

AVV. ANDREA STEFANELLI

AVV. SILVIA STEFANELLI

AVV. LAURA ASTI

AVV. FEDERICO BRESCHI

AVV. FABIO CARUSO

AVV. GASPARE CASTELLI

AVV. ADRIANO COLOMBAN

AVV. ALESSANDRA DELLI PONTI

AVV. ALESSIA DIOLI

AVV. RAFFAELE GAMMAROTA

AVV. ELEONORA LENZI

AVV. ANDREA MARINELLI

AVV. SILVIA PARI

AVV. ELEONORA PETTAZZONI

AVV. VITTORIA PIRETTI

AVV. MARIA LIVIA RIZZO

AVV. GIORGIA VERLATO

DOTT.SSA CAMILLA ANDERLINI

DOTT.SSA GABRILLE BAROUCH

DOTT.SSA NOEMI CONDITI

DOTT.SSA ALESSANDRA DI NUNZIO

DOTT.SSA ALICE GIANNINI

DOTT. FABIO MARINELLO

DOTT.SSA GIORGIA ROSATI

DOTT.SSA FEDERICA PUCARELLI

PROF. AVV. ALESSANDRA MAGLIARO *of counsel*

**CRUSCOTTO HEALTHDB**  
**OSSERVAZIONI DEL**  
**RESPONABILE PER LA PROTEZIONE DEI DATI DI**  
**CLICON SRL**

Member of CISQ Federation



Certificato n. 32945/15/S

Assistenza e consulenza  
legale giudiziaria e stragiudiziaria,  
per privati e aziende,  
sia nazionale che internazionale

**SEDE BOLOGNA**  
VIA AZZO GARDINO, 8/A - 40122 BOLOGNA  
TEL +39 051520315 - FAX +39 0510821641

**SEDE MILANO**  
VIA NINO BIXIO, 31 - 20129 MILANO  
TEL +02 87325559- FAX +39 0510821641

**SEDE VENEZIA**  
CASTELLO 2388 - 30122 VENEZIA

## INDICE

<b>I. PREMESSE</b> .....	<b>3</b>
<b>II. PROGETTI DI <i>OUTCOME RESEARCH</i></b> .....	Errore. Il segnalibro non è definito.
<b>III. TIPOLOGIA DI DATI TRATTATI</b> .....	<b>4</b>
<b>IV. RACCOLTA E TRASMISSIONE DEI DATI</b> .....	<b>4</b>
<b>V. INDIVIDUAZIONE DEI RUOLI PRIVACY</b> .....	<b>6</b>
<b>VI. COMUNICAZIONE A SOGGETTI TERZI</b> .....	<b>7</b>
<b>VII. DESCRIZIONE DEL TRATTAMENTO DEI DATI DA PARTE DI CLICON</b> .....	<b>7</b>
A. SUB RESPONSABILI ESTERNI .....	7
B. AUTORIZZATI AL TRATTAMENTO .....	8
C. RESPONSABILE PER LA PROTEZIONE DEI DATI .....	9
D. ESERCIZIO DIRITTI INTERESSATI .....	9
E. DATA BREACH .....	10
F. MODALITÀ DI TRATTAMENTO .....	10
G. MISURE DI SICUREZZA .....	13

Member of CISQ Federation



Certificato n. 32945/15/S  
Assistenza e consulenza  
legale giudiziaria e stragiudiziaria,  
per privati e aziende,  
sia nazionale che internazionale

## I. PREMESSE

Il presente documento, redatto dal Responsabile della protezione dei dati (di seguito anche solo DPO) di Clicon S.r.l. (di seguito anche solo Clicon), si pone l'obiettivo di analizzare i "CRUSCOTTI HEALTHDB", realizzati da Clicon, dal punto di vista della disciplina sulla protezione dei dati personali.

## II. CRUSCOTTO HEALTHDB

Il cruscotto di *business intelligence* è un software che permette il monitoraggio di un insieme di indicatori finalizzati ad evidenziare l'appropriatezza prescrittiva e l'aderenza al trattamento nell'ambito di diverse aree terapeutiche, con particolare riferimento all'assistenza farmaceutica territoriale ed ospedaliera. Il cruscotto, dunque, **ha l'obiettivo di supportare i decisori** (Regione, ASL ecc.) e/o gli operatori sanitari (MMG, Specialisti) nel processo di monitoraggio dell'aderenza delle modalità prescrittive rispetto agli standard terapeutici predefiniti e di valutazione degli effetti delle azioni finalizzate alla riduzione dello scostamento tra modalità prescrittive e standard terapeutici.

