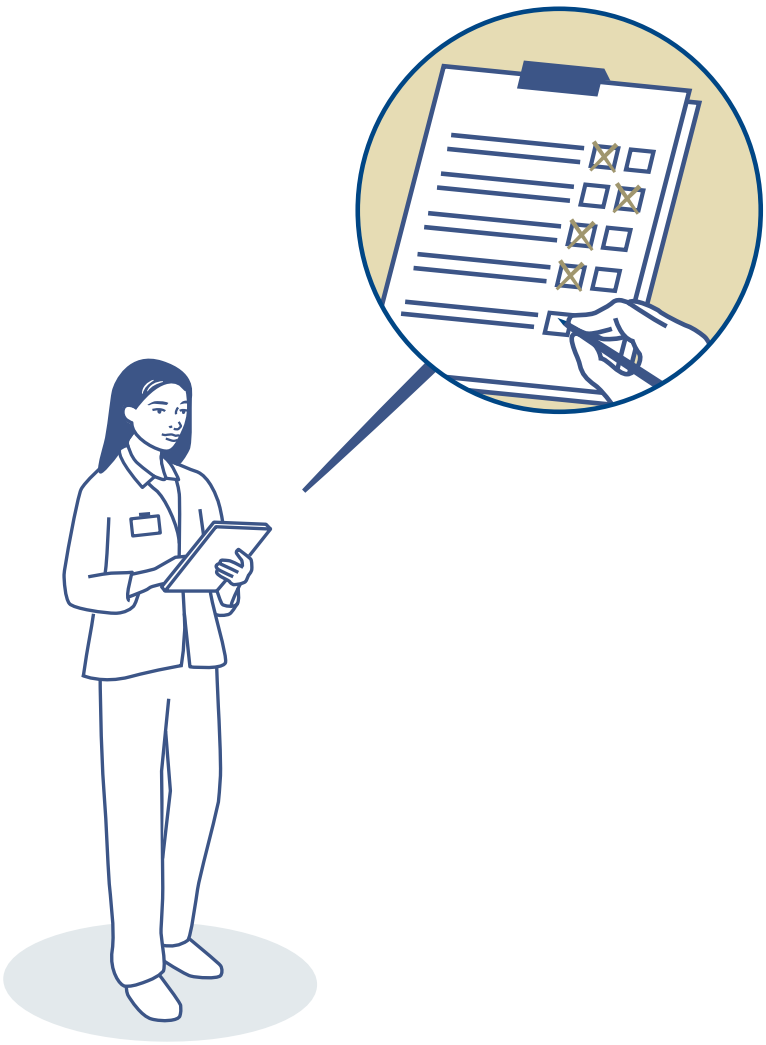
Modello di registro delle attività di trattamento dei dati e relativa guida



Versione 03/2023

FMH · Verbindung der Schweizer Ärztinnen und Ärzte · Fédération des médecins suisses
Postfach · CH-3000 Bern 16 · Telefon +41 31 359 11 11 · info@fmh.ch · www.fmh.ch

Premessa

La nuova Legge federale sulla protezione dei dati (LPD) e l'ordinanza sulla protezione dei dati (OPDa) perseguono l'obiettivo di proteggere la personalità e i diritti fondamentali delle persone fisiche. Per raggiungere tale obiettivo, nella legge e nell'ordinanza sono stati definiti requisiti per il trattamento dei dati personali.

Nell'ambito della loro attività, gli studi medici, i medici e il loro personale ausiliario trattano numerosi dati personali. In tale contesto sono pertanto tenuti a osservare e mettere in pratica, tra l'altro, le disposizioni della LPD.

Il presente documento, unitamente ad altri, intende fornire aiuto per l'attuazione e il rispetto delle norme in materia di protezione dei dati.

