Normas corporativas vinculantes del Grupo PROSEGUR

VERSIÓN PÚBLICA

SEPTIEMBRE DE 2023

PROSEGUR

www.prosegur.com

Índice

1. Propietario

Dirección de cumplimiento del Grupo PROSEGUR.

2. Introducción

2.1. Acerca de Prosegur

- **Prosegur Compañía de Seguridad España, SA** (en adelante, PROSEGUR): es la empresa matriz de un grupo líder mundial en el sector de la seguridad privada. Con nuestras cinco líneas de negocio: alarmas, seguridad, gestión de efectivo, externalización de procesos empresariales (AVOS) y ciberseguridad (Cipher), proporcionamos a empresas y hogares una seguridad de confianza, basada en las soluciones más avanzadas del mercado.

- **Alarmas**: Prosegur Alarmas cuenta con una amplia gama de productos que contribuyen a mejorar la seguridad y tranquilidad de familias y empresas. Las alarmas de triple seguridad de Prosegur ofrecen los sistemas más avanzados del mercado. La gama de empresa abarca desde sistemas de alarma con verificación por vídeo hasta la automatización de espacios interiores y exteriores, productos siempre personalizados que nos convierten en un referente mundial de la seguridad.

- **Seguridad**: Prosegur Seguridad ofrece servicios integrales de seguridad de alto valor añadido, al combinar la tecnología más avanzada y los mejores profesionales. La empresa está permanentemente centrada en la innovación tecnológica, integrada en la cadena de valor de cada segmento de negocio.

  La actividad de seguridad incluye la vigilancia tradicional y otros servicios auxiliares como la ciberseguridad.

  Estos servicios son el resultado de la experiencia y el conocimiento de las áreas de riesgo de los clientes.

- **Efectivo**: Prosegur Cash abarca todo el ciclo del efectivo y procesa más de 450 000 millones de euros al año. Opera en más de 500 centros de quince países y gestiona más de 100 000 puntos de caja.

  Prosegur Cash es líder mundial en la prestación de servicios de logística y gestión de efectivo, así como en la externalización de servicios a entidades financieras, comercios minoristas, organismos gubernamentales y bancos centrales, casas de la moneda, joyerías y otras actividades comerciales en todo el mundo, sobre todo, en los sectores de la banca y la distribución.

- **AVOS**: Prosegur AVOS es la rama de actividad centrada en la externalización de servicios empresariales, el diseño de soluciones innovadoras y la apuesta por nuevas capacidades tecnológicas.

  En Prosegur AVOS ayudamos a nuestros colaboradores a mejorar sus operaciones y adelantarse al mercado, asumir los procesos más complejos y perfeccionar la experiencia del cliente. Hemos diseñado una propuesta de valor diferencial cuyo principal objetivo es aprovechar el conocimiento adquirido a lo largo de los años y adaptarlo a las nuevas tendencias en tecnología y digitalización. En Prosegur AVOS nos proponemos el objetivo de proporcionar

a nuestros clientes la máxima agilidad, trazabilidad y visibilidad en todas las tareas desarrolladas en el centro de trabajo.

- **Ciberseguridad** Cipher es una empresa de ciberseguridad global que presta una amplia variedad de servicios: detección y respuesta gestionadas o MDR (Managed Detection and Response), servicios de seguridad gestionados o MSS (Managed Security Services), servicios de ciberinteligencia o CIS (Cyber Intelligence Services), servicios de Red Team o RTS (Red Team Services), gestión, riesgo y cumplimiento normativo o GRC (Governance, Risk and Compliance) e integración de tecnología de ciberseguridad o CTI (Cybersecurity Technology Integration). Estos servicios cuentan con la asistencia de Cipher Labs, un laboratorio de élite de desarrollo e investigación de ciberinteligencia y amenazas, así como de seis centros de operaciones de seguridad o SOC (Security Operations Centers), las 24 horas del día, 7 días a la semana.

- Operamos en los cinco continentes, donde el reto es ofrecer más servicios de valor añadido y ocupar una posición de liderazgo en el sector de la seguridad privada en cada mercado.