Dal punto di vista operativo:

- Clicon acquisisce i dati contenuti dei flussi amministrativi correnti (assistenza farmaceutica territoriale, farmaci in erogazione diretta, schede di dimissione ospedaliera, assistenza specialistica ambulatoriale, dipartimento di salute mentale, anagrafica degli assistibili e decessi, ecc.) o in altri archivi elettronici (laboratorio analisi, anatomia patologica, ecc.) generalmente disponibili presso le ASRL o le Regioni;<sup>[1]</sup><sup>[2]</sup>
- Clicon attribuisce ai dati raccolti una serie di indicatori di *performance*, progettati per valutare l'aderenza delle modalità prescrittive attuate in pratica clinica **rispetto a standard terapeutici predefiniti** (sulla base delle evidenze scientifiche, delle linee

Member of CISQ Federation



Certificato n. 32945/15/S

Assistenza e consulenza  
legale giudiziaria e stragiudiziaria,  
per privati e aziende,  
sia nazionale che internazionale

guida, delle note ministeriali, dei piani terapeutici), calcolabili in relazione a specifiche dimensioni contesti organizzativi;

- L'elaborazione di tali dati consente alla ASL/Regione di ottenere dati aggregati che forniscono informazioni necessarie ed idonee ad orientare le scelte di politica sanitaria o le decisioni organizzative interne.

### III. TIPOLOGIA DI DATI TRATTATI

Al fine dello svolgimento dei progetti di valutazione dei farmaci, Clicon tratta le seguenti categorie di dati personali:

- dati anagrafici e di contatto dei referenti delle strutture sanitarie;
- dati contabili e amministrativi delle strutture sanitarie che hanno affidato a Clicon lo svolgimento del progetto;
- dati relativi allo stato di salute dei pazienti, presenti all'interno degli archivi delle suddette strutture.

Per quanto attiene ai dati contabili e amministrativi, si precisa che gli stessi riguardano esclusivamente, e in ogni caso, persone giuridiche. Pertanto, ai sensi dell'art. 1, par. 1, del Regolamento (UE) 2016/679, a tale trattamento non si applica la disciplina sulla protezione dei dati personali in quanto riguarda dati di persone giuridiche.

### IV. RACCOLTA E TRASMISSIONE DEI DATI

Clicon riceve i dati sopra descritti dall'Ente, attraverso le modalità stabilite dallo stesso a seconda del tipo di progetto.

L'Ente, in base alle proprie esigenze e alla natura del progetto, decide a quale processo di de-identificazione sottoporre i dati personali.

Infatti, l'Ente, può decidere di rendere **anonimo** il dato, ossia di fare in modo che i dati non siano più in grado di risalire alla persona fisica cui si riferiscono.

Il Regolamento (UE) 2016/679 ha introdotto una disciplina che, rispetto alla precedente direttiva, definisce meglio la linea di demarcazione tra "dato personale" e "dato anonimo".

Circa il dato anonimo, il Considerando 26 stabilisce che:

*"[...] I principi di protezione dei dati **non dovrebbero pertanto applicarsi a informazioni anonime**, vale a dire informazioni che non si riferiscono a una persona fisica identificata o identificabile o a dati personali **resi sufficientemente anonimi da impedire o da non consentire più l'identificazione dell'interessato**. Il presente regolamento non si applica pertanto al trattamento di tali informazioni anonime, anche per finalità statistiche o di ricerca."*

Qualora l'Ente renda anonimo il dato personale, dunque, non dovrà applicarsi la disciplina relativa alla protezione dei dati personali.

L'Ente, poi, può decidere di pseudonimizzare i dati personali che comunica a Clicon.