Sommario

1 Definizioni dei termini

Termine	Descrizione
Dati personali/dati personali degni di particolare protezione	Sono considerati **dati personali**, tutti i dati che si riferiscono a una persona determinata o determinabile. Il fatto che una persona sia, direttamente o indirettamente, determinata o identificabile dipende in particolare dal contesto in cui si trovano i dati o in cui vengono trattati. Sono dati personali, tra l'altro, i dati anagrafici, i recapiti, il sesso, la data di nascita, la professione ecc. Ai sensi della LPD, i **dati personali degni di particolare protezione** comprendono i dati che forniscono informazioni su — la salute (ad es. stato di salute, diagnosi, cure, ecc.) e la sfera intima (ad es. sessualità); — l'appartenenza a una razza e l'etnia; — le opinioni e le attività religiose, ideologiche, politiche o sindacali; — le misure di assistenza sociale e — i procedimenti e le sanzioni amministrativi o penali. Rientrano tra i dati personali degni di particolare protezione anche i dati genetici e biometrici che identificano in modo univoco una persona.
Profilazione (profiling)	Con il termine **profilazione** (in inglese «profiling») si intende qualsiasi trattamento automatizzato di dati personali al fine di valutare, analizzare o prevedere aspetti personali di una persona fisica. Ai sensi della LPD, per la profilazione vengono utilizzati in particolare i seguenti aspetti personali al fine di effettuare analisi o previsioni: «prestazioni lavorative, situazione economica, salute, preferenze personali, interessi, affidabilità, comportamento, luogo di dimora o cambio di luogo».
Supporti dati	Il termine **supporto dati** viene utilizzato quando vengono utilizzati supporti dati sia fisici che digitali.
Supporti dati digitali (rimovibili)	I **supporti di dati digitali (rimovibili)** comprendono, tra l'altro, CD/DVD, chiavette USB, dischi rigidi esterni, nastri, laptop, server, ecc.
Supporti dati fisici	Sono considerati **supporti dati fisici** ad es. i documenti cartacei.
Trattamento	Il **trattamento** di dati comprende qualsiasi gestione di dati personali, indipendentemente dai mezzi e dalle procedure utilizzati. Con il termine trattamento ci si riferisce quindi, tra l'altro, a qualsiasi operazione di acquisizione, salvataggio, conservazione, utilizzo, modifica, comunicazione, archiviazione, cancellazione o distruzione di dati personali.
Trattamento automatizzato	Per **trattamento automatizzato** si intende il trattamento (cfr. il termine **«trattamento»**) di dati personali mediante procedure automatizzate. Un trattamento è **automatizzato** se si svolge in forma strutturata, di norma mediante apparecchiature per il trattamento dei dati (ad es. server, servizi di comunicazione, computer, sistemi o programmi informatici). Non rientrano nel concetto di **trattamento automatizzato** i sistemi di archiviazione analogica come, ad esempio, gli archivi cartacei o le registrazioni manuali.

2 Guida al modello di registro delle attività di trattamento dei dati

2.1 Aspetti generali

Con l'entrata in vigore della nuova Legge federale sulla protezione dei dati (LPD), i responsabili vengono obbligati, a determinate condizioni, a tenere un registro delle attività di trattamento dei dati. Tale obbligo riguarda i responsabili con più di 250 collaboratori, nonché i responsabili del trattamento che effettuano il trattamento di dati personali degni di particolare protezione. A causa della sensibilità dei dati sanitari, si raccomanda ai medici e agli studi medici di includere nel registro quantomeno le attività di trattamento focalizzate sul trattamento di dati personali degni di particolare protezione (ad es. tenuta e gestione delle cartelle cliniche, gestione dei dati dei pazienti per la fatturazione alle assicurazioni sociali, gestione del personale, ecc.). In linea di principio, sia il responsabile (ad es. lo studio medico) che determinati incaricati del trattamento (ad es. centri di fatturazione) devono tenere ciascuno un proprio registro.

2.2 Istruzioni per la compilazione del registro

Le seguenti spiegazioni relative alle singole colonne del registro intendono fornire ai responsabili supporto per la compilazione. Le colonne elencate riguardano i dati minimi che per legge devono essere riportati nel registro. Il modello contiene alcuni esempi (marcati in rosso) che possono essere ulteriormente adattati, integrati o eliminati qualora le attività di trattamento suggerite non siano pertinenti.

Attività di trattamento dei dati	Qui va indicata la specifica attività che prevede il trattamento di dati personali. Laddove risulti utile, le attività di trattamento correlate o simili possono anche essere raggruppate in un'unica attività di trattamento. La denominazione dell'attività deve essere il più possibile univoca e deve fornire informazioni su come vengono trattati i dati e in quale contesto.
Scopo	In questa colonna deve essere indicato lo scopo per il quale vengono trattati dati personali. È anche possibile indicare diversi scopi.
Responsabili	Qui deve essere indicata la persona responsabile dell'attività di trattamento e dei dati trattati. È responsabile la persona che decide in che modo e con quali strumenti devono essere trattati i dati (ad es. il medico). Se di un'attività di trattamento (ad es. la tenuta di una cartella clinica in uno studio medico di gruppo) sono responsabili più persone, si raccomanda di indicare il nome dello studio medico e le funzioni dei responsabili (ad es. medico curante). Più responsabili sono ammessi in particolare se più persone decidono riguardo ai mezzi e alle procedure da utilizzare per il trattamento (ad es. la direzione).
Categorie di persone interessate	Qui devono essere menzionate le categorie di persone riguardo alle quali vengono trattati dati personali. Per categorie di persone interessate si intendono gruppi tipizzati che abbiano determinate caratteristiche (ad es. pazienti, collaboratori, fornitori di servizi, ecc.).
Categorie di dati personali	Qui è possibile raggruppare i dati personali trattati in categorie (ad es. dati anagrafici, recapiti, dati salariali, dati relativi alle assicurazioni (sociali), coordinate bancarie, dati relativi alle cure, dati sanitari, ecc.). I dettagli della categorizzazione possono essere definiti in diversi modi.

