POLÍTICA DE PROTECCIÓN DE DATOS PERSONALES

Política de Protección de Datos adoptada en transposición del Reglamento (UE) 2016/679, con el fin de garantizar y proteger los derechos y libertades fundamentales de las personas físicas.

TÍTULO	Política de Protección de Datos
FECHA DE APLICACIÓN	10/06/2026
Autor	Delegado de Protección de Datos
Revisado por	Área de RR. HH. de Technacy
Aprobado por	Consejero Delegado de Technacy

HISTORIAL DE REVISIONES

Versión	Fecha	Revisado por	Naturaleza de los cambios
1.0	21 de mayo de 2021	DPD – Studio Paci & C.	Primera emisión
2.0	Junio de 2026	DPD – Avv. Elisa Rosso	Integración con el procedimiento de Protección de Datos de alto nivel; ampliación de funciones, responsabilidades, definiciones y disposiciones detalladas; armonización general del documento.

ÍNDICE

1. INTRODUCCIÓN

Technacy S.r.l. (en adelante también “Technacy”, “la Empresa” o “la Organización”) presta la máxima atención a la protección de los datos personales tratados en el marco de sus actividades. Este compromiso se extiende a los empleados, clientes, potenciales clientes, proveedores, socios comerciales y a cualquier otra persona que entre en contacto con la Empresa.

La presente Política de Protección de Datos Personales (en adelante también la “Política”) tiene por objeto proporcionar un marco de referencia común, coherente y armonizado para la protección de los datos personales, adoptando estándares homogéneos de seguridad y conformidad con el Reglamento (UE) 2016/679 (el “RGPD”), así como con los principios, directrices y buenas prácticas en materia de protección de datos personales aplicables a los contextos operativos de la Empresa.

En particular, el presente documento define los requisitos, obligaciones y comportamientos que deben adoptar el Responsable del tratamiento, así como las funciones internas en materia de privacidad – como el Delegado de Protección de Datos (DPD), los Responsables internos (de privacidad) del tratamiento, las personas autorizadas/encargadas y los Administradores de sistemas – para garantizar un tratamiento lícito, correcto y seguro de los datos personales y evitar la comunicación y/o difusión no autorizada de los mismos.

La Política se aplica tanto a los tratamientos realizados por la Empresa en calidad de “Responsable del tratamiento” como a los realizados en calidad de “Encargado del tratamiento” por cuenta de su clientela, y tiene como objetivo garantizar a todos los interesados una protección adecuada mediante la adopción de un Sistema de gestión de los datos personales, en el respeto de los derechos y libertades fundamentales de las personas.

2. OBJETO Y ÁMBITO DE APLICACIÓN

El objeto del presente documento es describir la política de la Organización, las modalidades y los procedimientos generales para el tratamiento, así como para la seguridad y la confidencialidad de los datos y de la información.

El presente documento se aplica a todos los tratamientos de datos personales realizados por Technacy S.r.l., ya sea directamente o a través de proveedores externos de servicios, así como a las actividades gestionadas por cuenta de terceros. La Política se aplica a todo el personal interno y se comparte con los terceros que colaboran en la gestión de la información, así como a todos los procesos y recursos implicados en el diseño, desarrollo, puesta en marcha y prestación continuada de los servicios.

Entran dentro del ámbito de aplicación:

- todos los tratamientos realizados en calidad de Responsable o de Encargado del tratamiento;
- las actividades de tratamiento realizadas en el contexto de servicios prestados a clientes públicos y privados;
- los tratamientos realizados en soportes digitales, en papel o mixtos.

Quedan excluidos del ámbito de la presente Política:

- los tratamientos de datos referidos a personas jurídicas (por ejemplo, sociedades con personalidad jurídica), incluidos el nombre, la forma jurídica y los datos de contacto corporativos;
- los tratamientos de datos anonimizados de manera irreversible, de modo que no permitan (ni siquiera indirectamente) la identificación de un interesado.

2.1. Actividades de la Empresa

La Política se aplica a las actividades principales y accesorias del Responsable del tratamiento, descritas en el Registro de Actividades de Tratamiento. La Empresa se dedica al desarrollo de software, aplicaciones e integraciones, en particular en el ámbito de los servicios accesorios a las telecomunicaciones.

Las operaciones de gestión, desarrollo de software y pruebas se llevan a cabo, cuando es técnicamente posible, en un entorno dedicado y separado del sistema informático utilizado para el tratamiento de los datos personales; en las actividades de prueba se utilizan, por lo general, datos ficticios y no datos reales. En los casos en que esto no sea posible, se establecen procedimientos específicos para la protección de los datos personales utilizados en las pruebas y en el desarrollo de software.

3. REFERENCIAS NORMATIVAS Y PROCEDIMIENTOS INTERNOS

La presente Política se basa en las siguientes referencias normativas y documentos internos.

3.1. Referencias normativas

- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, por el que se deroga la Directiva 95/46/CE (en adelante también “RGPD”);
- Decreto Legislativo italiano n.º 196, de 30 de junio de 2003 – Código en materia de protección de datos personales, y sus modificaciones posteriores;
- Decreto Legislativo italiano n.º 101, de 10 de agosto de 2018 – Disposiciones para la adecuación de la normativa nacional al RGPD;
- Resolución de la Autoridad italiana de Protección de Datos de 27 de noviembre de 2008 – “Medidas y disposiciones prescritas a los responsables de los tratamientos realizados con instrumentos electrónicos en relación con la atribución de las funciones de administrador de sistemas”;
- Resoluciones y Directrices de la Autoridad italiana de Protección de Datos en materia de marketing directo y lucha contra el spam, videovigilancia, tratamiento de los datos de los trabajadores y uso del correo electrónico e internet;
- Directrices del Grupo de Trabajo del artículo 29 y del Comité Europeo de Protección de Datos (CEPD) en materia de consentimiento, portabilidad de los datos, DPD, autoridad de control principal, EIPD, decisiones automatizadas y elaboración de perfiles, y notificación de brechas de seguridad;
- Ley italiana n.º 48, de 18 de marzo de 2008 – Ratificación y ejecución del Convenio del Consejo de Europa sobre la Ciberdelincuencia (Budapest, 23 de noviembre de 2001).