- Para ello, aspiramos a tener una fuerte presencia geográfica basada en un modelo de negocio probado. Además de nuestro enfoque global, también actuamos localmente. Operamos según las particularidades de cada mercado, ya que nuestro sector está altamente regulado y varía en función de la legislación de cada país.

- Además de ser líder mundial en la prestación de servicios de seguridad privada, el Grupo PROSEGUR está firmemente comprometido con la sociedad y con los más desfavorecidos, por lo que cuenta con una organización sin ánimo de lucro, la Fundación Prosegur, que materializa el compromiso del Grupo PROSEGUR de contribuir al progreso de las regiones con menos recursos en las que opera. Apoya la educación como motor indiscutible de cambio, la discapacidad intelectual y promueve acciones de voluntariado que canalizan la solidaridad de los profesionales de nuestra empresa.

  Nuestros proyectos solidarios emprendidos a través de la Fundación Prosegur en los ámbitos de la educación, la inclusión social, el voluntariado corporativo y la cultura, se implantan progresivamente en los diferentes países en los que operamos, teniendo en cuenta criterios de sostenibilidad, transparencia y réplica de buenas prácticas.

- El carácter global de este grupo de empresas compromete al Grupo PROSEGUR a llevar a cabo todos los esfuerzos necesarios para regularizar las transferencias internacionales de datos que puedan producirse entre las distintas entidades del Grupo ubicadas en diversas regiones —Europa, Latinoamérica, EEUU y resto del mundo—, con la adopción de las presentes Normas Corporativas Vinculantes (NCV), tal y como se definen a continuación.

2.2. Definiciones

A efectos del presente documento, los siguientes términos tienen el significado que aquí se les da.

- «**Acuerdo NCV**»: documento destinado a establecer el marco jurídico común para regular las TID que tengan lugar entre las entidades comprendidas en su ámbito de aplicación.

- «**Entidad NCV**»: entidad del Grupo PROSEGUR que se encuentra en el ámbito de aplicación del Acuerdo NCV.

- **«Normas corporativas vinculantes** o **NCV**»: políticas de protección de datos personales a las que se adhiere un responsable o un encargado del tratamiento en el territorio de un Estado miembro para las transferencias o conjuntos de transferencias de datos personales a un

responsable o encargado del tratamiento de uno o varios terceros países en el seno de un grupo de compromisos o empresas que ejercen una actividad económica conjunta.

- **«Autoridades supervisoras competentes»**: esta expresión hace referencia a las autoridades supervisoras de protección de datos del EEE competentes para las exportadoras de datos.

- «**Responsable del tratamiento**» o «**Responsable**»: persona física o jurídica, autoridad pública, agencia u otro organismo que en solitario o agrupada con otras determine los fines y medios del tratamiento de datos personales.

- «**Exportador de los datos**»: entidad NCV establecida en el Espacio Económico Europeo.

- «**Importadora de datos**»: entidad NCV establecida o ubicada en un tercer país.

- «**Encargado del tratamiento**» o «**Encargado**»: persona física o jurídica, autoridad pública, agencia u otro organismo que trate datos personales por cuenta del responsable del tratamiento.

- «**Evaluación del impacto de la protección de datos**»: análisis detallado de una o varias operaciones similares de tratamiento de datos personales, con el fin de identificar y evaluar los riesgos asociados al tratamiento y determinar las medidas que deben adoptarse para prevenirlos o mitigarlos.

- «**Delegado de Protección de Datos**»: persona responsable de asesorar a los responsables y encargados del tratamiento sobre sus obligaciones en virtud de la legislación aplicable en materia de protección de datos, supervisar el cumplimiento de dichas obligaciones y actuar como punto de contacto para las autoridades.

- **«Divulgación»**: comunicación mediante transmisión, difusión o cualquier otra forma de acceso.

- «**Normativa europea de protección de datos**»: el RGPD y las leyes de protección de datos vigentes en los Estados miembros.

- «**Espacio Económico Europeo**» o «**EEE**»: Estados miembros de la Unión Europea, junto con Liechtenstein, Islandia y Noruega.

