

CAMELOT BIOMEDICAL SYSTEMS SRL

Personally Identifiable Information Policy

2	24/08/2026	Aggiornamento complessivo della politica in adeguamento alla ISO/IEC 27001	FUMAGALLI	SANTORO
1	13/11/2025	Prima versione	FUMAGALLI	SANTORO
REV	DATA	DESCRIZIONE	AUTORE	APPROVATORE
		Personally Identifiable Information Policy	Pagina 1 di 6	

Sommario

Campo di Applicazione.....	3
Premessa.....	3
Principi fondamentali per la protezione delle <i>PII</i>	3
Integrità e riservatezza.....	3
Protezione delle <i>PII</i> sin dalla fase di progettazione e per impostazione predefinita	3
Gestione dei diritti degli interessati	4
Gestione delle violazioni delle <i>PII</i> (<i>data breach</i>)	4
Misure operative per la protezione delle <i>PII</i>	4
Controllo degli accessi	4
Registrazione degli eventi (<i>logging</i>).....	4
Restituzione e cancellazione sicura.....	5
Obblighi contrattuali e gestione dei sub-fornitori.....	5
Formazione e consapevolezza	5

Campo di Applicazione

La presente politica definisce i principi, le misure e le responsabilità per la protezione delle *Informazioni Personali Identificabili (PII)* trattate da CAMELOT Biomedical Systems S.r.l. per conto dei propri clienti, in qualità di responsabile del trattamento. Lo scopo è garantire che ogni trattamento di *PII* avvenga in conformità con i requisiti contrattuali, le normative vigenti e gli standard internazionali, con riferimento anche alla norma ISO/IEC 27018.

Questa politica si applica a tutti/e i/le dipendenti, collaboratori/collaboratrici e processi aziendali coinvolti nel trattamento di *PII*.

Premessa

Il Regolamento Europeo sulla protezione dei dati personali (*General Data Protection Regulation "GDPR" Regulation 2016/679*), approvato dal Consiglio dell'Unione Europea e dal Parlamento Europeo, costituisce un quadro normativo unificato, valido per tutta l'Unione Europea, per la protezione dei dati personali che definisce le regole e i requisiti fondamentali per la tutela dei diritti correlati ai trattamenti di tali dati.

Con Informazioni Personali Identificabili (*PII*) si intende qualsiasi informazione che può essere utilizzata per identificare una persona specifica (per esempio: nomi, dati di contatto, cartelle cliniche, indirizzi IP ed estratti conto bancari).

Principi fondamentali per la protezione delle *PII*

A integrazione di quanto presente nella **Privacy Policy** a proposito di liceità, correttezza e trasparenza, limitazione delle finalità e minimizzazione dei dati, si aggiungono i seguenti punti:

Integrità e riservatezza

CAMELOT adotta misure tecniche e organizzative per proteggere l'integrità e la riservatezza delle *PII* da accessi non autorizzati, perdite, alterazioni o divulgazioni. Tutto il personale e i/le collaboratori/collaboratrici che hanno accesso alle *PII* sono vincolati da obblighi di riservatezza. Tali obblighi persistono anche dopo la cessazione del rapporto di lavoro.

L'/La **RSGSI (Responsabile del Sistema di Gestione per la Sicurezza delle informazioni)** è responsabile dell'implementazione e del monitoraggio delle misure di sicurezza, inclusa la crittografia dei dati in transito su reti pubbliche, come dettagliato nella **QSP_IS_ECM - Encryption and Cryptographic Key Management**.

Protezione delle *PII* sin dalla fase di progettazione e per impostazione predefinita

La protezione delle *PII* è un requisito integrato in ogni fase del ciclo di vita dello sviluppo del software e nella progettazione dei servizi. L'/La **RSGSI** deve assicurare che i principi di *privacy by design* e *privacy by default* siano applicati, trattando per impostazione predefinita solo i dati personali necessari per ogni specifica finalità.

Le metodologie e i controlli da adottare sono descritti nella **QSP-DesCon - Design Control**.

Gestione dei diritti degli interessati

CAMELOT si impegna a mettere a disposizione dei propri clienti le risorse tecniche e organizzative necessarie per consentire loro di adempiere agli obblighi relativi alla gestione e all'agevolazione dell'esercizio dei diritti degli interessati (accesso, rettifica, cancellazione, limitazione, opposizione e portabilità).

Il/La **PriM (Privacy Manager)**, in collaborazione con il/La **TM (Technologies' Manager)**, deve garantire che le soluzioni software e le piattaforme cloud consentano al cliente di gestire tali richieste in modo tempestivo ed efficace, come specificato negli accordi contrattuali.

