aggiornamento 14/07/2025

Annex 1 all'Accordo sul trattamento dei dati personali (DPA) – Nanosystems S.r.l.

MISURE DI SICUREZZA TECNICHE E ORGANIZZATIVE (TOM)

A) Misure organizzative:

· *Nomina dei sub-responsabili:* Nanosystems potrà avvalersi, quale responsabile del trattamento, di sub-responsabili del trattamento per lo svolgimento delle proprie attività nel rispetto del contratto sottoscritto dall'utente e del DPA.
I sub-responsabili del trattamento sono stati comunicati al momento della sottoscrizione del suddetto contratto, i quali presentano sufficienti garanzie di adeguatezza in relazione alla tutela dei diritti e della libertà degli interessati.
Qualora Nanosystems decidesse di avvalersi di ulteriori sub-responsabili o di sostituire quelli precedenti, modificando i relativi accordi, provvederà a richiedere l'autorizzazione al Titolare del trattamento in conformità all'art. 28 del Regolamento (UE) 2016/679 (GDPR).

· *Nomine degli Autorizzati:* nomina rilasciata a persone fisiche, espressamente designate, autorizzate a compiere, mediante l'attribuzione di specifici compiti e funzioni, operazioni di trattamento dal Titolare o dal responsabile, sotto la loro autorità; tali nomine sono registrate appositamente nel registro accessibilità dei dati in possesso di Nanosystems.

· *Conservazione cartacea in luoghi protetti:* i documenti contenenti dati personali particolarmente sensibili, ove trattati in formato cartaceo, sono conservati in contenitori fisici protetti (es. armadietti o cassetti chiusi a chiave) collocati in aree ad accesso limitato.
L'accesso a tali documenti è consentito esclusivamente a personale autorizzato, previamente individuato dalla Società.
La Società adotta e mantiene un registro degli accessi fisici a tali contenitori, al fine di garantire la tracciabilità degli accessi e il rispetto del principio di integrità e riservatezza previsto dall'art. 32 GDPR.

· *Regolamento aziendale sulla sicurezza e Privacy:* Nanosystems ha adottato un Regolamento interno sulla protezione dei dati personali con l'obiettivo di tutelare i dati personali trattati e prevenire i rischi connessi al trattamento, in conformità ai principi stabiliti dalla normativa europea e nazionale in materia di privacy.
Il Regolamento definisce le procedure interne per l'adempimento agli obblighi previsti dal D.Lgs. 30 giugno 2003, n. 196 e successive modifiche (Codice della Privacy), nonché dal GDPR, con riferimento al trattamento dei dati personali in ambito aziendale.
In particolare, individua:

- le disposizioni operative interne applicabili ai trattamenti effettuati dalla Società;
- i ruoli e le responsabilità delle figure coinvolte;
- gli adempimenti da osservare in conformità alle decisioni e ai provvedimenti dell'Autorità Garante per la protezione dei dati personali.

In aggiunta, Nanosystems ha adottato una politica interna sulla sicurezza delle informazioni, volta a definire le misure organizzative, tecniche e procedurali per garantire la riservatezza, l'integrità e la disponibilità dei dati trattati.

· *Procedura modifica credenziali:* Nanosystems adotta una procedura sicura per la gestione e la modifica delle credenziali di accesso ai servizi aziendali collegati al dominio corporate.
Tutti i dipendenti accedono ai sistemi tramite account utente nominativi; le relative password possono essere ripristinate esclusivamente dal Responsabile della Sicurezza o da personale espressamente autorizzato.
È attiva una policy interna per la generazione delle credenziali, che stabilisce:
- requisiti minimi di complessità (lunghezza, caratteri speciali, maiuscole, numeri);
- divieto di riutilizzo delle ultime password;
- scadenza obbligatoria delle credenziali ogni 90 giorni;
- obbligo di modifica immediata in caso di sospetto accesso non autorizzato.

Tali misure si applicano a tutti i servizi interni collegati al dominio aziendale, inclusi strumenti di posta elettronica, ambienti cloud, VPN, strumenti di amministrazione e gestione remota.

· *Procedura databreach:* Nanosystems ha predisposto un manuale per la gestione di Data Breach, che ha l'obiettivo di definire ruoli, responsabilità e principali modalità operative adottate per proteggere i dati personali e gestire i rischi che incombono sul trattamento degli stessi, in coerenza con i principi definiti dal GDPR.
Nel caso in cui un soggetto appartenente alla data protection governance di Nanosystems o ad uno degli altri Uffici delle società medesima rilevi una perdita accidentale di dati (i.e. smarrimento PC, USB ovvero invio di e-mail a destinatari errati) ovvero un attacco fraudolento all'integrità dei propri sistemi ovvero comunque una violazione di riservatezza o confidenzialità, una violazione di integrità o una violazione di disponibilità, ne dà comunicazione tempestivamente al Titolare del trattamento. Esiste, pertanto, una procedura per la gestione delle violazioni rilevate che possano incidere sui dati personali degli interessati che si basa sulla distribuzione dei ruoli secondo la competenza, la verifica dei potenziali pregiudizi e la valutazione del rischio conseguente alla violazione dei dati personali, la gestione delle contromisure da adottare, così come la modalità di comunicazione al Cliente e l'adozione degli adempimenti connessi ai sensi della normativa privacy.