3.2. Procedimientos y documentos internos

La presente Política se completa y se aplica mediante los siguientes documentos internos, a los que se remite íntegramente para el detalle operativo:

- Procedimiento corporativo de gestión de los derechos de los interesados;
- Procedimiento (política) corporativo de conservación de datos;
- Procedimiento corporativo de brechas de seguridad;
- Procedimiento para la realización de EIPD;
- Contratos/cláusulas de nombramiento como Encargado del tratamiento conforme al art. 28 RGPD;
- Reglamento informático.

4. TÉRMINOS Y DEFINICIONES

Dato personal común: cualquier información relativa a una persona física identificada o identificable (el "interesado"). El dato personal puede referirse únicamente a una persona física e incluye también a los empresarios individuales y a los profesionales por cuenta propia, pero no incluye los datos de las personas jurídicas. La dirección de correo electrónico corporativa vinculada a una persona concreta (por ejemplo, nombre.apellido@technacy.it) es un dato personal, mientras que la dirección de correo electrónico genérica (por ejemplo, info@technacy.it) no se considera un dato personal. En caso de duda sobre si una información constituye un dato personal, cada empleado debe consultar a su Responsable interno (de privacidad).

Categorías especiales de datos: datos personales que revelen el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, la afiliación sindical, así como datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o a la vida sexual o la orientación sexual de una persona física. Incluyen, en particular, los datos relativos a la salud, los datos genéticos y los datos biométricos. En caso de tratamiento de estas categorías, el RGPD prevé obligaciones mayores y específicas.

Datos judiciales: datos personales aptos para revelar resoluciones judiciales firmes, el registro de sanciones administrativas derivadas de delitos y las correspondientes causas pendientes, o la condición de imputado o investigado a efectos de los arts. 60 y 61 del Código de Procedimiento Penal italiano.

Datos de riesgo: datos cuyo tratamiento presenta riesgos específicos para los derechos y libertades fundamentales y para la dignidad del interesado; incluyen, en particular, los datos de geolocalización y los datos de videovigilancia.

Interesado: la persona física a la que se refieren los datos personales (por ejemplo, empleados, proveedores, clientes, usuarios, visitantes de los sitios web, otras personas).

Consentimiento del interesado: toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta el tratamiento de datos personales que le conciernen. El consentimiento debe obtenerse únicamente sobre la base de los modelos previamente aprobados por el Responsable interno (de privacidad); en caso de duda, es necesario consultar al Responsable competente o al DPD.

Elaboración de perfiles: todo tratamiento automatizado de datos personales consistente en utilizar dichos datos para evaluar determinados aspectos personales de una persona física (rendimiento profesional, situación económica, salud, preferencias, intereses, fiabilidad, comportamiento, ubicación o movimientos). Se considera una actividad "de riesgo" a efectos del RGPD.

Seudonimización: el tratamiento de datos personales de manera que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure separadamente y esté sujeta a medidas técnicas y organizativas adecuadas.

Responsable del tratamiento: la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento de datos personales.

Responsable interno (de privacidad) del tratamiento: persona formalmente designada que tiene el control y la responsabilidad de los tratamientos realizados en su área/unidad de competencia, garantizando el cumplimiento de la normativa y un acceso adecuado a los datos personales y a los sistemas informáticos.

Delegado de Protección de Datos (DPD): la persona nombrada por la Empresa de conformidad con los arts. 37 y siguientes del RGPD, implicada en todas las cuestiones relativas al tratamiento de datos personales en las que la Empresa actú como Responsable o Encargado.

Personas autorizadas/encargadas del tratamiento: personas físicas (empleados y/o otros terceros) autorizadas a realizar operaciones de tratamiento de datos personales de los que la Empresa sea

Responsable.

Administrador de sistemas: figura profesional dedicada a la gestión o al mantenimiento de las infraestructuras de procesamiento o de sus componentes mediante los cuales se realizan tratamientos de datos personales (sistemas de gestión de bases de datos, software de base complejo, sistemas de correo electrónico y telefonía, redes y sistemas de seguridad), en la medida en que permitan intervenir sobre los datos personales.

Encargado del tratamiento (externo): la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento (por ejemplo, gestorías laborales, proveedores de infraestructura informática).

Tercero: la persona física o jurídica, autoridad pública, servicio u otro organismo distinto del interesado.

Tratamiento: cualquier operación o conjunto de operaciones realizadas sobre datos personales, con o sin medios automatizados, como la recogida, el registro, la organización, la estructuración, la conservación, la adaptación o modificación, la extracción, la consulta, el uso, la comunicación, el cotejo, la limitación, la supresión o la destrucción.

Violación de datos personales (brecha de seguridad): la violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.

Difusión: dar a conocer los datos personales a un número indeterminado de sujetos, en cualquier forma, incluso poniéndolos a disposición o permitiendo su consulta.

Comunicación: dar a conocer los datos personales a uno o varios sujetos determinados distintos del interesado, del responsable, del encargado y de las personas autorizadas, en cualquier forma.

Autoridad de control: en Italia, el Garante per la protezione dei dati personali (Autoridad italiana de Protección de Datos). En general, la autoridad nacional encargada de verificar el cumplimiento de la normativa en materia de protección de datos personales.

Medidas de seguridad adecuadas: el conjunto de medidas técnicas, informáticas, organizativas, logísticas y de procedimiento adecuadas para proteger los datos en relación con el nivel de riesgo asociado a los tratamientos.

Registro de Actividades de Tratamiento: documento elaborado por la Empresa que mapea los tratamientos de datos personales realizados mediante instrumentos en papel y electrónicos.

Normativa de privacidad: el Código italiano de Protección de Datos, el RGPD y cualquier otra normativa sobre protección de datos personales aplicable, ya en vigor o que entre en vigor, incluidas las resoluciones, directrices y dictámenes de la Autoridad italiana de Protección de Datos, del CEPD y de cualquier otra autoridad competente.

