

Guida all'utilizzo dell'Accordo sulla riservatezza e dell'Accordo per un trattamento di dati su incarico



Versione 03/2023

Sommario

1	Contenuto della guida	3
2	Chi è soggetto al segreto professionale?	3
3	Quando deve essere stipulato un accordo sulla riservatezza o un accordo per un trattamento di dati su incarico?	3
4	Qual è il contenuto di un accordo sulla riservatezza?	3
5	Che cosa si intende per trattamento su incarico?	3
6	Quali aspetti è necessario osservare richiedendo un accordo sul trattamento dei dati?	4
7	In quali casi l'incaricato del trattamento dei dati deve disporre di un apposito regolamento?	4
8	In quali casi l'incaricato del trattamento dei dati deve disporre di un registro dei trattamenti?	4
9	In quali casi l'incaricato del trattamento dei dati ha l'obbligo di redigere un verbale?	4
10	Si è tenuti a informare i propri pazienti riguardo a un trattamento di dati su incarico?	4

1 Contenuto della guida

La presente guida illustra i modelli per la stipulazione di un accordo sulla riservatezza e di un accordo per un trattamento di dati su incarico.

2 Chi è soggetto al segreto professionale?

I medici e i loro ausiliari sono soggetti al segreto professionale ai sensi dell'art. 321 CP. In questo contesto, il concetto di «ausiliari» è molto ampio e comprende tutte le persone che, direttamente o indirettamente, supportano il medico nello svolgimento della sua attività professionale.

3 Quando deve essere stipulato un accordo sulla riservatezza o un accordo per un trattamento di dati su incarico?

Tutte le volte che un terzo viene incaricato di effettuare un trattamento di dati, è necessario stipulare l'accordo per un trattamento di dati su incarico e l'accordo sulla riservatezza.

4 Qual è il contenuto di un accordo sulla riservatezza?

Mediante un accordo sulla riservatezza, il partner contrattuale si impegna a mantenere riservate determinate informazioni che gli sono state trasmesse o rese note. Nell'accordo sulla riservatezza, è possibile stabilire liberamente quali informazioni devono rimanere riservate. L'obbligo di riservatezza può quindi riferirsi a tutte le informazioni trasmesse o ricevute oppure solo a una parte qualificata di esse (ad es. segreti professionali, dati personali). L'accordo sulla riservatezza può quindi servire a garantire contrattualmente la riservatezza dei segreti professionali e dei dati personali. Esso può tuttavia assoggettare all'obbligo di riservatezza anche le informazioni la cui trasmissione ed elaborazione non sono limitate o regolate dal segreto professionale o dalla legge sulla protezione dei dati.

Se il destinatario delle informazioni tratta i dati su incarico del medico (ad es. fornitore di servizi basati su cloud, servizio di segreteria telefonica ecc.), devono essere osservate anche ulteriori norme di legge che non sono coperte dall'accordo sulla riservatezza. In tali casi è quindi necessario stipulare un accordo per un trattamento di dati su incarico. La stipulazione di un accordo sulla riservatezza è quindi adatta solo a situazioni in cui il destinatario entri in contatto con informazioni riservate più che altro per caso e non sia incaricato del trattamento di tali dati (ad es. team addetto alle pulizie, team di supporto esterno, addetti alla sicurezza, ecc.).

5 Che cosa si intende per trattamento su incarico?

Nell'ambito dell'esecuzione di un incarico, il mandatario tratta dati personali secondo le istruzioni. Tipicamente, sussiste un trattamento su incarico nelle seguenti situazioni.

- **Servizi basati su cloud:** fornitori di servizi di cloud computing/esternalizzazione di sistemi IT e/o di dati presso un centro di calcolo esterno (outsourcing).
- **Servizi informatici:** inserimento dati/conversione di dati/esternalizzazione di backup e archiviazione/servizi di analisi e tracciamento (ad es. Google Analytics).
- **Distruzione e conservazione di dati:** distruzione di documenti e atti cartacei/distruzione di supporti dati/servizi di archiviazione.
- **Marketing/comunicazione commerciale:** call center esterno incaricato/servizi di hosting Web e e-mail/fornitori di servizi per newsletter/trattamento di indirizzi per scopi pubblicitari/agenzie di marketing che trattano dati di clienti/fornitori di analisi di marketing.
- **Contabilità:** contabilità su cloud/outsourcing dei conteggi salariali.

6 Quali aspetti è necessario osservare richiedendo un accordo sul trattamento dei dati?

Il servizio effettivo da fornire è disciplinato da un contratto separato (il cosiddetto «contratto principale»). L'accordo per un trattamento di dati su incarico contiene solo le disposizioni in materia di protezione dei dati da osservare per l'adempimento del contratto principale. Nell'accordo per un trattamento di dati su incarico è quindi necessario specificare con esattezza il contratto principale. Inoltre, il contratto principale non deve prevedere alcuna priorità riguardo alle disposizioni dell'accordo per un trattamento di dati su incarico. Clausole di questo tipo dovrebbero essere cancellate dal contratto principale. Nell'accordo per un trattamento di dati su incarico devono essere definiti anche i dati personali interessati e il tipo di trattamento dei dati (vedi modello). Infine, devono essere stabilite le misure tecniche e organizzative che il mandatario deve mettere in atto per garantire la sicurezza dei dati. Tali misure dipendono dal tipo e dall'entità dei dati trattati, nonché dai rischi in materia di protezione dei dati correlati al trattamento. È quindi possibile definire in astratto solo ambiti in cui devono essere attuate misure concrete (vedi modello).

7 In quali casi l'incaricato del trattamento dei dati deve disporre di un apposito regolamento?

Un regolamento del trattamento di dati deve essere disponibile solo in presenza di un rischio superiore, ad es. se (a) vengono trattati dati personali degni di particolare protezione in grande quantità o (b) viene effettuata una profilazione ad alto rischio. Sono pertanto esclusi i casi in cui vengono trattati dati personali degni di particolare protezione solo occasionalmente. Molte aziende, in particolare le PMI «tradizionali», non effettuano trattamenti di questo tipo e non sono pertanto soggette a questo obbligo.

8 In quali casi l'incaricato del trattamento dei dati deve disporre di un registro dei trattamenti?

Gli operatori del settore del trattamento dei dati con più di 250 dipendenti hanno l'obbligo di tenere un registro in cui siano elencati in modo chiaro tutti i trattamenti di dati. Chi, al 1° gennaio di un determinato anno, occupa meno di 250 addetti deve tenere un registro dei trattamenti solo se (a) vengono trattati dati personali degni di particolare protezione in grande quantità o (b) viene effettuata una profilazione ad alto rischio.

9 In quali casi l'incaricato del trattamento dei dati ha l'obbligo di redigere un verbale?

In caso di trattamento di grandi quantità di dati personali degni di particolare protezione o di profilazione ad alto rischio, è necessario redigere un verbale dei trattamenti effettuati qualora, in caso contrario, non sia possibile stabilire se i dati sono stati trattati per gli scopi previsti. Devono essere messi a verbale, come minimo, i processi di salvataggio, modifica, lettura, comunicazione, cancellazione e distruzione dei dati.

10 Si è tenuti a informare i propri pazienti riguardo a un trattamento di dati su incarico?

In caso di trattamento di dati su incarico, la legge non prevede alcun obbligo di informare le persone interessate.