Accordo per un trattamento di dati su incarico

Versione 03/2023

tra

Nome dello studio medico:

Indirizzo: _____

NPA località: _____

(di seguito detto «cliente»)

e

[Nome]
[Indirizzo]
[NPA e località]

(di seguito detto «fornitore»)

concernente l'esecuzione di un incarico da parte del fornitore

Sommario

1 Oggetto e ambito di applicazione

1.1 Il presente accordo definisce concretamente gli obblighi delle parti in materia di protezione dei dati derivanti dall'elaborazione dell'ordine descritto nel contratto del [Data] concernente [Descrizione del contratto] (di seguito detto «contratto principale»).

1.2 Tutti gli obblighi descritti nel presente accordo trovano applicazione a tutte le attività in relazione al contratto principale, nell'ambito delle quali il fornitore, i suoi collaboratori ed eventuali terzi da esso incaricati entrino o possano entrare in contatto con dati personali del cliente (di seguito detti «dati personali»). Qualora le disposizioni del presente accordo siano in contraddizione con quelle del contratto principale, le disposizioni del presente accordo hanno sempre la precedenza.

1.3 Il fornitore tratta i dati personali per conto del cliente secondo la descrizione delle prestazioni contenuta nel contratto principale. Il trattamento può riguardare in particolare i seguenti dati personali:

- **Trattamenti di dati effettuati:** trattamento dei dati secondo il contratto ecc.
- **Categorie di dati interessate:** dati anagrafici personali (ad es. collaboratori, pazienti, clienti e partner commerciali); dati sanitari; recapiti e dati per la comunicazione (telefono, e-mail, indirizzi IP ecc.); dati contrattuali (ad es. rapporti contrattuali, interessi relativi ai prodotti); cronistorie clienti; dati di fatturazione e pagamento; dati di pianificazione e controllo ecc.
- **Dati personali degni di particolare protezione:** dati sanitari dei pazienti (ad es. referti, documentazione medica, diagnosi, immagini, documenti ecc.); dati genetici e biometrici; dati relativi alla sfera intima ecc.
- **Categorie di persone interessate:** pazienti, clienti, potenziali clienti, collaboratori, fornitori, partner commerciali ecc.

2 Responsabilità e garanzia

2.1 Nell'ambito del presente accordo per un trattamento di dati su incarico e delle istruzioni impartitegli in quanto «responsabile», il cliente è responsabile nei confronti di terzi della legittimità del trattamento dei dati e del rispetto degli obblighi di informazione previsti dalla legge. Nell'ambito del rapporto interno, il cliente e il fornitore sono di volta in volta direttamente responsabili del rispetto delle disposizioni in materia di protezione dei dati applicabili in relazione ai trattamenti di dati effettuati.

2.2 Fornitore e cliente si garantiscono reciprocamente di avere imposto ai propri collaboratori e ai terzi da essi incaricati l'obbligo di riservatezza oppure che questi ultimi sono soggetti all'obbligo di riservatezza previsto dalla legge. Garantiscono inoltre di aver fatto presente per iscritto a tali persone che l'obbligo di riservatezza resta valido anche dopo la cessazione della loro attività.

3 Potere di impartire istruzioni del cliente

3.1 Il fornitore tratterà i dati personali solo nell'ambito di quanto concordato e secondo le istruzioni del cliente, in particolare non per scopi propri. Sono esclusi i casi in cui il trattamento è imposto al fornitore da motivi legali cogenti. In tali situazioni il fornitore, prima di iniziare il trattamento, informerà il cliente nella misura consentita in merito ai relativi requisiti legali.

3.2 Nell'ambito del presente accordo, per un trattamento di dati su incarico, il cliente si riserva il diritto di impartire ampie istruzioni in merito al tipo di trattamento di dati, alla sua estensione e alla procedura da utiliz-

zare, concretizzandole o integrandole poi mediante singole istruzioni specifiche. Il fornitore è tenuto a documentare immediatamente per iscritto l'istruzione ricevuta, sottoponendo la documentazione al cliente per l'approvazione. Il fornitore informerà immediatamente il cliente qualora ritenga che un'istruzione ricevuta violi le leggi applicabili. Il fornitore può rinviare l'esecuzione dell'istruzione fino a quando il cliente non provveda a modificarla o a confermarla fornendo chiarimenti sulla responsabilità.