5. COMPETENCIAS Y RESPONSABILIDADES

5.1. Responsable del tratamiento

El Responsable del tratamiento tiene la responsabilidad de:

- nombrar y revocar al Responsable interno (de privacidad) para la correcta coordinación de los tratamientos corporativos;
- suscribir los actos no delegables;
- supervisar el cumplimiento de la normativa de privacidad y de las obligaciones conexas, delegando para ello en los Responsables internos del tratamiento;
- dar cumplimiento a las obligaciones en materia de protección de datos personales previstas en el RGPD y en el Decreto Legislativo italiano n.º 196/2003 y sus modificaciones;
- supervisar las operaciones de tratamiento realizadas dentro de la Empresa con el fin de garantizar su conformidad con las disposiciones legales.

5.2. Delegado de Protección de Datos (DPD)

La Empresa ha designado como Delegada de Protección de Datos a la Sra. Elisa Rosso, abogada, a quien se puede contactar a través de la dirección de correo electrónico dpo@technacy.it.

El nombramiento del DPD, de conformidad con el art. 37 del RGPD, es obligatorio en supuestos específicos (tratamiento por parte de una autoridad u organismo público; actividades principales que requieran una observación habitual y sistemática de interesados a gran escala; tratamiento a gran escala de categorías especiales de datos o de datos relativos a condenas e infracciones penales). A falta de una obligación específica, el Reglamento permite la designación voluntaria de un DPD; en tal caso se aplican las mismas disposiciones de los arts. 37–39 del RGPD. Se hace referencia a las Directrices sobre la figura del DPD (WP243), confirmadas por el CEPD.

El DPD tiene la función de:

- informar y asesorar al Responsable del tratamiento y a los empleados que se ocupen del tratamiento de las obligaciones que les incumben en virtud del RGPD y de otras disposiciones en materia de protección de datos;
- supervisar el cumplimiento del RGPD y de las políticas del Responsable en materia de protección de datos personales, incluida la asignación de responsabilidades, la sensibilización y la formación del personal;
- preparar, con la colaboración de los Responsables internos (de privacidad), las modificaciones y correcciones de la presente Política y de los demás procedimientos, para preservar su coherencia;
- supervisar las actividades formativas e informativas dirigidas a las personas autorizadas para el tratamiento;
- colaborar en la elaboración y revisión de las cláusulas informativas, las fórmulas de consentimiento y los nombramientos de encargados del tratamiento;
- verificar periódicamente la correcta llevanza del registro de tratamientos, del registro de brechas de seguridad y de la lista de encargados del tratamiento;
- colaborar en la respuesta oportuna a las solicitudes de ejercicio de los derechos de los interesados;
- proporcionar su recomendación en el marco de las EIPD a que se refiere el art. 35 del RGPD y supervisar su desarrollo;
- cooperar con la Autoridad de control y actuar como punto de contacto, también a efectos de la consulta previa prevista en el art. 36 del RGPD.

En la oficina del DPD se archivan todas las comunicaciones dirigidas a la Autoridad de control competente.

5.3. Responsable interno (de privacidad) del tratamiento

Los Responsables internos (de privacidad) actúan siguiendo las directrices impartidas por el Responsable del tratamiento y tienen el control y la responsabilidad de los tratamientos realizados en su área/unidad de competencia. En particular, son responsables de:

- garantizar el cumplimiento de la normativa vigente en su función/área de competencia, prestando especial atención a la existencia de una base jurídica adecuada para cada tratamiento;
- supervisar la aplicación de las medidas de seguridad técnicas y organizativas exigidas por la normativa;
- supervisar la actualización/inventario de las operaciones de tratamiento y la actualización del Registro de Tratamientos, señalando cualquier transferencia de datos fuera del Espacio Económico Europeo (EEE);
- supervisar, cuando sea necesario, los procesos de evaluación de impacto y de riesgo de los tratamientos de su competencia;
- garantizar la participación de las personas autorizadas en los planes/cursos de formación;
- identificar a los posibles Encargados (externos) del tratamiento y supervisar el correcto cumplimiento de sus funciones, también mediante comprobaciones periódicas e inspecciones;
- informar al Responsable del tratamiento sobre eventuales violaciones de datos personales y sobre las no conformidades detectadas;
- colaborar en la actualización de las cláusulas informativas y de los consentimientos, también en las relaciones con los proveedores externos;
- prestar apoyo en la atención de las solicitudes de los interesados conforme a los arts. 15–22 del RGPD;
- mantener actualizado el registro de brechas de seguridad;
- preparar, con la ayuda de las funciones competentes, las EIPD a que se refiere el apartado dedicado a continuación;
- colaborar con las funciones de la Empresa para garantizar el cumplimiento de los principios de privacidad desde el diseño y por defecto;
- someter al DPD las cuestiones más relevantes en materia de tratamiento de datos personales.

5.4. Personas autorizadas/encargadas del tratamiento

Son todos los empleados y colaboradores que, actuando bajo la autoridad del Responsable interno (de privacidad) de su área, tratan datos personales. Son responsables de:

- realizar las actividades de tratamiento de acuerdo con las instrucciones recibidas;
- no modificar los tratamientos existentes ni introducir otros nuevos sin la autorización expresa de su Responsable;
- respetar las normas de seguridad para la protección de los datos;
- informar con prontitud al Responsable interno (de privacidad) en caso de violación de datos personales de la que tengan conocimiento o que sospechen;
- participar en los cursos de formación organizados por la Empresa.

En el momento de la contratación o de la firma del contrato de colaboración, cada empleado o colaborador recibe y acepta expresamente, además de la cláusula informativa sobre el tratamiento de sus propios datos personales, también la presente Política. Cada usuario es responsable de realizar con regularidad la formación en materia de privacidad puesta a disposición por la Empresa; el incumplimiento de esta obligación puede dar lugar a medidas disciplinarias.

5.5. Administradores de sistemas

Tienen la función de mantener y gestionar las infraestructuras de procesamiento o sus componentes a través de los cuales se realizan tratamientos de datos personales. Para las modalidades de nombramiento y verificación de su labor, se remite al apartado específico “Nombramientos” de Confluence, disponible en la siguiente dirección: https://technacy.atlassian.net/wiki/spaces/ADS/overview.

