Actualización 14/07/2025

Anexo 1 al Acuerdo sobre el tratamiento de datos personales (DPA) – Nanosystems S.r.l.

MEDIDAS DE SEGURIDAD TÉCNICAS Y ORGANIZATIVAS (TOM)

A) Medidas organizativas:

· Nombramiento de los subencargados del tratamiento: Nanosystems podrá recurrir, en calidad de encargado del tratamiento, a subencargados del tratamiento para el desempeño de sus actividades, de conformidad con el contrato suscrito por el usuario y el DPA.
Los subencargados del tratamiento se comunicaron en el momento de la firma del contrato mencionado, y ofrecen garantías suficientes en relación con la protección de los derechos y libertades de los interesados.
Si Nanosystems decidiera recurrir a otros subencargados o sustituir a los anteriores, modificando los acuerdos correspondientes, solicitará la autorización del responsable del tratamiento de conformidad con el artículo 28 del Reglamento (UE) 2016/679 (RGPD).

· Nombramiento de los autorizados: nombramiento otorgado a personas físicas, expresamente designadas, autorizadas para realizar, mediante la asignación de tareas y funciones específicas, operaciones de tratamiento por parte del responsable o del encargado, bajo su autoridad; dichos nombramientos se registran específicamente en el registro de accesibilidad de los datos en poder de Nanosystems.

· Conservación en papel en lugares protegidos: los documentos que contienen datos personales especialmente sensibles, cuando se tratan en formato papel, se conservan en contenedores físicos protegidos (por ejemplo, armarios o cajones cerrados con llave) situados en zonas de acceso restringido.
El acceso a dichos documentos está permitido exclusivamente al personal autorizado, previamente identificado por la empresa.
La empresa adopta y mantiene un registro de los accesos físicos a dichos contenedores, con el fin de garantizar la trazabilidad de los accesos y el cumplimiento del principio de integridad y confidencialidad previsto en el artículo 32 del RGPD.

· Normativa de la empresa sobre seguridad y privacidad: Nanosystems ha adoptado una normativa interna sobre protección de datos personales con el objetivo de proteger los datos personales tratados y prevenir los riesgos relacionados con el tratamiento, de conformidad con los principios establecidos por la normativa europea y nacional en materia de privacidad.
El Reglamento define los procedimientos internos para el cumplimiento de las obligaciones previstas en el Decreto Legislativo n.º 196, de 30 de junio de 2003, y sus modificaciones posteriores (Código de Privacidad), así como en el RGPD, en lo que se refiere al tratamiento de datos personales en el ámbito empresarial.
En particular, identifica:

- las disposiciones operativas internas aplicables a los tratamientos realizados por la Sociedad;
- las funciones y responsabilidades de las personas implicadas;
- los requisitos que deben cumplirse de conformidad con las decisiones y medidas de la Autoridad Garante para la Protección de Datos Personales.

Además, Nanosystems ha adoptado una política interna de seguridad de la información, destinada a definir las medidas organizativas, técnicas y procedimentales para garantizar la confidencialidad, integridad y disponibilidad de los datos tratados.

· Procedimiento de modificación de credenciales: Nanosystems adopta un procedimiento seguro para la gestión y modificación de las credenciales de acceso a los servicios empresariales vinculados al dominio corporativo.
Todos los empleados acceden a los sistemas a través de cuentas de usuario nominativas; las contraseñas correspondientes solo pueden ser restablecidas por el responsable de seguridad o por personal expresamente autorizado.
Existe una política interna para la generación de credenciales, que establece:

- requisitos mínimos de complejidad (longitud, caracteres especiales, mayúsculas, números);
- prohibición de reutilizar las últimas contraseñas;
- caducidad obligatoria de las credenciales cada 90 días;
- obligación de modificación inmediata en caso de sospecha de acceso no autorizado.

Estas medidas se aplican a todos los servicios internos relacionados con el dominio de la empresa, incluidos las herramientas de correo electrónico, entornos en la nube, VPN, herramientas de administración y gestión remota.

· Procedimiento de violación de datos: Nanosystems ha elaborado un manual para la gestión de violaciones de datos, cuyo objetivo es definir las funciones, las responsabilidades y las principales modalidades operativas adoptadas para proteger los datos personales y gestionar los riesgos que pesan sobre su tratamiento, de conformidad con los principios definidos por el RGPD.
En caso de que una persona perteneciente a la gobernanza de protección de datos de Nanosystems o a una de las otras oficinas de la misma empresa detecte una pérdida accidental de datos (por ejemplo, pérdida de un ordenador, USB o envío de correos electrónicos a destinatarios erróneos) o un ataque fraudulento a la integridad de sus sistemas o, en cualquier caso, una violación de la confidencialidad, la integridad o la disponibilidad, lo comunicará sin demora al responsable del tratamiento.
Por lo tanto, existe un procedimiento para gestionar las violaciones detectadas que puedan afectar a los datos personales de los interesados, basado en la distribución de funciones según la competencia, la verificación de los posibles perjuicios y la evaluación del riesgo derivado de la violación de los datos personales, la gestión de las contramedidas que deben adoptarse, así como la forma de comunicación al Cliente y la adopción de las medidas relacionadas con la normativa de privacidad.

