essere fornita gratuitamente. In via eccezionale è possibile richiedere una partecipazione ai costi pari a max. CHF 300.–. L'accesso alle informazioni può avvenire a pagamento laddove l'operazione comporti un onere eccessivo (ad es. nel caso di dati ormai anonimizzati).Se alla/al paziente è stato comunicato di dover per questo motivo contribuire alle spese e, tuttavia, non giunge risposta entro 10 giorni, la richiesta è da considerarsi ritirata.

3.2.4 Esternalizzazione del trattamento dei dati

Lo studio può anche decidere di esternalizzare il trattamento dei dati a un apposito responsabile (ad es. un hosting-provider o un fornitore di software, persone prestanti servizio nei siti web, ecc.), a condizione che:

- l'esternalizzazione non comporti la violazione degli obblighi di segretezza;
- il responsabile del trattamento elabori i dati soltanto per conto dello studio committente e non a fini personali;
- il responsabile del trattamento sia in grado di garantire la sicurezza dei dati.

Esempio

Lo studio terapico XY raccoglie i dati delle/dei pazienti in un software gestito dal proprio fornitore di servizi. Le collaboratrici e i collaboratori registrano i dati per conto dello studio e, all'occorrenza, si avvalgono del sistema per fornire delle prestazioni di supporto. Lo studio terapico XY è il titolare del trattamento dei dati delle/dei pazienti e, in quanto tale, è tenuto a stipulare un accordo sul trattamento dei dati (vedi paragrafo successivo) con il fornitore del software (persona o azienda).

In questo caso, il titolare del trattamento stipula con il responsabile del trattamento un cosiddetto accordo sul trattamento dei dati (DPA) che regolamenta i diritti e gli obblighi

delle parti («Modello_accordo_trattamento dei dati»[2]). Si prega di selezionare le relative opzioni scegliendo l'apposita casella o cancellando dal modello i passaggi non applicabili.

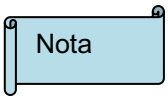
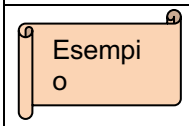
3.2.5 Sicurezza dei dati

I dati personali devono essere trattati in sicurezza. L'adozione di misure tecniche e organizzative (TOM) nel trattamento dei dati personali consente di eliminare o comunque minimizzare i seguenti rischi:

- il trattamento non autorizzato
- il trattamento illecito
- la perdita involontaria
- la distruzione involontaria
- il danneggiamento involontario

Si consideri che rientrano nell'ambito delle misure di protezione e sicurezza anche:

- i controlli degli ingressi agli archivi
- le regole di accesso e la protezione della password nelle varie applicazioni
- la verbalizzazione degli accessi ai dati

	La protezione dei dati deve essere valutata già al momento della progettazione e realizzazione di infrastrutture e procedure (privacy by design). Attraverso impostazioni predefinite nei programmi di trattamento utilizzati, lo studio garantisce di raccogliere ed elaborare soltanto i dati personali strettamente necessari al raggiungimento della specifica finalità del trattamento (privacy by default).
	Il sistema non deve ad esempio presentare dei campi di testo libero dove inserire dei dati personali superflui ai fini del trattamento (ad es. il numero del passaporto, ammesso che non sia determinato da una base giuridica).

3.2.6 Notifica di violazione della sicurezza dei dati

Qualora la violazione della sicurezza dovesse comunque verificarsi (ad es. attacco hacker o perdita di dati per interruzione del sistema), si applicano innanzitutto delle misure correttive.

Esempio	Nel caso venga smarrito un tablet con accesso al sistema di dati delle/dei pazienti, una prima misura potrebbe essere quella di bloccarlo in modo tale da impedire che qualcuno possa accedere da questo dispositivo.

Lo studio deve inoltre ottemperare a degli obblighi di notifica.

Obbligo di notifica all'IFPDT	Obbligo di notifica alla persona interessata

Lo studio è tenuto a **segnalare** all'IFPDT le violazioni di misure per la sicurezza dei dati nel caso comportino un rischio elevato per le persone interessate. Su richiesta dell'IFPDT o, se necessario, per proteggere la persona interessata, anche quest'ultima dovrà essere informata.

Esempio	Un caso simile potrebbe essere la risoluzione di un incidente che presuppone, da parte di tutte le persone interessate, il cambio della password nel sistema di prenotazione. Se la misura correttiva appropriata fosse questa, occorrerebbe informare le persone interessate.

Al momento in cui lo studio diventa operativo **in veste di responsabile del trattamento dei dati**, esso deve notificare senza indugio al titolare del trattamento tutti i casi di violazione della sicurezza dei dati.

3.3 Ulteriori obblighi

Ai fini di applicare la legge sulla protezione dei dati in maniera corretta, lo studio è chiamato ad attuare ulteriori misure.

3.3.1 Conservazione dei dati

Di regola, i dati e i documenti sono conservati per un determinato tempo, nel rispetto di periodi di conservazione differenti.[7]

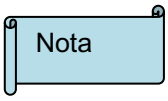
Documento	Periodo di conservazione	Inizio del periodo di conservazione
Fascicoli delle/dei pazienti	20 anni	Dalla fine dell'anno civile in cui si è concluso il trattamento.
Contratti	10 anni	Dalla fine dell'anno civile in cui è avvenuto l'adempimento, la disdetta o la scadenza del contratto.