4 Luogo del trattamento dei dati

4.1 Il fornitore e i terzi da esso incaricati possono trattare dati personali solo in Svizzera, in uno stato membro dell'Unione Europea (UE) o in uno Stato aderente all'Accordo sullo Spazio economico europeo (SEE). Il fornitore informerà per iscritto il cliente sui luoghi di trattamento dei dati, nonché su eventuali spostamenti all'interno dei suddetti paesi. In assenza di opposizione scritta e motivata entro 30 giorni, un tale spostamento si intende approvato.

4.2 Qualsiasi trattamento dei dati al di fuori della Svizzera, della UE o dello SEE necessita del previo consenso scritto del cliente. Il cliente acconsente al trattamento dei dati a condizione che nel luogo in questione sussista dimostratamente un livello di protezione dei dati equivalente e che ciò non sia in contrasto con nessuna disposizione di legge applicabile al cliente. L'obbligo di prova a questo riguardo spetta al fornitore.

4.3 Nella misura in cui il trattamento dei dati abbia luogo al di fuori della Svizzera, il fornitore è in ogni caso responsabile dell'osservanza e dell'attuazione dei requisiti di legge in materia di garanzia di un adeguato livello di sicurezza per tutti i trattamenti di dati e il traffico dati.

5 Obblighi del fornitore

5.1 Trattamento dei dati: il fornitore si impegna a trattare i dati personali e i relativi risultati solo nell'ambito delle istruzioni del cliente. Qualora il fornitore riceva da parte delle autorità l'ordine di consegnare dati del cliente, è tenuto – nella misura in cui ciò sia consentito – a informarne senza indugio il cliente, invitando l'autorità a rivolgersi a quest'ultimo.

5.2 Misure di sicurezza: il fornitore deve strutturare la propria organizzazione in modo da soddisfare i requisiti specifici in materia di protezione dei dati. Il fornitore deve adottare tutte le misure tecniche e organizzative adeguate al rischio e conformi allo stato della tecnica al fine di garantire la riservatezza, la disponibilità e l'integrità dei dati personali, nonché la tracciabilità del trattamento e l'affidabilità dei suoi servizi a tale riguardo, osservando come minimo le misure di sicurezza di cui all'Allegato 1. Su richiesta, il fornitore esibisce nei confronti del cliente e delle autorità di vigilanza prove delle misure adottate e della loro attuazione.

5.3 Registro dei trattamenti e regolamento: nella misura in cui il fornitore o il cliente sia soggetto al relativo obbligo, il fornitore terrà un registro delle attività concernenti il trattamento dei dati svolte presso le sue sedi. Su richiesta, metterà a disposizione del cliente in qualsiasi momento il suo registro, nonché i dati necessari alla creazione di un registro dei trattamenti da parte del cliente. Nella misura in cui abbia luogo un trattamento automatizzato di grandi quantità di dati personali degni di particolare protezione, il fornitore è tenuto a redigere un regolamento del trattamento di dati. Il regolamento deve contenere in particolare informazioni sull'organizzazione interna, sulla procedura per il trattamento e il controllo dei dati, nonché sulle misure per garantire la sicurezza dei dati. Il cliente e il fornitore devono aggiornare periodicamente il regolamento.

5.4 Valutazione sulla protezione dei dati: se il cliente deve effettuare una valutazione sulla protezione dei dati, il fornitore gli metterà a disposizione i fatti e le informazioni tecniche necessari per la valutazione, con riferimento ai trattamenti di dati personali effettuati dal fornitore per conto del cliente, e fornirà il relativo supporto al cliente nelle consultazioni con le autorità di vigilanza.

5.5 Obblighi di supporto: il fornitore è tenuto a supportare il cliente nel rispetto dei suoi obblighi di legge in relazione alla protezione dei dati (ad es. misure per la sicurezza dei dati, notifiche di violazioni all'autorità di vigilanza, notifica alla persona interessata da una violazione). In particolare, il fornitore informerà senza indugio il cliente in merito a tutte le violazioni di norme o istruzioni relative ai dati personali di cui venga a conoscenza e adotterà tutte le misure necessarie per contrastare e attenuare le possibili conseguenze negative per le persone interessate.