· Procedimiento de derechos de los interesados: en caso de que Nanosystems reciba solicitudes relativas al ejercicio de derechos por parte de interesados en relación con

los datos personales que analiza y trata por cuenta del Responsable del tratamiento, deberá remitirlas lo antes posible a este último, quien se encargará de gestionar dichas solicitudes. El Encargado del tratamiento, es decir, Nanosystems, ayudará al Responsable proporcionándole toda la información relativa a los servicios gestionados por Nanosystems en virtud del presente acuerdo e invitará al interesado a dirigirse al Responsable del tratamiento con el fin de ejercer sus derechos, subrayando su condición de Encargado del tratamiento. Nanosystems se compromete a gestionar adecuadamente los derechos de los interesados.
En caso de que el Responsable del tratamiento deba responder a preguntas relativas a los interesados para el ejercicio de sus derechos en relación con los datos personales objeto del presente acuerdo, Nanosystems facilitará la información solicitada, si obra en su poder, en virtud del presente acuerdo, en relación con los servicios adquiridos y utilizados por el Responsable del tratamiento. En cualquier caso, este último tratará directamente dicha solicitud.
En caso de que sea necesario que el Responsable del tratamiento satisfaga solicitudes de portabilidad de los datos personales, el Encargado del tratamiento proporcionará, únicamente para los servicios adquiridos por el Responsable del tratamiento, la información necesaria para extraerlos en un formato acorde con la normativa de privacidad y si ello es razonablemente posible. Si, por el contrario, el Responsable del tratamiento solicita la asistencia técnica esencial para llevar a cabo dicha extracción, Nanosystems considerará su viabilidad técnica y acordará con el primero los procedimientos correspondientes y los costes a cargo del Responsable del tratamiento.

· Instrucción y formación de las personas autorizadas: El Encargado del tratamiento prevé una formación práctica, tras la teoría y una prueba de evaluación de las competencias adquiridas, en la que se simularán, en un entorno seguro, todas las situaciones críticas que puedan surgir durante la actividad laboral y que puedan dar lugar a un incidente con los datos.

· Revisiones y actualizaciones: Las presentes medidas técnicas y organizativas están sujetas a revisión periódica. Cualquier actualización se comunicará sin demora al Responsable del tratamiento. Las medidas se adaptarán en función de la evolución de los riesgos y de las tecnologías disponibles.

B) medidas técnicas

· Autenticación: El tratamiento de datos personales con instrumentos electrónicos está permitido a los encargados que dispongan de credenciales de autenticación que permitan superar un procedimiento de autenticación relativo a un tratamiento específico o a un conjunto de tratamientos. A cada persona autorizada se le asigna o se le asocia individualmente una o varias credenciales para la autenticación. En las instrucciones impartidas a las personas autorizadas se prescribe la adopción de las precauciones necesarias para garantizar la confidencialidad del componente reservado de la credencial y la custodia diligente de los dispositivos en posesión y uso exclusivo del autorizado. Se dan instrucciones a los autorizados para que no dejen

desatendidos y accesibles los instrumentos electrónicos durante una sesión de tratamiento.

· Autorización: Solo las personas autorizadas tienen acceso al sistema que recopila y trata los datos personales. Nanosystems utiliza múltiples niveles de autorización al conceder el acceso a los sistemas. Las autorizaciones se actualizan periódicamente.

· Cifrado de datos: Nanosystems codifica la información obtenida a partir de los datos personales, de modo que no pueda ser comprendida por terceros, garantizando así la confidencialidad. Estos sistemas se basan en algoritmos y protocolos informáticos que cumplen con los estándares internacionales.

· Separación: La práctica de mantener sistemas, datos o entornos separados para limitar el acceso y reducir los riesgos.

· Cortafuegos: Nanosystems utiliza dispositivos físicos y lógicos de protección perimetral de la infraestructura informática para prevenir ataques informáticos e intrusiones externas por parte de terceros.

· Continuidad del negocio: Plan y soluciones para restaurar datos y sistemas tras un evento catastrófico.

· Recuperación ante desastres: estrategias y medidas para garantizar la continuidad operativa incluso en caso de eventos adversos (fallos, ataques, desastres).

· Detección de intrusiones: Nanosystems adopta herramientas capaces de supervisar el tráfico entrante y saliente de una red, con el fin de detectar cualquier actividad sospechosa o ataque informático.

· *Seudonimización:* Nanosystems utiliza la seudonimización cuando no afecta a la eficacia de los procedimientos y/o cuando es necesaria la protección de los datos en función de la finalidad del tratamiento. Siempre que es posible, como parte del proceso de análisis estadístico, se utiliza la anonimización. Nanosystems sigue un procedimiento para evaluar el intercambio interno de datos y utiliza la seudonimización para limitar el uso de datos personales para determinados fines.

· Copias de seguridad y recuperación: El responsable del tratamiento prevé copias de seguridad automáticas diarias y realiza pruebas periódicas, que se registran.

· Verificación de las medidas de seguridad: Nanosystems realiza auditorías de seguridad periódicas para verificar la eficacia de las medidas técnicas y organizativas de forma constante.

· Eliminación y devolución de datos: El Encargado del tratamiento ha establecido procedimientos estándar para la devolución o eliminación segura de los datos al término de la relación contractual.