5.6 Operadores de sistemas

Tienen la función de gestionar y supervisar el correcto funcionamiento de los sistemas y de las aplicaciones que tienen encomendados, actuando según las instrucciones de la Empresa. Para las modalidades de nombramiento y verificación de su labor, se remite al apartado específico “Nombramientos” de Confluence, disponible en la siguiente dirección: https://technacy.atlassian.net/wiki/spaces/ADS/overview.

5.7. Funciones organizativas y formación

Las funciones definidas dentro de la Organización son: administración, atención al cliente, comercial y marketing, dirección, ingeniería de sistemas, desarrolladores, administradores de sistemas y operadores de sistemas.

De conformidad con el art. 29 del RGPD y el art. 2-quaterdecies del Decreto Legislativo 196/2003, todas las personas autorizadas para el tratamiento deben recibir la debida instrucción y formación sobre sus funciones, responsabilidades y operaciones de tratamiento, y estar sujetas al deber de confidencialidad. La formación se caracteriza por ser:

- **Específica** – acorde con el tipo de función/puesto desempeñado;
- **Adecuada** – en relación con el tipo de tratamientos realizados;
- **Permanente** – con programación temporal y actualización periódica, en particular para el personal de nueva incorporación;
- **Documentada** – su realización y las posteriores actualizaciones deben quedar acreditadas mediante registros, certificados u otros medios que las evidencien;
- **Eficaz** – debe verificarse periódicamente la comprensión y la asimilación de los procedimientos adoptados.

6. DISPOSICIONES GENERALES PARA EL TRATAMIENTO DE DATOS PERSONALES

6.1. Tratamiento del dato personal

Los datos personales solo pueden tratarse para los fines indicados en la cláusula informativa entregada al interesado en el primer contacto útil y de conformidad con lo previsto en los nombramientos individuales de encargado/autorizado. En general, los datos deben tratarse:

- de manera lícita, leal y transparente;
- recogidos y registrados con fines determinados, explícitos y legítimos, y utilizados de manera compatible con dichos fines;
- adecuados, pertinentes y no excesivos en relación con los fines para los que se recogen o tratan;
- exactos y, si es necesario, actualizados;
- conservados de forma que se permita la identificación del interesado durante un periodo no superior al necesario para los fines del tratamiento;

- tratados de manera que se garantice una seguridad adecuada, mediante medidas técnicas y organizativas apropiadas.

Los datos personales no pueden comunicarse a terceros salvo que el interesado haya prestado su consentimiento expreso o que exista otra base jurídica (por ejemplo, terceros cuya intervención sea necesaria para la gestión del contrato, como asesores o gestorías que traten los datos en calidad de Encargados). Para la transferencia al extranjero, se remite al apartado correspondiente.

6.2. Clasificación de los datos personales

Los datos personales se clasifican, conforme al RGPD, en las siguientes categorías:

- datos personales comunes;
- categorías especiales de datos personales (art. 9 RGPD);
- datos relativos a condenas e infracciones penales o a las correspondientes medidas de seguridad (art. 10 RGPD), cuyo tratamiento solo puede realizarse bajo el control de una autoridad pública o si está autorizado por el Derecho de la Unión o de los Estados miembros;
- datos de riesgo (de elaboración de perfiles, geolocalización, videovigilancia y comportamentales);
- datos de autenticación (códigos, contraseñas o PIN que permitan el acceso físico o lógico a sistemas, aplicaciones o instalaciones).

6.3. Principios y normas del tratamiento

De conformidad con los arts. 5 y 24 del RGPD, en el tratamiento de los datos personales deben respetarse los siguientes principios: licitud, lealtad y transparencia; limitación de la finalidad; minimización de datos; exactitud; limitación del plazo de conservación; integridad y confidencialidad. Estos principios y garantías se aplican y verifican también en cascada respecto de los eventuales subencargados.

Licitud, transparencia y lealtad

Un tratamiento es lícito únicamente si concurre, al menos, una de las siguientes bases jurídicas: consentimiento del interesado; ejecución de un contrato o de medidas precontractuales; cumplimiento de una obligación legal; salvaguarda de intereses vitales; ejecución de una misión de interés público; interés legítimo del responsable o de terceros, siempre que no prevalezcan los derechos y libertades del interesado. El consentimiento es, por tanto, solo una de las bases jurídicas y no la única. Para fines distintos de los del contrato al que se refiere la cláusula informativa (por ejemplo, marketing) es necesario un consentimiento expreso y separado, documentado y registrado.

Limitación de la finalidad

Los datos deben recogerse con fines determinados, explícitos y legítimos, y tratarse posteriormente de manera no incompatible con dichos fines. La introducción de una nueva finalidad exige compartir oportunamente con los interesados la documentación actualizada (cláusula informativa y, en su caso, consentimiento).

Minimización de datos

Los datos deben ser adecuados, pertinentes y limitados a lo necesario en relación con los fines. Cuando no sea posible utilizar datos anónimos o agregados, el uso de datos personales debe limitarse al mínimo indispensable.

Exactitud

Los datos deben ser exactos y, si es necesario, estar actualizados; deben preverse procedimientos para la supresión o rectificación oportuna de los datos inexactos.

Limitación del plazo de conservación

Los datos deben conservarse de forma que se permita la identificación de los interesados durante un periodo no superior al necesario para alcanzar los fines del tratamiento.

Integridad y confidencialidad

Los datos personales deben tratarse de manera que se garantice su integridad y confidencialidad, impidiendo el acceso o uso no autorizados.

6.4. Información sobre protección de datos

El interesado debe recibir una adecuada información sobre la protección de sus datos. Cuando los datos se obtengan directamente del interesado, la información se facilita conforme al art. 13 del RGPD en el momento de la recogida. Cuando los datos se obtengan a través de terceros, la información se facilita conforme al art. 14: dentro de un plazo razonable y, en cualquier caso, no superior a un mes; a más tardar en el momento del primer contacto, en caso de comunicación con el interesado; o, a más tardar, en el momento de la primera comunicación, si los datos van a comunicarse a otro destinatario.

La actualización de las cláusulas informativas corresponde al Responsable interno (de privacidad) competente, quien debe consultarlo con el DPD. No es posible modificar las cláusulas informativas adoptadas sin la previa aprobación por escrito del Responsable interno (de privacidad) y/o del DPD.