5.6 Diritti della persona interessata: il fornitore è tenuto ad adottare misure tecniche e organizzative atte a consentire al cliente di soddisfare i diritti della persona interessata ai sensi delle leggi in materia di protezione dei dati applicabili, in particolare i diritti di informazione, correzione, cancellazione (rispettivamente anonimizzazione) e trasferibilità dei dati e i diritti di opposizione, nonché di mettere in atto il processo decisionale automatizzato nel singolo caso, fornendo al cliente tutte le informazioni necessarie a tal fine. Se viene inviata una relativa richiesta al fornitore, quest'ultimo la inoltrerà senza indugio al cliente per l'elaborazione.

5.7 Obbligo di cancellazione e consegna: il fornitore corregge, cancella (rispettivamente anonimizza) o blocca i dati personali solo se così istruito del cliente, garantendo processi conformi alle norme in materia di protezione dei dati. Sono fatti salvi i diritti di informazione e di consegna. Al termine del contratto o su richiesta del cliente, il fornitore è tenuto a consegnare a quest'ultimo singoli o tutti i documenti e i risultati dei trattamenti contenenti dati personali oppure a distruggerli previ accordi con il cliente. Se il fornitore tratta i dati in un formato speciale dal punto di vista tecnico è tenuto, dietro pagamento di un adeguato indennizzo, a consegnare i dati in tale formato oppure, a scelta del cliente, in un altro formato comune, affinché i dati possano essere trasferiti a una nuova applicazione per quanto possibile senza perdite e mantenendone la struttura e la logica.

5.8 Verbalizzazione: se vengono trattate in modo automatizzato grandi quantità di dati personali degni di particolare protezione o se viene effettuata una profilazione ad alto rischio, il fornitore è tenuto a verbalizzare come minimo i processi di salvataggio, modifica, lettura, comunicazione, cancellazione e distruzione dei dati. La verbalizzazione deve avvenire in particolare qualora, in caso contrario, non sia possibile stabilire se i dati sono stati trattati per gli scopi per i quali sono stati raccolti o resi noti. La verbalizzazione deve fornire indicazioni sull'identità della persona che ha effettuato il trattamento, il tipo, la data e l'ora del trattamento, nonché eventualmente l'identità del/della destinatario/a dei dati. I verbali devono essere conservati per almeno un anno separatamente dal sistema in cui vengono trattati i dati personali. I verbali devono essere accessibili esclusivamente agli organi e alle persone cui spetta la verifica dell'applicazione delle disposizioni in materia di protezione dei dati oppure la tutela o il ripristino della riservatezza, integrità, disponibilità e tracciabilità dei dati e possono essere utilizzati solo a tale scopo.

5.9 Insolvenza Qualora i dati del cliente presso il fornitore siano a rischio di pignoramento o sequestro, per una procedura di insolvenza o di concordato oppure per altri eventi o provvedimenti di terzi, il fornitore è tenuto a informarne senza indugio il cliente. In tale contesto, il fornitore informerà inoltre senza indugio tutte le autorità coinvolte in merito al fatto che la titolarità e la proprietà dei dati spettano esclusivamente al cliente.

5.10 Obbligo di controllo: il fornitore è tenuto a controllare e monitorare l'adempimento dei suddetti obblighi, dimostrandolo in modo adeguato su richiesta del cliente.

6 Rispetto del segreto professionale

6.1 Il fornitore potrà trattare – o avervi accesso – anche dati soggetti al segreto professionale ai sensi dell'art. 321 CP e la cui divulgazione non autorizzata è punibile ai sensi del CP e della LPD. Il fornitore si impegna a mantenere la riservatezza sui segreti professionali, acquisendone conoscenza solo nella misura necessaria all'adempimento dei compiti assegnatigli. Se necessario, il fornitore deve avvalersi della facoltà di non deporre ai sensi dell'art. 171 CPP e del divieto di sequestro ai sensi dell'art. 262 CPP.

6.2 Il fornitore è tenuto a garantire che tutti i collaboratori e i terzi da esso coinvolti si siano impegnati per iscritto a non divulgare senza autorizzazione i segreti professionali loro resi accessibili e che abbiano confermato di essere stati istruiti sulla possibile responsabilità penale ai sensi del CP e della LPD.