Più esattamente l'art. 4, punto 5, del GDPR, definisce il processo di pseudonimizzazione come:

*"[...] il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni **aggiuntive**, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile"*

Un dato quindi può definirsi "dato pseudonimizzato" quando ha subito un trattamento all'esito del quale la riferibilità all'interessato può essere ottenuta solo con informazioni aggiuntive (detenute separatamente).

In questo ultimo caso, la disciplina sul trattamento dei dati personali è applicabile.

## **V. INDIVIDUAZIONE DEI RUOLI PRIVACY**

Ai sensi dell'art. 4, par. 1, n. 8, del GDPR responsabile del trattamento è:

*“la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo **che tratta dati personali per conto del titolare del trattamento**”*

Il responsabile è un soggetto esterno cui il titolare “affida”, tramite contratto (art. 28), un trattamento specifico, dandogli le relative istruzioni.<sup>[L][SEP]</sup>

Nonostante le finalità e le modalità debbano essere stabilite dal Titolare, il Responsabile, anche in base alla tipologia di attività che svolge, **potrà assumere una serie di decisioni autonome**. Ad esempio:<sup>1</sup>

- quale sistema IT o altro metodo utilizzare per raccogliere i dati personali;<sup>[L][SEP]</sup>
- in che modo conservare i dati personali;<sup>[L][SEP]</sup>
- i dettagli relativi alle misure di sicurezza;<sup>[L][SEP]</sup>
- i mezzi utilizzati per trasferire i dati personali da un'organizzazione a un'altra;
- i metodi per garantire i termini di conservazione dei dati personali;
- i mezzi utilizzati per cancellare e disporre dei dati.

Nel caso del cruscotto di *business intelligence*, Clicon svolge per conto delle ASL un trattamento di dati personali.<sup>[L][SEP]</sup>

In tale processo di trattamento infatti le ASL perseguono una finalità istituzionale (la valutazione della performance dell'Ente stesso) e determinano anche le modalità del trattamento.

**Clicon dovrà essere nominato Responsabile del trattamento dei dati, così come previsto dall'art. 28 del GDPR.**

<sup>1</sup> In questo senso si veda anche il documento che l'Autorità garante inglese (detta ICO) ha realizzato al fine di distinguere la figura del titolare da quella del responsabile del trattamento: ICO, Information Commissioner's Office, Data controllers and data processors: what the difference is and what the governance implications are.

Tenuto poi conto dell'elevato livello di specializzazione di Clicon nello svolgimento di tale attività si ritiene che quest'ultimo abbia la possibilità di determinare in modo autonomo diversi aspetti riguardanti il trattamento stesso.

## **VI. COMUNICAZIONE A SOGGETTI TERZI**

Clicon ha predisposto e tiene aggiornato l'elenco dei destinatari dei dati personali, che raccoglie indicando il fondamento giuridico per tale comunicazione.

Per quanto attiene, nello specifico, alle attività legate ai progetti di outcome research, Clicon dichiara che i dati, individuali e riconducibili a una numerosità inferiore a 4 soggetti, forniti dall'Ente non vengono comunicati a terzi.<sup>[1]</sup>

## **VII. DESCRIZIONE DEL TRATTAMENTO DEI DATI DA PARTE DI CLICON**

### **A. SUB RESPONSABILI ESTERNI**

Clicon ha predisposto opportuni documenti di nomina di altri responsabili e sub-responsabili esterni per il trattamento dei dati nel caso in cui risultasse necessario, nell'ambito delle proprie attività, avere necessità di tali figure. Tali nomine potranno essere effettuate previa comunicazione al titolare del trattamento e comprendono le seguenti indicazioni:

- Tipologia dei dati personali che il Responsabile ha la facoltà di trattare;
- Tassative finalità del trattamento, le quali hanno come obiettivo quello di tracciare il perimetro d'azione del Responsabile, il quale risulterà automaticamente titolare del trattamento (con tutte le conseguenze che ne derivano) qualora svolgesse un trattamento di dati personali al di fuori delle finalità tracciate;
- Durata del trattamento;

Member of CISQ Federation



Certificato n. 32945/15/S  
Assistenza e consulenza  
legale giudiziaria e stragiudiziaria,  
per privati e aziende,  
sia nazionale che internazionale

- Modalità del trattamento, le cui misure devono tenere conto dell'accordo di Responsabilità Esterna del trattamento e quindi delle modalità di trattamento decise dal Titolare del trattamento dei dati;
- Gestione sicurezza del dato, le cui misure devono tenere conto dell'accordo di responsabilità esterna al trattamento e quindi delle modalità di trattamento decise dal Titolare del trattamento;
- Gestione data breach, prevedendo un termine di tempo massimo entro il quale il sub-responsabile è tenuto a comunicare al responsabile una violazione di dati personali.