- «**Leyes europeas**»: el derecho de la Unión Europea y de sus Estados miembros.

- «**RGPD**» o «**Reglamento General de Protección de Datos**»: 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 y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).

- «**Transferencias internacionales de datos**» o «**TID**»: Divulgación de datos personales de un exportador de datos a un importador de datos.

- «**Estados miembros**»: Estados miembros de la Unión Europea, junto con Liechtenstein, Islandia y Noruega.

- «**Transferencias a terceros**”: divulgación de datos personales de un importador de datos a destinatarios, que pueden pertenecer o no al Grupo PROSEGUR.

- «**Datos personales**» o «**Datos**»: cualquier información relativa a una persona física identificada o identificable («**interesado**»); una persona física identificable es aquella que puede ser

identificada, directa o indirectamente, en particular por referencia a un identificador como un nombre, un número de identificación, datos de localización, un identificador en línea o a uno o más factores específicos de la identidad física, fisiológica, genética, mental, económica, cultural o social de dicha persona física

- «**Fallo de seguridad de los datos personales**»: vulneración de la seguridad que provoque la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, almacenados o tratados de otro modo, o la comunicación o acceso no autorizados a dichos datos.

- «**Personal**»: cualquier persona, a tiempo completo o temporal, interna o externa, que preste servicios o ejerza una actividad profesional en el ámbito de una entidad del Grupo PROSEGUR.

- «**Tratamiento**»: toda operación o conjunto de operaciones, efectuadas o no mediante procedimientos automatizados, relativas a datos personales o a conjuntos de datos personales, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, borrado o destrucción.

- «**PROSEGUR**»: Prosegur Compañía de Seguridad España, S.A., empresa matriz del Grupo PROSEGUR.

- «**Grupo PROSEGUR**»: todas las entidades que forman parte del grupo de empresas PROSEGUR, estén o no bajo el ámbito de aplicación del Acuerdo NCV.

- «**Destinatario**»: persona física o jurídica, autoridad pública, agencia u otro organismo al que se comuniquen los datos personales, ya sea un tercero o no. No obstante, no se considerarán destinatarios las autoridades que puedan recibir datos personales en el marco de una investigación concreta de conformidad con el derecho de la Unión Europea o de los Estados miembros; el tratamiento de dichos datos por parte de dichas autoridades deberá ajustarse a las normas de protección de datos aplicables en función de los fines del tratamiento;

- **«Categorías especiales de datos personales»:** los datos personales que revelen el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, así como los datos genéticos (relativos a las características genéticas heredadas o adquiridas de una persona física que proporcionen una información única sobre la fisiología o la salud de dicha persona física y que resulten, en particular, de un análisis de una muestra biológica de la persona física en cuestión), los datos biométricos destinados a identificar de manera unívoca a una persona física (resultantes de un tratamiento técnico específico relativo a las características físicas fisiológicas o de comportamiento de una persona física, que permiten o confirman la identificación única de dicha persona física, como imágenes faciales o datos dactiloscópicos), datos relativos a la salud (relacionados con la salud física o mental de una persona física, incluida la prestación de servicios de asistencia sanitaria, que revelan información sobre su estado de salud) o datos relativos a la vida sexual o a la orientación sexual de una persona física.

- «**Cláusulas contractuales tipo**»: cláusulas tipo de protección de datos adoptadas por la Comisión Europea con arreglo al procedimiento de examen contemplado en el artículo 93, apartado 2, del RGPD o adoptadas por una autoridad de supervisión y aprobadas por la Comisión Europea con arreglo al procedimiento de examen contemplado en el artículo 93, apartado 2, del RGPD;

- «**Autoridad de supervisión**»: una autoridad pública independiente, establecida por un Estado miembro para supervisar la aplicación del RGPD, con el fin de proteger los derechos y libertades fundamentales de las personas físicas en relación con el tratamiento y facilitar la libre circulación de datos personales dentro de la Unión Europea.

- «**Tercer país**»: se aplica a cualquier país no perteneciente al Espacio Económico Europeo.