6.4.1. Información directa (art. 13 RGPD)

Cuando los datos se recojan del interesado, la cláusula informativa debe contener, entre otros extremos: la identidad y los datos de contacto del responsable; los datos de contacto del DPD; los fines y la base jurídica del tratamiento; los intereses legítimos que, en su caso, se persigan; los posibles destinatarios; la intención, en su caso, de transferir los datos a un tercer país y las correspondientes garantías; el plazo de conservación; los derechos del interesado; el derecho a retirar el consentimiento; el derecho a reclamar ante la Autoridad de control; el carácter obligatorio o facultativo de facilitar los datos; y la existencia de decisiones automatizadas.

6.4.2. Información posterior (art. 14 RGPD)

Cuando los datos no se recojan del interesado, la información, facilitada dentro de un plazo razonable no superior a un mes, contiene, además de lo previsto en el art. 13, las categorías de datos recogidos y la indicación de su origen. No procede su entrega cuando el interesado ya disponga de la información, cuando el registro esté previsto por ley, o cuando informar al interesado resulte imposible o exija un esfuerzo desproporcionado.

6.4.3. Información adicional (nuevas finalidades)

Cuando se introduzcan nuevas finalidades, se facilita al interesado una cláusula informativa adicional específica, antes del inicio del tratamiento para la nueva finalidad. Simultáneamente, los Responsables internos (de privacidad) actualizan el registro de tratamientos.

6.5. Tratamiento de los datos personales de la Empresa

Los tratamientos se refieren principalmente a los datos de empleados, clientes, proveedores, personas afectadas por instalaciones de videovigilancia y visitantes de los sitios web.

6.5.1. Empleados

Los datos personales de los trabajadores, tanto en la fase previa a la constitución de la relación laboral como durante su desarrollo, se recogen del propio trabajador y, solo cuando sea necesario, de terceros, con fines relacionados con la selección, la constitución y la gestión de la relación laboral. La Empresa trata dichos datos, incluso sin consentimiento, cuando ello sea necesario para cumplir obligaciones

contractuales, legales o de la negociación colectiva, así como para la defensa de un derecho en sede judicial y para la protección de la salud del trabajador. En los demás casos, se recaba el consentimiento expreso.

6.5.2. Acceso a los datos en ausencia de la persona autorizada (accesos de emergencia)

En caso de necesidad de acceder a datos y/o dispositivos electrónicos asignados a un empleado ausente (por ejemplo, extinción de la relación laboral, enfermedad, fallecimiento), el responsable jerárquico directo, una vez comprobada la ausencia de alternativas, solicita por escrito al Responsable interno (de privacidad) el acceso a los datos. El Responsable interno (de privacidad), tras verificar la solicitud, facilita las instrucciones oportunas y lo comunica al Responsable de Sistemas de Información. Al finalizar las operaciones, el solicitante lo comunica por escrito y, en la medida de lo posible, informa a la persona autorizada ausente.

6.5.3. Clientes

Los clientes son informados, mediante cláusulas informativas específicas, sobre el tratamiento de sus datos personales, tanto con fines comerciales como contractuales.

6.5.4. Proveedores nombrados Encargados del tratamiento conforme al art. 28 RGPD

Respecto de los proveedores nombrados Encargados del tratamiento, la Empresa utiliza sus datos exclusivamente para fines contractuales.

6.5.5. Visitantes de los sitios web

Los visitantes de los sitios web son informados, mediante una cláusula informativa específica y, en su caso, una política de cookies disponibles en los sitios corporativos, sobre los datos registrados durante la conexión, la navegación, el registro y/o la cumplimentación de formularios.

6.5.6. Videovigilancia

Cuando se instalen sistemas de videovigilancia, los interesados son informados de las modalidades de tratamiento mediante cláusulas informativas específicas, facilitadas tanto en forma extensa como mediante la señalización oportuna colocada antes del radio de acción de las cámaras.

7. DERECHOS DEL INTERESADO

La Empresa pone a disposición de los interesados una dirección postal y una dirección de correo electrónico a través de las cuales pueden ejercer los derechos previstos en el Capítulo III del RGPD (arts. 15–22): acceso, rectificación, supresión, limitación, portabilidad, oposición y derecho a no ser objeto de decisiones automatizadas, incluida la elaboración de perfiles.

La Organización ha adoptado un Procedimiento específico para la Gestión de los Derechos de los Interesados, al que se remite para el detalle operativo. En síntesis, el procedimiento regula:

- la recepción de las solicitudes (por correo electrónico, formulario web, correo postal ordinario);
- la verificación de la identidad del solicitante antes de dar curso a la solicitud;
- los plazos de respuesta: un mes desde la recepción, prorrogable por dos meses adicionales (hasta un máximo total de tres meses) en caso de especial complejidad o de un elevado número de solicitudes, con la obligación de comunicar la prórroga al interesado dentro del primer mes; la respuesta es obligatoria incluso en caso de denegación;
- el registro de cada solicitud y de su correspondiente resultado en un registro interno específico;
- las modalidades de implicación del DPD en los casos de incertidumbre jurídica o de posible conflicto entre los derechos del interesado y las obligaciones legales.

Si un empleado recibe una solicitud de ejercicio de derechos, debe comunicarlo de inmediato a su Responsable interno (de privacidad).

8. MEDIDAS DE SEGURIDAD TÉCNICAS Y ORGANIZATIVAS (ART. 32 RGPD)

La Organización adopta medidas técnicas y organizativas adecuadas al riesgo, de conformidad con el art. 32 del RGPD, teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como el riesgo para los derechos y libertades de las personas físicas.

En función de la evaluación del riesgo, la Empresa adopta, o se compromete a adoptar, a título ejemplificativo y no exhaustivo, las siguientes medidas:

- cifrado de los datos personales en tránsito y en reposo, cuando sea técnicamente aplicable;
- seudonimización de los datos en los entornos de desarrollo y pruebas;
- control de accesos basado en roles (RBAC) y autenticación multifactor (MFA) para los sistemas críticos;
- procedimientos de copia de seguridad periódicos con verificación periódica de la restauración;
- planes de continuidad de negocio y de recuperación ante desastres, sometidos a pruebas periódicas;
- actividades periódicas de evaluación de vulnerabilidades y pruebas de penetración;
- supervisión y registro de los accesos a los sistemas de tratamiento.