[7] L'elenco tabellare non è esaustivo; in particolare, possono valere degli obblighi di conservazione previsti da legislazioni speciali.

Fatture (debitori), fatture (creditori Svizzera), note spese	10 anni	Dalla fine del periodo d'imposta in cui le fatture erano esigibili.
Corrispondenza commerciale, comprese le e-mail (solo se pertinenti agli affari)	10 anni	A chiusura dell'esercizio o alle fine di un'operazione commerciale.
Dossier del personale	10 anni	Alla fine del rapporto di lavoro.
Dichiarazioni di imposta	15 anni	A partire dalla fine dell'anno in cui è stata stabilita l'imposta.

Alla scadenza del termine di conservazione i documenti possono o devono essere distrutti.

- I documenti inerenti la gestione dello studio (ad es. fatture o corrispondenza pertinenti agli affari) possono ma non devono essere distrutti.



In talune circostanze può essere necessario continuare a conservare alcuni documenti per motivi probatori.

- Nel caso di dati personali (ad es. i dossier del personale), la legge sulla protezione dei dati prescrive che siano distrutti alla scadenza del periodo di conservazione in quanto non possono essere conservati per sempre.

3.3.2 Controllo del sito web

La configurazione del sito web influisce altresì sulle questioni relative alla protezione dei dati, motivo per cui è opportuno tenere conto di alcuni elementi:

La dichiarazione sulla protezione dei dati deve essere reperibile sul sito web unitamente a una descrizione della modalità di trattamento dei dati tramite sito web.

- Cookie
- Modulo di contatto
- Webshop
- Tool di registrazione online
- Newsletter
- Ecc.

Nota	I dati sulla persona comprendono anche l'indirizzo IP.Per questo motivo, la dichiarazione sulla protezione dei dati deve contenere l'informazione che l'indirizzo IP sarà elaborato nel quadro dell'utilizzo del cookie X.
Nota	Nel caso di alcuni cookie, le/gli utenti devono fornire il proprio consenso attraverso un apposito cookie banner. Anche se in Svizzera tale consenso non è in genere richiesto, le/gli utenti devono comunque essere informate/i sull'uso di cookie (di solito nella dichiarazione sulla protezione dei dati).
Esempio	Se, ad esempio, il tracciamento degli utenti avviene tramite Google Analytics, lo studio è soggetto al regolamento europeo sulla protezione dei dati (GDPR), salvo che non sia in grado di garantire, attraverso geo-blocking, che nessuna persona dell'UE sarà tracciata sulla pagina web. Laddove non sia possibile escludere l'accesso di persone dell'UE/SEE, occorre fornire un cookie banner che consenta alla/all'utente di esprimere il proprio consenso al tracciamento utilizzando l'apposito pulsante sullo schermo. La/l'utente che non acconsente ai cookie, non sarà tracciata/o!

3.4 Invio di newsletter

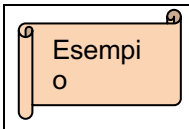
L'invio di newsletter è soggetto a una serie di regole che differiscono a seconda che la/il destinataria/o sia o meno una/un cliente già esistente.

Le newsletter alle/ai **non clienti** possono essere inviate solo previo loro **consenso**.

Nota	Per fornire il proprio consenso, in Svizzera è sufficiente **un semplice opt-in**, vale a dire che la persona interessata acconsente a ricevere le newsletter registrandosi tramite il tool newsletter o altra procedura. L'UE impone invece il cosiddetto **double opt-in**: la/il destinataria/o è tenuta/o a fornire il consenso ben due volte e, pertanto, non può ricevere una mail pubblicitaria subito dopo essersi registrata/o.

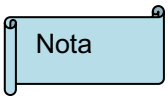
Se la/il destinataria/o risulta già tra le/i **clienti**, la newsletter **non necessita del consenso**, **a condizione che**:

- la pubblicità riguardi dei **servizi o dei prodotti uguali o analoghi** a quelli che le/i clienti hanno già acquistato;



Se le/i clienti si sono rivolte/i allo studio XY per un consulto, le newsletter possono contenere ulteriori offerte relative alle prestazioni erogate, ma non possono esulare dall'oggetto in questione, ad esempio pubblicizzando all'improvviso delle automobili.

- alla stipula del contratto, le/i clienti forniscono il proprio indirizzo e-mail allo studio;
- le/i clienti devono essere informate/i sul diritto di poter **negare** il consenso all'invio di mail pubblicitarie.



La stessa newsletter deve offrire la possibilità di negare il consenso per evitare che le/i clienti ricevano delle newsletter non richieste.

4 Procedura nel caso di domande o dubbi

Nel caso di domande o dubbi sull'applicazione della protezione dei dati, si prega di contattare la segreteria dell'ASE per l'ulteriore procedere:

evs-ase@ergotherapie.ch

5 Modelli di documento

I modelli di documento ivi indicati sono disponibili per il download sul sito web dell'Associazione:
www.ergotherapie.ch > esercizio della professione> basi legali