Categorie di destinatari	Anche i destinatari che, nell'ambito di un trattamento, possono prendere visione dei dati personali o avervi accesso possono essere raggruppati in categorie. Per quanto concerne i destinatari, non ha alcuna rilevanza se abbia o meno luogo attivamente un trasferimento di dati o se vi abbiano accesso direttamente. I destinatari possono essere persone fisiche, aziende, autorità, ecc. Si raccomanda di scegliere per ogni categoria di destinatari una denominazione significativa (ad es. casse malati, assicurazioni di invalidità, contabilità, amministrazione tributaria, autorità di vigilanza, fornitori di servizi (IT), ecc.).
Durata di conservazione/ criteri di conservazione	Se noti, devono essere indicati i termini concreti per la conservazione dei dati (ad es. il numero di giorni o di anni). A tale proposito devono essere tenuti in considerazione in particolare i termini di conservazione previsti dalla legge o dai regolamenti di categoria. Se non sussistono termini di conservazione previsti dalla legge o dai regolamenti di categoria, è opportuno indicare in base a quali criteri vengono conservati i dati personali (ad es. fino al raggiungimento dello scopo, fino all'uscita del/della collaboratore/trice).
Misure per la sicurezza dei dati	Qui bisogna indicare se e quali misure tecniche e organizzative sono già state implementate per proteggere i dati da violazioni della riservatezza, dell'integrità e della disponibilità (ad es. armadi chiusi a chiave per le cartelle cliniche in formato fisico, traffico e-mail criptato, limitazione degli accessi agli archivi digitali, formazione del personale, ecc.). Qui esiste in linea di principio anche la possibilità di rinviare a sistemi di sicurezza giàesistenti.
Comunicazione di dati all'estero	In questa colonna è possibile indicare, mediante «Sì» o «No», se nell'ambito delle attività di trattamento vengono comunicati dati all'estero. Si ha una comunicazione, tra l'altro, se i dati personali vengono trasmessi a un altro medico o a un laboratorio all'estero o se per l'attività di trattamento viene utilizzato un sistema il cui fornitore ha sede all'estero e quindi, potenzialmente, può accedere ai dati (ad es. utilizzando sistemi basati su cloud, nella misura in cui il provider abbia o possa teoricamente avere accesso ai dati in chiaro).
Indicazione dello stato e garanzie/strumenti	Se alla risposta concernente la comunicazione di dati personali all'estero si è risposto «Sì», deve essere indicata la nazione in questione. In aggiunta, va indicato in che modo viene garantita un'adeguata protezione dei dati personali e, con essa, dei diritti della personalità delle persone interessate. A causa della complessità dei processi informatici, si raccomanda di chiarire con il rispettivo fornitore di servizi IT, se i dati personali vengono trasmessi all'estero. In caso di comunicazione all'estero, è necessario accertare anche mediante quali misure vengono rispettati i requisiti di legge. La protezione dei dati si considera garantita se il Consiglio federale ha emesso una decisione di adeguatezza per la nazione o il governo in questione. Per sapere se tale decisione di adeguatezza esiste, è possibile consultare l'elenco degli stati [1]. Se tale atto legislativo manca, la legge stabilisce altri requisiti che devono essere soddisfatti per la comunicazione di dati all'estero (art. 16 segg. Legge federale sulla protezione dei dati). In assenza di una decisione di adeguatezza e di una base giuridica sufficiente nella nazione di destinazione, si raccomanda di rinunciare alla comunicazione di dati personali all'estero, in particolare in presenza di un elevato rischio per la personalità o i diritti fondamentali di una persona interessata. In ogni caso, bisogna accertarsi che la protezione dei dati e in particolare la loro sicurezza siano garantite. Inoltre, i dati sanitari sono dati degni di particolare protezione. La maggiore necessità di protezione deve essere considerata adottando le relative misure tecniche e organizzative. I requisiti minimi in fatto di sicurezza dei dati sono stabiliti nell'Ordinanza relativa alla legge federale sulla protezione dei dati (OPDa). Un ulteriore aiuto per la protezione dei dati è rappresentato dai requisiti minimi per la protezione di base IT [2].

[1] Allegato 1 all'Ordinanza sulla protezione dei dati (OPDa)
[2] https://www.fmh.ch/ Servizi / E-Health / Requisiti minimi per la protezione di base

Colophon
Editrice: FMH Federazione die medici svizzeri
Pubblicazione: marzo 2023
www.fmh.ch