La adecuación de las medidas se revisa al menos una vez al año y con ocasión de modificaciones significativas de los sistemas o de los procesos de tratamiento. Las medidas se refuerzan en los tratamientos que afecten a categorías especiales de datos, de conformidad con el principio de proporcionalidad.

9. CONTRATOS: NOMBRAMIENTO DE PROVEEDORES TERCEROS COMO ENCARGADOS DEL TRATAMIENTO (ART. 28 RGPD)

Cada vez que un proveedor o, en general, un sujeto externo tenga acceso a datos personales tratados por la Empresa, es necesario proceder a su nombramiento como Encargado del tratamiento de conformidad con el art. 28 del RGPD, previa verificación de su idoneidad para tratar datos personales de conformidad con la Normativa de privacidad aplicable, mediante los controles que, en su caso, requiera el Responsable interno (de privacidad) de acuerdo con el DPD.

Si de los controles resulta que el proveedor no es capaz de ofrecer garantías suficientes desde el punto de vista técnico y/u organizativo, no será posible suscribir el contrato. En caso de resultado positivo, el responsable de la función corporativa competente obtiene la aprobación del Responsable interno (de privacidad) para la firma de la carta de nombramiento conforme al art. 28 del RGPD. Concluida la verificación y firmado el nombramiento, el Responsable interno (de privacidad) actualiza la lista de encargados del tratamiento y notifica el nombramiento al DPD; la Empresa conserva una copia del nombramiento.

Estos principios y garantías se verifican respecto de cada proveedor cuyo servicio implique el tratamiento de datos personales, también mediante auditorías periódicas y el seguimiento sistemático del estado de aplicación de las garantías. Las garantías se aplican y verifican también en cascada respecto de los eventuales subencargados.

Se especifica que, cuando sea Technacy la que trate datos personales por cuenta de un Cliente, es la propia Empresa la que debe recibir el nombramiento como Encargado del tratamiento conforme al art. 28 del RGPD.

10. PRIVACIDAD DESDE EL DISEÑO Y PRIVACIDAD POR DEFECTO (ART. 25 RGPD)

El Responsable interno (de privacidad) supervisa el correcto tratamiento de los datos personales, su exactitud, fiabilidad y actualización, tanto en la fase de adquisición como durante el tratamiento. Cada nuevo tipo de tratamiento se comunica al Responsable interno (de privacidad), quien valora la conveniencia de implicar al DPD y la eventual actualización del registro.

Cuando se pretenda llevar a cabo una nueva actividad, o desarrollar o actualizar un producto o servicio que implique el tratamiento de datos personales, deben respetarse los siguientes principios:

- **Principio de privacidad desde el diseño:** todo proyecto o producto debe desarrollarse teniendo en cuenta las cuestiones de protección de datos personales desde la fase de diseño, determinando las medidas técnicas y organizativas adecuadas sobre la base de la evaluación del riesgo;
- **Principio de privacidad por defecto:** todo proyecto o producto debe garantizar que, por defecto, solo se traten los datos personales necesarios para cada finalidad específica del tratamiento (calidad de los datos, alcance del tratamiento, plazo de conservación y accesibilidad), evitando que los datos se hagan accesibles a un número indefinido de personas sin la intervención de la persona física afectada.

A tal fin, el usuario se coordina con su Responsable interno (de privacidad), quien a su vez se coordina con el DPD para valorar si procede realizar una EIPD y si deben implicarse otras unidades en el análisis de riesgos y en la definición del plan de acción. Al finalizar el proyecto, el Responsable interno (de privacidad) realiza, junto con el DPD, una valoración general de la conformidad del nuevo producto o servicio con los principios del RGPD. No se pueden desarrollar nuevos productos, servicios, herramientas o funcionalidades que impliquen el tratamiento de datos personales sin seguir estas indicaciones.

11. TRATAMIENTO DE CATEGORÍAS ESPECIALES DE DATOS (ART. 9 RGPD)

La Organización, en su condición de Responsable del tratamiento, puede llegar a tratar categorías especiales de datos: en tal caso, identifica previamente una base jurídica adecuada entre las previstas en el art. 9, apartado 2, del RGPD (entre ellas, el consentimiento explícito del interesado; las obligaciones en materia de Derecho laboral y de Seguridad Social; los fines de medicina del trabajo o de asistencia sanitaria; las razones de interés público en el ámbito de la salud pública).

En ocasiones, en su condición de Encargado del tratamiento por cuenta de clientes, la Empresa puede llegar a tratar – aunque de forma esporádica – categorías especiales de datos personales conforme al art. 9 del RGPD (por ejemplo, datos de salud, biométricos, relativos al origen étnico) en función de la naturaleza de los servicios prestados. En tales casos:

- el Registro de Actividades de Tratamiento indica expresamente el tipo de datos especiales tratados para cada cliente/tratamiento;
- los contratos conforme al art. 28 del RGPD con los clientes responsables del tratamiento especifican las instrucciones aplicables y las medidas de seguridad reforzadas exigidas;
- las medidas técnicas y organizativas adoptadas para dichos tratamientos se refuerzan respecto del estándar, de conformidad con el principio de proporcionalidad;
- se evalúa sistemáticamente la necesidad de realizar una EIPD antes del inicio o de la modificación de tratamientos que afecten a categorías especiales de datos.

12. GESTIÓN DE LAS VIOLACIONES DE DATOS PERSONALES (BRECHAS DE SEGURIDAD) (ARTS. 33–34 RGPD)

Los artículos 33 y 34 del RGPD establecen los requisitos del proceso de gestión de incidentes de privacidad. Dicho incidente se configura como una violación de la seguridad que ocasione, de forma accidental o ilícita, la destrucción, la pérdida, la alteración, la comunicación no autorizada o el acceso a los datos personales tratados, o su indisponibilidad.