Nello specifico caso dei progetti di *valutazione del farmaco*, Clicon ha nominato quali Responsabili esterni del trattamento dei dati:

- Amazon Web Services (AWS), in qualità di fornitore di Amazon Elastic Compute Cloud (Amazon EC2).

## **B. AUTORIZZATI AL TRATTAMENTO**

Clicon ha individuato le persone autorizzate all'utilizzo dei dati e ne mantiene un elenco aggiornato all'interno del proprio Documento Programmatico sulla Sicurezza (DPS) che provvede ad aggiornare annualmente, ovvero più frequentemente laddove ne fosse individuata la necessità.

Inoltre, Clicon, al fine di creare una struttura al suo interno con l'obiettivo di conferire ruoli legati alla gestione del "sistema privacy" nonché di sensibilizzare l'organizzazione stessa ad un corretto e consapevole trattamento dei dati personali, ha deciso di:

- nominare un **Referente Privacy Generale**, il quale ha il compito di verificare costantemente la *compliance* dell'azienda alla normativa privacy e di comunicare con il DPO.

All'apice di tale strutturazione relativa all'organizzazione privacy vi è il **DPO**.



### **C. RESPONSABILE PER LA PROTEZIONE DEI DATI**

Vista la natura delle attività svolte, nonché la tipologia di dati trattati (dati relativi allo stato di salute dei pazienti), Clicon ha ritenuto di nominare il proprio Responsabile della Protezione dei dati (RDP) più spesso individuato come DPO (Data Protection Officer).

La suddetta scelta è stata compiuta anche al fine di garantire ai propri committenti e fornitori e agli Enti che usufruiscono dei suoi servizi di analisi dei dati (i quali trattano dati particolari e hanno, dunque, esigenze di riservatezza e sicurezza) **un trattamento dei dati personali che sia nel pieno rispetto della normativa privacy vigente.**

Tale figura per Clicon è:

**Avv. Silvia Stefanelli**

e-mail: dpo\_clicon@clicon.it

Tel. 051 0821641

### **D. ESERCIZIO DIRITTI INTERESSATI**

Gli interessati esercitano i propri diritti dei confronti del Titolare del trattamento, ossia, nel caso dei progetti di valutazione del farmaco, nei confronti dell'Ente.

Qualora sia necessario, l'Ente comunica tempestivamente a Clicon la richiesta pervenuta dall'interessato, **in modo tale che quest'ultimo possa impegnarsi a collaborare con l'Ente al fine di riscontrare entro i termini di legge le richieste degli interessati.**

Clicon monitora costantemente le richieste da parte degli interessati al fine di:

- generare uno storico delle richieste da parte degli interessati, che ha l'obiettivo di fornire riscontri sempre più tempestivi nei confronti dell'Ente;
- comprendere quali sono i casi che potenzialmente pongono maggiori problematiche, fornendo così supporto all'Ente nel miglioramento della gestione degli interessati.

Member of CISQ Federation



Certificato n. 32945/15/S

Assistenza e consulenza  
legale giudiziaria e stragiudiziaria,  
per privati e aziende,  
sia nazionale che internazionale

## **E. DATA BREACH**

**Violazione dei dati personali subita dal Titolare (Ente).** Nel caso in cui il Titolare subisca una violazione dei dati personali, Clicon, ove necessario, si impegna a collaborare con il primo al fine di reperire tutte le informazioni utili ex artt. 33 e 34 GDPR.

**Violazione dei dati personali subita dal Responsabile (Clicon).** Qualora sia Clicon a subire una violazione dei dati personali, lo stesso si impegna a notificare al Titolare, tramite una comunicazione PEC, senza indugio (e comunque entro una tempistica inferiore alle 72 ore), la violazione avvenuta, insieme a tutte le informazioni relative alla violazione di cui sia in possesso.