6.3 Il fornitore è tenuto a selezionare con la massima diligenza gli eventuali subfornitori, obbligandoli a mantenere la riservatezza sui dati soggetti al segreto professionale nella misura in cui vi abbiano accesso. Inoltre, tali subfornitori devono a loro volta obbligare per iscritto il personale impiegato a mantenere la riservatezza, istruendolo sulle conseguenze di eventuali violazioni di tale obbligo. Ciò vale per analogia anche per tutti gli ulteriori subfornitori.

7 Rapporti di subfornitura

7.1 Nella misura in cui il fornitore, per il trattamento dei dati personali, si avvalga dei servizi di terzi che trattano i dati personali su suo incarico («subfornitori»), il fornitore è tenuto ad elencarne qui di seguito i singoli nomi, indirizzi e compiti.

Nomi/indirizzo	Compiti	Luogo del trattamento dei dati

7.2 L'eventuale incarico ad altri subfornitori deve essere comunicato per iscritto al cliente. In assenza di opposizione scritta entro 30 giorni, l'incarico si intende accettato.

8 Obblighi di informazione e diritti di audit

8.1 Il fornitore è tenuto a informare il cliente in modo completo in merito a tutte le circostanze che mettano a rischio l'erogazione dei servizi. In caso di incidenti rilevanti per la sicurezza e la protezione dei dati, il fornitore è tenuto a informare il cliente per iscritto il più rapidamente possibile, ma al più tardi entro 72 ore dal momento in cui è venuto a conoscenza di un incidente in misura sufficiente. Fornirà inoltre a posteriori le informazioni eventualmente ottenute in un momento successivo. Il fornitore è tenuto a supportare il cliente nell'elaborazione del caso e a fornirgli tutti i documenti ai quali abbia accesso. È poi responsabilità del cliente effettuare tutte le denunce necessarie alle autorità competenti in materia di protezione dei dati, preposte al perseguimento penale o di vigilanza, informando il fornitore in modo trasparente sulla procedura prevista.

8.2 Il fornitore è tenuto a dimostrare con mezzi adeguati il rispetto delle norme in materia di protezione dei dati del presente accordo per un trattamento di dati su incarico, comunicando al cliente, su richiesta, tutte le informazioni necessarie. Il cliente ha facoltà di verificare il rispetto di questi obblighi nella misura necessaria. Qualora, nel singolo caso, si renda necessaria un'ispezione da parte dell'autorità di vigilanza, del cliente o di un controllore da quest'ultimo incaricato, essa si svolgerà negli orari di apertura, con adeguato preavviso e nel

rispetto dell'operatività del fornitore. Nella misura in cui non sia applicabile un obbligo di segretezza previsto dalla legge, il fornitore può subordinare l'ispezione a una dichiarazione di segretezza riguardo ai dati di altri clienti e alle misure tecniche e organizzative predisposte. I concorrenti del fornitore sono in ogni caso esclusi dall'ispezione. Il cliente provvederà a risarcire al fornitore in misura adeguata gli oneri derivanti dall'ispezione.

9 Responsabilità

9.1 Il fornitore e il cliente sono responsabili in solido nei confronti della persona interessata dei danni causati da un trattamento non conforme alla legge o all'accordo.

9.2 Il fornitore risponde esclusivamente per i danni derivanti da un trattamento dei dati da esso effettuato e in relazione al quale (a) non abbia rispettato gli obblighi di legge o contrattuali, (b) abbia agito senza rispettare le istruzioni legittimamente impartite dal cliente o (c) abbia agito in contrasto con le istruzioni legittimamente impartite dal cliente.

9.3 Nella misura in cui il cliente sia tenuto a risarcire la persona interessata, ha la facoltà di rivalersi sul fornitore. Sono fatte salve ulteriori pretese di responsabilità in base alle leggi generali.

10 Durata ed effetti del contratto

10.1 Il presente accordo per un trattamento di dati su incarico viene in essere con la firma di entrambe le parti. L'accordo per un trattamento di dati su incarico sostituisce tutti gli accordi dello stesso tipo e, in caso di contraddizioni, ha la priorità su tutti gli altri accordi.

10.2 La durata del presente accordo dipende dalla durata del contratto principale nella misura in cui le disposizioni del presente accordo non prevedano diversamente. L'accordo resta valido quantomeno finché il fornitore tratta dai personali del cliente, può trattarli o è tenuto a trattarli, a meno che il presente accordo per un trattamento di dati su incarico non venga sostituito da un altro accordo analogo valido e conforme ai requisiti di legge.