Una violación, si no se aborda de manera adecuada y oportuna, puede provocar daños físicos, materiales o inmateriales a las personas físicas (pérdida de control sobre sus datos, discriminación, robo o usurpación de identidad, pérdidas financieras, perjuicio para la reputación, etc.).

El RGPD impone al Responsable del tratamiento la obligación de comunicar a la Autoridad de control la violación producida en un plazo de 72 horas (o, en cualquier caso, sin dilación indebida). Cuando la violación entrañe un alto riesgo para los derechos y libertades de los interesados, estos también deben ser informados sin dilación. A tal fin, la Organización dispone de un registro de incidentes (registro de brechas de seguridad).

Cualquier persona que detecte un caso, incluso meramente sospechoso, de violación de datos personales debe comunicarlo lo antes posible a su Responsable interno (de privacidad) y seguir lo establecido en el Procedimiento específico de brechas de seguridad, al que se remite íntegramente.

13. EVALUACIÓN DE IMPACTO RELATIVA A LA PROTECCIÓN DE DATOS (EIPD) (ART. 35 RGPD)

De conformidad con el art. 35 del RGPD, el Responsable del tratamiento debe realizar una Evaluación de Impacto relativa a la Protección de Datos (EIPD) cuando un tipo de tratamiento entrañe un alto riesgo para los derechos y libertades de las personas físicas. La obligación de realizar una EIPD existe, en particular, cuando concurren al menos dos de los factores de alto riesgo identificados por el CEPD (Directrices WP248 rev. 01):

- evaluación o puntuación sistemática, incluida la elaboración de perfiles;
- decisiones automatizadas que produzcan efectos jurídicos o afecten significativamente al interesado;
- observación sistemática, incluso de zonas de acceso público;
- tratamiento a gran escala de categorías especiales de datos (art. 9) o de datos relativos a condenas e infracciones penales (art. 10);
- tratamiento de datos a gran escala;
- cotejo o combinación de conjuntos de datos;
- datos relativos a sujetos vulnerables (en particular, menores de edad);
- uso innovador o aplicación de nuevas tecnologías;
- tratamientos que impidan a los interesados ejercer un derecho o utilizar un servicio o un contrato.

Se remite asimismo a la lista de tratamientos que requieren una EIPD publicada por la Autoridad italiana de Protección de Datos de conformidad con el art. 35, apartado 4, del RGPD. La Organización ha adoptado un Procedimiento para la realización de EIPD, al que se remite. La EIPD se realiza con carácter previo al inicio del tratamiento y, cuando sea necesario, con la consulta del DPD; los resultados se documentan y conservan en el expediente.

Cuando el DPD valore que el tratamiento presenta un alto riesgo en ausencia de medidas de mitigación, se procede a la consulta previa de la Autoridad de control de conformidad con el art. 36 del RGPD.

14. REGISTRO DE ACTIVIDADES DE TRATAMIENTO (ART. 30 RGPD)

La Organización elabora y mantiene actualizado el Registro de Actividades de Tratamiento, tanto en su condición de Responsable como de Encargado del tratamiento. Aunque el art. 30, apartado 5, del RGPD prevé una exención formal para las organizaciones con menos de 250 empleados, dicha exención resulta, en la práctica, inaplicable a Technacy S.r.l., dado que la Empresa:

- realiza tratamientos no ocasionales en el marco de los servicios prestados de forma continuada a su clientela;
- trata datos por cuenta de terceros en calidad de encargado del tratamiento, con tratamientos que pueden incluir datos de categorías especiales conforme al art. 9 del RGPD;
- opera en el sector de las telecomunicaciones y del desarrollo de software, con tratamientos que, por su naturaleza y escala, hacen obligatorio el registro.

El Registro contiene, entre otros datos: el nombre y los datos de contacto del Responsable del tratamiento (y, en su caso, del corresponsable, del representante y del Responsable interno); los fines del tratamiento; una descripción de las categorías de interesados y de datos personales; las categorías de destinatarios; las posibles transferencias a terceros países y las correspondientes garantías; los plazos previstos para la supresión de las distintas categorías de datos; y una descripción general de las medidas de seguridad adoptadas.

El Registro se conserva bajo la responsabilidad del Responsable interno (de privacidad), quien se encarga de su actualización para su área. Cualquier cambio se comunica al DPD. El Registro constituye un instrumento permanente de rendición de cuentas y se pone a disposición de la Autoridad de control cuando esta lo solicite.

15. PLAZOS DE CONSERVACIÓN (ARTS. 5 Y 17 RGPD)

Los datos personales se tratan durante el tiempo estrictamente necesario para dar cumplimiento a la finalidad indicada en la cláusula informativa. Los plazos de conservación específicos para cada categoría de tratamiento, así como las modalidades de supresión o anonimización al término del plazo de conservación, se establecen en el Procedimiento de conservación de datos, al que se remite íntegramente.

El procedimiento establece también los responsables internos de la ejecución de las actividades de supresión y las modalidades de verificación y documentación de las mismas. Todos los usuarios tienen la obligación de no utilizar los datos una vez transcurrido el correspondiente plazo de conservación y de comunicar a su Responsable interno (de privacidad) cualquier vencimiento que no haya ido seguido de la supresión o anonimización correspondiente.

16. TRANSFERENCIAS DE DATOS A TERCEROS PAÍSES (ARTS. 44–49 RGPD)

El Responsable del tratamiento, en el marco de sus actividades, tiende a no transferir datos personales a países fuera de la UE. En caso de que surja dicha necesidad, se informa previamente a los interesados y se adoptan las garantías adecuadas que, según los casos, podrán consistir en:

- comprobación de la existencia de una decisión de adecuación de la Comisión Europea para el país de destino (art. 45 RGPD); entre ellas cabe destacar el Marco de Privacidad de Datos UE–EE. UU., adoptado mediante la Decisión de Ejecución (UE) 2023/1795, de 10 de julio de 2023, con verificación de la certificación del destinatario en el registro oficial del DPF antes de la transferencia;
- suscripción de cláusulas contractuales tipo adoptadas por la Comisión Europea (art. 46, apartado 2, letra c, del RGPD);
- adopción de medidas adicionales cuando sea necesario, de conformidad con la Recomendación 01/2020 del CEPD y sus posteriores actualizaciones;
- como excepción a las garantías anteriores, para tratamientos específicos (art. 49 RGPD), comprobación de la existencia de un contrato o de medidas precontractuales en interés del interesado, o bien obtención del consentimiento explícito a la transferencia.