Clicon, al fine di garantire una corretta gestione delle violazioni dei dati personali, ha adottato:

- F. Una procedura di *Data Breach*;
- G. Un registro delle violazioni;
- H. Un *tool* di valutazione del rischio, per verificare l'opportunità delle notifiche di cui agli artt. 33 2 34 GDPR.

## **I. MODALITÀ DI TRATTAMENTO**

Qui di seguito si fornisce un elenco esemplificativo e non esaustivo delle modalità attraverso le quali Clicon tratta i dati personali per conto dell'Ente: <sup>[L]</sup><sub>[SEP]</sub>

- L'archiviazione dei dati è effettuata in database installati presso macchine virtuali fornite da Amazon Elastic Compute Cloud (Amazon EC2), una parte centrale della piattaforma di Cloud computing Amazon Web Services (AWS). <sup>[L]</sup><sub>[SEP]</sub>
- Le macchine virtuali sono configurate con Sistema Operativo Ubuntu 18.04.4 LTS (GNU/Linux 4.15.0-1058-aws x86\_64). <sup>[L]</sup><sub>[SEP]</sub>
- I dati pseudonimizzati sono raccolti all'interno del RDBMS 11.7 (Ubuntu 11.7-1.pgdg18.04+1). <sup>[L]</sup><sub>[SEP]</sub>

Member of CISQ Federation



Certificato n. 32945/15/S  
Assistenza e consulenza  
legale giudiziaria e stragiudiziaria,  
per privati e aziende,  
sia nazionale che internazionale

- L'utilizzo di macchine virtuali di questo tipo permette di avere grande scalabilità senza rinunciare alla sicurezza. In particolare, la piattaforma è conforme agli standard e alle normative di sicurezza, con particolare riferimento a determinati ambiti applicativi incluso il settore sanitario. Per maggiori dettagli e per visionare l'elenco delle certificazioni è possibile consultare il seguente link:  
<https://aws.amazon.com/it/compliance/>.
- Le "Service Level Agreement" (SLA) di Amazon garantiscono una disponibilità applicativa mensile del 99,95%, che potrebbe anche crescere in determinati scenari di deployment che coinvolgono diverse regioni geografiche.
- I server di Amazon utilizzati risiedono nel territorio della comunità europea.
- Le policy di backup prevedono che sia possibile configurare in maniera flessibile il numero e la periodicità delle copie, consistenti nel clonare gli interi dischi utilizzati dalle macchine virtuali, sia per quanto riguarda la parte applicativa, sia per quanto riguarda il database. L'infrastruttura in questo contesto garantisce un AFR (Annual Failure Rate) dello 0,1-0,5%, ovvero di molto superiore a quella relativa all'utilizzo di dischi fisici che si attesta attorno al 4%. Il Backup viene effettuato, in forma criptata, una volta al mese, e viene conservato lo storico relativo ai due mesi precedenti.
- Ogni accesso al database è tracciato mediante opportuno file di log in cui è possibile risalire a chi ha operato l'accesso e a quali attività ha effettuato.
- L'accesso è controllato mediante la fornitura di un codice utente ed una password, password che viene rinnovata con periodicità di sei mesi.
- L'area di Cloud di AWS, denominata S3, prevede la possibilità di criptare i singoli bucket (si tratta delle cartelle) utilizzati. Nel caso dell'eventuale bucket che potrebbe essere utilizzato per scambio di file con l'Ente, questa cartella sarà crittografata mediante l'algoritmo "industry-standard AES-256". Lo stesso

meccanismo di criptazione è applicato ai volumi contenenti dati nelle macchine virtuali configurate sul servizio AWS EC2. <sup>[L]</sup><sub>[SEP]</sub>

L'articolo 32, GDPR, pone l'obbligo per il Responsabile del Trattamento di: <sup>[L]</sup><sub>[SEP]</sub>

- mettere in atto misure tecniche ed organizzative adeguate a proteggere i dati personali al momento della determinazione dei mezzi di Trattamento sia all'atto <sup>[L]</sup><sub>[SEP]</sub> di Trattamento stesso (i.e., principio di "Privacy by Design"); <sup>[L]</sup><sub>[SEP]</sub>
- mettere in atto misure tecniche ed organizzative idonee a garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari al perseguimento delle specifiche finalità per cui sono raccolti e per il periodo strettamente necessario a tale fine (i.e., principio di "Privacy by Default").