10.3 Con il presente accordo, il fornitore rinuncia a qualsiasi diritto di ritenzione dei dati personali oggetto del contratto eventualmente sussistente per qualsivoglia motivo giuridico.

11 Disposizioni finali

11.1 Il contratto e i suoi allegati regolano in modo esaustivo il contenuto del contratto. Le modifiche al contratto necessitano della forma scritta. A tale requisito formale è possibile rinunciare solo per iscritto. Ciò comprende le modifiche contrattuali tramite i cosiddetti accordi «shrink-wrap» e «click-wrap».

11.2 I diritti e gli obblighi derivanti dal rapporto contrattuale non possono essere ceduti, trasferiti o costituiti in pegno senza il consenso scritto della controparte.

11.3 Qualora una o più disposizioni del presente contratto dovessero risultare inefficaci, ciò non inficia la validità delle restanti disposizioni. In tal caso le parti dovranno modificare il contratto in modo tale da raggiungere per quanto possibile lo scopo previsto dalla parte inefficace.

12 Diritto applicabile e foro competente

Al presente accordo per un trattamento di dati su incarico si applica esclusivamente il diritto svizzero con l'esclusione delle norme di conflitto del diritto internazionale, nonché della Convenzione delle Nazioni Unite

sui contratti per la vendita internazionale di beni. Unico foro competente esclusivo è sempre quello della sede del cliente.

13 Firme

Per il fornitore:

Luogo e data:

_____

Firma:

_____

Per il cliente:

Luogo e data:

_____

Firma:

_____

Allegato 1

Per garantire la **riservatezza**, il fornitore deve adottare misure affinché:

a. le persone autorizzate abbiano accesso solo ai dati personali necessari per l'adempimento delle loro mansioni (controllo degli accessi).
Misure idonee:
_____
_____

b. Solo persone autorizzate abbiano accesso ai locali e agli impianti in cui vengono elaborati dati personali (controllo degli accessi).
Misure idonee:
_____
_____

c. Le persone non autorizzate non possano utilizzare i sistemi di elaborazione automatizzata dei dati attraverso le strutture di trasmissione dei dati (controllo degli utenti).
Misure idonee:
_____
_____

Per garantire la **disponibilità** e l'**integrità**, il fornitore deve adottare misure affinché:

a. le persone non autorizzate non possano leggere, copiare, modificare, spostare, cancellare o distruggere i supporti dati (controllo dei supporti dati).
Misure idonee:
_____
_____

b. Le persone non autorizzate non possano salvare, leggere, modificare, cancellare o distruggere i dati personali presenti in memoria.
Misure idonee:
_____
_____

c. Le persone non autorizzate non possano leggere, copiare, modificare, cancellare o distruggere i dati personali durante la loro comunicazione o il trasporto (controllo del trasporto).
Misure idonee:
_____
_____

d. In caso di incidente fisico o tecnico, la disponibilità dei dati personali e l'accesso ad essi possano essere ripristinati rapidamente (ripristino).
Misure idonee:

_____
_____

e. Tutte le funzioni del sistema di elaborazione automatica dei dati siano disponibili (disponibilità), i malfunzionamenti vengano segnalati (affidabilità) e i dati personali salvati non possano essere danneggiati da malfunzionamenti del sistema (integrità dei dati).
Misure idonee:
_____
_____

f. I sistemi operativi e i software applicativi siano sempre mantenuti aggiornati allo stato dell'arte in fatto di sicurezza e le lacune critiche note vengano eliminate (sicurezza del sistema).
Misure idonee:
_____
_____

Per garantire la **tracciabilità**, il fornitore deve adottare misure affinché:

a. sia possibile verificare quali dati personali siano stati inseriti o modificati nel sistema di elaborazione automatica, a che ora e da chi (controllo degli inserimenti).
Misure idonee:
_____
_____

b. Sia possibile verificare a chi sono stati resi noti dati personali con l'ausilio di dispositivi per la trasmissione di dati (controllo della divulgazione).
Misure idonee:
_____
_____

c. Le violazioni della sicurezza dei dati possano essere rapidamente individuate (individuazione), adottando misure per mitigare o eliminarne le conseguenze (eliminazione).
Misure idonee:
_____
_____