La Organización revisa periódicamente la adecuación de las garantías adoptadas, también a la luz de la evolución normativa y jurisprudencial, actualizando las medidas en caso de modificación del marco de referencia.

17. SUPERVISIÓN Y CONTROL

Por razones organizativas y productivas, y para la protección del patrimonio corporativo, la Empresa puede tener necesidad de controlar el uso de sus propios sistemas TIC. Esta actividad no constituye un control del empleado y se lleva a cabo de conformidad con la legislación italiana en materia de derechos de los trabajadores y de protección de datos personales. Tal y como se detalla en el Reglamento informático, al que se remite íntegramente, las razones del control incluyen: identificar y prevenir accesos o comunicaciones no autorizados; garantizar el cumplimiento de leyes y reglamentos; prevenir e identificar actividades delictivas; controlar virus y código malicioso; garantizar la continuidad del negocio; investigar, en caso de sospecha, usos inapropiados o incumplimientos; responder a reclamaciones; y llevar a cabo investigaciones disciplinarias o legales.

El control se lleva a cabo dentro de los límites permitidos o exigidos por la ley y en la medida en que resulte necesario y justificable. La información identificada (incluida la personal) puede utilizarse y conservarse durante la duración de cualquier procedimiento y comunicarse a terceros cuando sea necesario. El uso de los sistemas informáticos que no se ajuste a la presente Política puede dar lugar a la aplicación de sanciones disciplinarias.

18. GESTIÓN DE LAS RELACIONES CON LAS AUTORIDADES DE CONTROL

El DPD es el único punto de contacto para las relaciones con las Autoridades de control en materia de privacidad y coordina el correspondiente proceso de comunicación. Las distintas funciones de la Empresa colaboran, cuando sea necesario, en relación con las comunicaciones con la Autoridad de control italiana y, en su caso, con las autoridades de otros países. Las relaciones con las Autoridades comprenden, en particular: la consulta previa cuando un tratamiento entrañe un alto riesgo residual; la notificación de violaciones de datos; y la representación de la Empresa en las auditorías realizadas por las Autoridades.

19. CONDICIONES GENERALES PARA LA IMPOSICIÓN DE SANCIONES

La aplicación efectiva de la presente Política está garantizada por un sistema disciplinario adecuado, que puede sancionar el incumplimiento y la vulneración de las normas en ella contenidas, con independencia de la eventual incoación de un procedimiento penal.

El art. 83 del RGPD establece los criterios para la imposición de sanciones administrativas pecuniarias, teniendo en cuenta, entre otros factores: la naturaleza, gravedad y duración de la infracción; su carácter doloso o negligente; las medidas adoptadas para paliar los daños; el grado de responsabilidad; las infracciones anteriores que, en su caso, se hayan cometido; el grado de cooperación con la Autoridad; las categorías de datos afectadas; la forma en que la Autoridad tuvo conocimiento de la infracción; y la adhesión a códigos de conducta o a mecanismos de certificación.

Las infracciones de las obligaciones del Responsable y del Encargado del tratamiento (arts. 8, 11, 25–39, 42 y 43 del RGPD) están sujetas a multas de hasta 10.000.000 € o, tratandose de empresas, de hasta el 2 % del volumen de negocio total anual a escala mundial, si esta última cifra fuera superior. Las infracciones de los principios básicos del tratamiento, de los derechos de los interesados y de las normas sobre transferencias (arts. 5, 6, 7, 9, 12–22 y 44–49 del RGPD) están sujetas a multas de hasta 20.000.000 € o, tratandose de empresas, de hasta el 4 % del volumen de negocio total anual a escala mundial, si esta última cifra fuera superior.

20. RESPONSABILIDAD POR LA ADOPCIÓN DE LA POLÍTICA

La Organización, tanto en su condición de Responsable como de Encargado del tratamiento, es responsable de la política de protección de datos, en coherencia con la evolución del contexto empresarial y del mercado, valorando las medidas que deban adoptarse ante eventos tales como:

- cambios significativos en el negocio;
- nuevas amenazas en relación con las consideradas en el análisis de riesgos;
- incidentes de seguridad significativos;
- la evolución del marco normativo o legislativo en materia de tratamiento seguro de la información;
- el uso de nuevas tecnologías.

21. REVISIÓN Y ACTUALIZACIÓN DE LA POLÍTICA

Periódicamente, al menos una vez al año, se lleva a cabo una revisión para verificar la eficiencia, la eficacia y la adecuación de las medidas técnicas y organizativas aplicadas. Las instrucciones impartidas al personal designado para los tratamientos constituyen la política corporativa en materia de tratamiento de datos y se revisan y/o actualizan al menos una vez al año.

Además de la revisión ordinaria, está prevista una revisión extraordinaria de la presente Política cuando concurra uno o varios de los siguientes supuestos: modificaciones normativas o reglamentarias significativas; adopción de nuevas tecnologías de tratamiento; resultado crítico de una EIPD; violación de datos personales de especial gravedad; auditoría interna o inspección de la Autoridad de control. El resultado de la revisión y las eventuales modificaciones introducidas se documentan en el Historial de Revisiones que figura al inicio del presente documento.

22. MODALIDADES DE DIFUSIÓN DE LA POLÍTICA

Technacy S.r.l. publica y difunde la presente Política entre su personal y colaboradores, también a través de los canales internos de información (por ejemplo, la intranet corporativa), garantizando que sea conocida por todas las personas autorizadas para el tratamiento y compartida, cuando proceda, con los terceros implicados.

TECHNACY S.R.L.

Domicilio social y centro de operaciones: Via Molveno, 5 – 48015 Cervia (RA), Italia

NIF/IVA: 02399920392 | Correo electrónico: info@technacy.it | Sitio web: www.technacy.it

Para su aprobación – Responsable del tratamiento

_____

(Fecha, sello y firma)

Cervia, 24 de junio de 2026