Gestione delle violazioni delle *PII (data breach)*

In caso di violazione dei dati personali (*data breach*), come un accesso non autorizzato che comporti la perdita, la divulgazione o l'alterazione di *PII*, il/La **RSGSI** deve garantire che il cliente interessato sia informato senza ingiustificato ritardo. Le modalità e le tempistiche di notifica sono definite contrattualmente con ciascun cliente. Ogni incidente e le relative misure correttive devono essere documentati e gestiti secondo quanto stabilito nella **QSP-DPM - Data Protection Management**. Il/La **QM (Quality Manager)** è responsabile di conservare un registro degli incidenti che includa una descrizione dell'evento, le conseguenze e le azioni intraprese.

Misure operative per la protezione delle *PII*

Controllo degli accessi

L'accesso alle *PII* è limitato al personale autorizzato sulla base del principio del minimo privilegio e della necessità di sapere (*need-to-know*). Il/La **InfM (Infrastructure Manager)** deve assicurare che a ogni individuo autorizzato sia assegnato un ID utente univoco per l'identificazione, l'autenticazione e l'autorizzazione. Deve essere sempre rintracciabile la lista degli utenti autorizzati ad accedere ai sistemi che trattano *PII*. Le procedure di registrazione, modifica e revoca degli accessi sono formalizzate nella **QSP-IS_ECM - Encryption and Cryptographic Key Management**.

Registrazione degli eventi (*logging*)

Il/La **RSGSI** deve assicurare che siano implementati sistemi di registrazione (*logging*) per tracciare gli eventi rilevanti per la sicurezza delle *PII*. Devono essere registrate tutte le divulgazioni di *PII* a terze parti, specificando quali dati sono stati divulgati, a chi e in quale momento. Anche i tentativi di ripristino dei dati devono essere registrati, indicando la persona responsabile e una descrizione dei dati ripristinati. Tali registrazioni devono essere conservate in modo sicuro e rese disponibili per audit secondo quanto stabilito nella **QSP-DPM - Data Protection Management**.

Restituzione e cancellazione sicura

Al termine di un contratto, o su richiesta del cliente, CAMELOT deve provvedere alla restituzione, al trasferimento o alla cancellazione sicura delle *PII*. Il **PriM** è responsabile di rendere disponibile ai clienti, mettendola sul sito web, la **Information Retention & Disposal Policy**, che definisce le modalità di smaltimento e i periodi di conservazione temporanea per prevenire la perdita accidentale di dati. L'**InfMan** deve garantire che, quando uno spazio di archiviazione viene riassegnato, tutti i dati precedentemente presenti siano resi inaccessibili e cancellati in modo sicuro. Anche i file temporanei generati durante le normali operazioni devono essere cancellati in modo sicuro entro un periodo di tempo documentato.

Obblighi contrattuali e gestione dei sub-fornitori

I contratti con i clienti devono definire in modo chiaro le misure tecniche e organizzative minime per la protezione dei dati personali (*PII*), nonché le responsabilità e le istruzioni relative al trattamento. Tali misure non possono essere modificate o ridotte unilateralmente da CAMELOT.

L'eventuale ricorso a sub-fornitori (sub-responsabili) per il trattamento di dati personali (*PII*) deve essere preventivamente comunicato al cliente, che mantiene il diritto di opporsi. Il/La **PriM**, in collaborazione con il/La **PurM (Purchase Manager)**, garantisce che i contratti con i sub-fornitori prevedano obblighi di protezione dei dati almeno equivalenti, se non più stringenti, rispetto a quelli assunti da CAMELOT nei confronti dei propri clienti. Tali contratti devono inoltre indicare esplicitamente i Paesi in cui i dati possono essere trattati. Qualsiasi richiesta legalmente vincolante di divulgazione di *PII* da parte di un'autorità sarà comunicata al cliente, salvo che tale comunicazione sia vietata dalla normativa applicabile.

Formazione e consapevolezza

L'/La **HRM (Human Resources Manager)**, in collaborazione con il/La **PriM** e l'/la **RSGSI**, deve garantire che tutto il personale che tratta *PII* riceva una formazione adeguata e continua sui principi di protezione dei dati, sulle procedure di sicurezza e sugli obblighi derivanti dalla presente politica e dal *GDPR*. Tutto il personale deve essere consapevole delle proprie responsabilità in materia di protezione delle *PII* e degli obblighi di riservatezza. La partecipazione e l'efficacia della formazione devono essere documentate.

24/08/2026, Matteo Santoro (CEO)



	CAMELOT BIOMEDICAL SYSTEMS S.R.L.
	Sede Legale: Via Al Ponte Reale n. 2/20, 16124, Genova (GE)
	Codice Fiscale / Partita IVA: 01859390997 Capitale Sociale: 500.000,00 € i.v.
	Iscritta al Registro delle Imprese di Genova - REA: GE - 441013
	PEC: camelotbio@legalmail.it E-mail: info@camelotbio.com Web: https://www.camelotbio.com/