· *Procedura Diritti degli interessati:* qualora Nanosystems ricevesse richieste relative all'esercizio di diritti da parte di interessati con riferimento a dati personali che analizza ed elabora per conto del Titolare del trattamento, dovrà inviarle, il prima possibile, a quest'ultimo, il quale gestirà le predette richieste. Il Responsabile del trattamento, ovvero Nanosystems, aiuterà il Titolare procurandogli tutte le informazioni relative ai servizi gestiti da Nanosystems in base al presente accordo ed inviterà l'interessato a rivolgersi al Titolare del trattamento con lo scopo di esercitare i propri diritti, sottolineando la propria posizione di Responsabile del trattamento. Nanosystems si impegna a gestire in modo adeguato i diritti degli interessati.
Nel caso in cui il Titolare del trattamento debba soddisfare domande relative ad

interessati per l'esercizio dei loro diritti con riferimento a dati personali oggetto del presente accordo, Nanosystems procurerà le informazioni richieste, se in suo possesso, in base al presente accordo, in relazione ai servizi acquistati e utilizzati dal Titolare del trattamento. In ogni caso, quest'ultimo tratterà direttamente la suddetta domanda.
Nell'eventualità che sia necessario da parte del Titolare del trattamento soddisfare istanze di portabilità dei dati personali, il Responsabile del trattamento fornirà, solamente per i servizi acquistati dal Titolare del trattamento, le informazioni necessarie per estrarli in formato concorde alla normativa sulla privacy e se ciò sia ragionevolmente possibile. Se il Titolare del trattamento richieda invece l'assistenza tecnica essenziale per attuare la suddetta estrazione, Nanosystems ne considererà la fattibilità tecnica e concorderà con il primo, le procedure relative e i costi a carico del Titolare del trattamento.

· *Istruzione e formazione agli autorizzati:* Il Responsabile del trattamento del trattamento prevede una formazione pratica, successiva alla teoria e a un test valutativo delle competenze acquisite, nella quale simulare, in ambiente sicuro, tutte quelle criticità riscontrabili durante l'attività lavorativa che potrebbero comportare un incidente sui dati.

· *Revisioni e aggiornamenti:* Le presenti misure tecniche e organizzative sono soggette a revisione periodica. Eventuali aggiornamenti saranno comunicati tempestivamente al Titolare del trattamento. Le misure saranno adeguate in funzione dell'evoluzione dei rischi e delle tecnologie disponibili.

B) Misure tecniche

· *Autenticazione:* Il trattamento di dati personali con strumenti elettronici è consentito agli incaricati dotati di credenziali di autenticazione che consentano il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti. Ad ogni incaricato sono assegnate o associate individualmente una o più credenziali per l'autenticazione. Con le istruzioni impartite agli incaricati è prescritto di adottare le necessarie cautele per assicurare la segretezza della componente riservata della credenziale e la diligente custodia dei dispositivi in possesso ed uso esclusivo dell'incaricato. Sono impartite istruzioni agli incaricati per non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento.

· *Autorizzazione:* Solamente le persone autorizzate hanno accesso al sistema che raccoglie e tratta i dati personali. Nanosystems utilizza livelli di autorizzazioni multipli nel momento in cui si concede l'accesso ai sistemi. Le autorizzazioni vengono aggiornate regolarmente.

· *Cifratura dei dati:* Nanosystems codifica le informazioni ricavate dai dati personali, affinché non possano essere comprese da soggetti terzi, così da garantire la confidenzialità. Questi sistemi si basano su algoritmi e protocolli informatici che soddisfano gli standard internazionali.

- *Separazione*: La pratica di mantenere distinti sistemi, dati o ambienti per limitare l'accesso e ridurre i rischi.

- *Firewall:* Nanosystems utilizza dispositivi fisici e logici di protezione perimetrale dell'infrastruttura IT, per prevenire gli attacchi informatici e le intrusioni dall'esterno da parte di terzi.

- *Business Continuity:* Piano e soluzioni per ripristinare dati e sistemi in seguito a un evento catastrofico.

- *Disaster Recovery:* Strategie e misure per assicurare la continuità operativa anche in caso di eventi avversi (guasti, attacchi, disastri).

- *Intrusion detection:* Nanosystems adotta strumenti che sono in grado di monitorare il traffico in entrata e in uscita da una rete, affinché vengano rilevate tutte le attività sospette o attacchi informatici.

- *Pseudonimizzazione:* Nanosystems utilizza la pseudonimizzazione qualora non pregiudichi l'efficienza delle procedure e/o laddove sia necessaria la protezione dei dati in funzione della finalità del trattamento. Dove possibile, come parte del processo di analisi statistiche, viene utilizzata l'anonimizzazione. Nanosystems segue una procedura per valutare la condivisione interna dei dati e utilizza la pseudonimizzazione per limitare l'uso di dati personali per certi scopi.

- *Backup e ripristino:* Il Responsabile del trattamento prevede backup automatizzati giornalieri ed effettua test periodicamente, i quali vengono registrati.

- *Verifica delle misure di sicurezza:* Nanosystems esegue audit di sicurezza su base periodica in modo da verificare l'efficacia delle misure tecniche e organizzative in maniera costante.

- *Cancellazione e restituzione dei dati:* Il Responsabile del trattamento ha previsto procedure standard per la restituzione o cancellazione sicura dei dati alla cessazione del rapporto contrattuale.