- «**Terceros**»: persona física o jurídica, autoridad, agencia u organismo distintos del interesado, responsable del tratamiento, encargado del tratamiento y personas que, bajo la autoridad directa del responsable del tratamiento o del encargado del tratamiento, estén autorizadas a tratar datos personales.

3. Ámbito

3.1. Ámbito material

- Estas NCV se aplican a las TID y al tratamiento realizado por los importadores de datos como resultado de dichas TID. También se aplicarán en lo sucesivo a las transferencias a terceros a entidades NCV y al tratamiento efectuado por estas como consecuencia de dichas transferencias a terceros.

3.2. Ámbito geográfico

3.2.1. Entidades y personal sujetos a las NCV

- Estas NCV son vinculantes para todas las entidades NCV y su personal. La lista actualizada de entidades NCV figura en el Anexo 1.
- La estructura del Grupo PROSEGUR se muestra en la dirección URL https://www.prosegur.com/en/about.
- Los datos de contacto de las entidades NCV se facilitan, por países, en las siguientes URL https://www.prosegur.com/en/legal-notice y https://www.prosegur.com/en/privacy-policy.
- El incumplimiento por parte del personal de cualquiera de las obligaciones contenidas en estas NCV se considera incumplimiento de las instrucciones de PROSEGUR o de las entidades NCV en su condición de empleadoras o empresarias. En este caso, PROSEGUR o las entidades NCV se reservan el derecho a ejercitar las acciones legales oportunas (incluyendo, sin carácter limitativo, acciones de índole laboral, civil, administrativa o penal), en relación con los daños y perjuicios ocasionados como consecuencia de dicho incumplimiento, y de conformidad con lo establecido en el convenio colectivo o en las cláusulas contractuales aplicables.

3.2.2. Actividades de tratamiento y datos personales sujetas a las NCV

- Las actividades de tratamiento de datos personales y de TID sujetas a las NCV se detallan en el Mapa de transferencia internacional de datos adjunto como Anexo 2 y se resumen a continuación:

PAÍSES	ESPACIO ECONÓMICO EUROPEO	FUERA DEL ESPACIO ECONÓMICO EUROPEO
Las NCV serán aplicables a las transferencias efectuadas entre entidades NCV establecidas en los siguientes países:	España; Alemania; Portugal	Argentina, Australia, Brasil, Canadá, Chile, Colombia, Costa Rica, Ecuador, El Salvador, Estados Unidos, Guatemala, Honduras, México, Nicaragua, Panamá,

		Paraguay, Perú, Reino Unido, Sudáfrica y Uruguay.

CATEGORÍAS DE INTERESADOS	CATEGORÍAS DE DATOS	OBJETOS
Empleados y sus beneficiarios/familiares (incluidos los menores)	Datos de identificación (nombre, apellidos, dirección, correo electrónico, fax, teléfono, DNI/pasaporte, firma) Características personales (estado civil, información familiar, fecha de nacimiento, lugar de nacimiento, edad, sexo, nacionalidad, lengua materna, etc.). Datos sobre salud Datos de circunstancias sociales (información sobre vivienda, propiedades, aficiones, asociaciones a las que pertenece, licencias y autorizaciones) Datos académicos y profesionales (CV y experiencia profesional, cualificaciones, datos del puesto) Datos económicos/financieros/de seguros (datos económicos de la nómina, ingresos, datos bancarios; información fiscal, seguros, plan de pensiones) Datos de transacciones de bienes y servicios (bienes y servicios recibidos por el interesado, transacciones financieras) Datos relativos a infracciones y faltas administrativas Datos relativos a las actas del consejo de administración de la empresa, poderes y contratos	Prestación de servicios informáticos entre empresas del Grupo PROSEGUR: (i) soporte y mantenimiento informático; (ii) herramientas/sistemas digitales globales; (iii) gestión de incidencias técnicas a diferentes áreas y negocios. Prestación de servicios de gestión de relaciones laborales y RR. HH. entre empresas del Grupo PROSEGUR: (i) Gestión de nóminas; (ii) Prevención de riesgos laborales Tareas de gestión de equipos efectuadas por los directivos en relación con las personas a su cargo, como, por ejemplo, apoyo a la contratación, formación, evaluación del rendimiento y promoción. Página web con información de Prosegur relacionada con noticias, listas de teléfonos, datos organizativos e información de la empresa. Creación de un identificador único para acceder a la red Prosegur Gestión de expatriados Auditoría (evaluación de los controles internos) Gestión del canal de denuncia de irregularidades Gestión de flotas Procesos contables, fiscales y financieros Contratos y gestión jurídica Gestión de riesgos Cumplimiento de obligaciones legales (por ejemplo, solicitud de Hacienda de retener una cantidad