In altri termini,

- per la privacy by design è richiesto al Responsabile di adottare e attuare misure tecniche e organizzative che tutelino i principi di protezione dei dati sin dal momento della progettazione oltre che nell'esecuzione del trattamento.
- per la privacy by default è richiesto al Responsabile di effettuare il Trattamento con modalità tali da garantire che il trattamento stesso sia limitato, per impostazione predefinita a monte, ai dati personali strettamente necessari al perseguimento delle finalità ed il trattamento sia altresì strutturato in modo tale da garantire il rispetto dei diritti e delle libertà degli interessati in modo automatico.

In quest'ottica, i dati trattati per la realizzazione delle analisi per la fornitura del cruscotto di business intelligence finalizzato alla valutazione di indicatori di appropriatezza, per la loro natura di dato pseudonimizzato, non rappresentano una criticità per quanto attiene questi aspetti, in ogni caso prima della sottoscrizione del contratto con l'Ente, Clicon, valuta rispetto al principio di Privacy by Design e Privacy by Default l'impatto che il nuovo trattamento potesse comportare in termini di rispetto della privacy.

Member of CISQ Federation



Certificato n. 32945/15/S

Assistenza e consulenza  
legale giudiziaria e stragiudiziaria,  
per privati e aziende,  
sia nazionale che internazionale

Inoltre, nel caso siano attivati:

- nuovi processi / attività aziendali per effetto dei quali sono introdotti dei nuovi trattamenti,
- nuovi servizi informatici che insistono su trattamenti esistenti o che introducono essi stessi un nuovo trattamento,
- cambiamenti significativi a livello organizzativo, con effetti su processi e relativi trattamenti


Clicon si impegna a valutare già in fase di progettazione e sviluppo il rispetto dei principi della privacy by design e by default.

Infine, nel caso di nuovi trattamenti possano rappresentare rischi elevati per i diritti e le libertà delle persone fisiche (in ragione della loro natura, portata o finalità, oppure quando i trattamenti possono procurare un danno economico o sociale importante), Clicon si impegna ad effettuare la Valutazione d’Impatto ex art. 35 GDPR.

## **J. MISURE DI SICUREZZA**

Clicon provvede ad aggiornare annualmente il proprio DPS (Documento Programmatico sulla Sicurezza) all’interno del quale sono raccolte tutte le misure messe in atto da Clicon stessa al fine di garantire la sicurezza dei propri sistemi di trattamento dei dati.

Tali misure riguardano, in estrema sintesi:

- gestione della password robusta (lunghezza minima, caratteri maiuscolo, minuscolo, numeri, caratteri speciali, ciclo di vita e obbligo di rinnovo); 
- produzione del file di log (tracciamento e registrazione delle operazioni compiute sui dati da parte di ogni utente);
- cifratura del canale di trasmissione dei dati: per gli accessi ai servizi WEB vengono usati canali *https* (es. per accesso alla piattaforma di Office 365), per l’accesso ai server virtuali mediante l’utilizzo di certificati di sicurezza in *ssh*;
- strategie di backup;

Member of CISQ Federation



Certificato n. 32945/15/S  
Assistenza e consulenza  
legale giudiziaria e stragiudiziaria,  
per privati e aziende,  
sia nazionale che internazionale

- strategie di *disaster recovery*;
- è stato costituito e viene mantenuto il registro del trattamento dei dati come  
previsto dal GDPR;
- viene gestito e mantenuto il censimento degli strumenti informatici in uso presso  
la struttura;
- viene gestito e mantenuto il registro dei software installati presso gli strumenti  
informatici di cui al punto precedente.

**Bologna, 9.07.2020**

Data Protection Officer

Avv. Silvia Stefanelli



Member of CISQ Federation



Certificato n. 32945/15/S  
Assistenza e consulenza  
legale giudiziaria e stragiudiziaria,  
per privati e aziende,  
sia nazionale che internazionale