		de dinero a un empleado para pagar una sanción de tráfico). Evaluar el coste contencioso o laboral de la empresa para la venta Gestión/cumplimiento de los derechos y obligaciones en materia de protección de datos (por ejemplo, solicitudes/reclamaciones del interesado)
Candidatos	Datos de identificación y contacto, características personales, circunstancias sociales, académicas y profesionales, datos laborales, económicos y financieros	Procesos de contratación Prestación de servicios informáticos entre empresas del Grupo PROSEGUR: (i) soporte técnico; (ii) gestión global de incidencias técnicas de herramientas/sistemas digitales. Gestión/cumplimiento de los derechos y obligaciones en materia de protección de datos (por ejemplo, solicitudes/reclamaciones del interesado)
Proveedores y representantes o personas de contacto de los proveedores	Datos de identificación y contacto, académicos y profesionales, laborales, económicos y financieros, transacciones de bienes y servicios, infracciones	Gestión de las relaciones con los proveedores, incluidos los aspectos contables, fiscales y jurídicos. Auditoría (evaluación de los controles internos) Gestión del canal de denuncia de irregularidades Prestación de servicios informáticos entre empresas del Grupo PROSEGUR: (i) soporte técnico; (ii) herramientas/sistemas digitales globales; gestión de incidencias técnicas a diferentes áreas y negocios. Cumplimiento de las obligaciones legales (por ejemplo, solicitud de las autoridades fiscales) Gestión de contratos Gestión de la cadena de suministro y compras

		Creación de un identificador único para acceder a la red Prosegur y proteger la red Prosegur Gestión/cumplimiento de los derechos y obligaciones en materia de protección de datos (por ejemplo, solicitudes/reclamaciones del interesado)
Usuarios, clientes, clientes potenciales y representantes o personas de contacto de clientes y clientes potenciales	Datos de identificación y contacto, información profesional, laboral, económica y financiera, transacciones de bienes y servicios, infracciones	Prestación de servicios informáticos entre empresas del Grupo PROSEGUR: (i) soporte técnico; (ii) herramientas/sistemas digitales globales; gestión de incidencias técnicas a diferentes áreas y negocios. Prestación de servicios comerciales entre empresas del Grupo PROSEGUR, incluidas visitas comerciales, acciones de fidelización de clientes, publicidad y prospección comercial, atención al cliente y gestión de siniestros. Prestación de servicios entre empresas del Grupo PROSEGUR para el negocio de Gelt: prestación de servicios de análisis de datos y gestión de bases de datos Gestión de las relaciones con los clientes, incluidos los aspectos contables, fiscales y jurídicos. Prestación de servicios a los clientes Auditoría (evaluación de los controles internos) Gestión del canal de denuncia de irregularidades Prevención del blanqueo de capitales Cumplimiento de las obligaciones legales (por ejemplo, solicitud de las autoridades fiscales)

		Gestión de contratos Gestión/cumplimiento de los derechos y obligaciones en materia de protección de datos (por ejemplo, solicitudes/reclamaciones del interesado)
Inquilinos y propietarios	Datos de identificación y contacto, académicos y profesionales, datos de empleo, información comercial	Gestión de inmuebles Gestión de contratos
Representantes, personas de contacto y empleados de las empresas destinatarias	Datos de identificación y contacto, características personales, particularidades académicas y profesionales, datos laborales, económicos y financieros	Evaluar el coste contencioso o laboral de la empresa para comprar Gestión de reclamaciones
Beneficiarios (incluidos los menores)	Datos de identificación y contacto, características personales, datos sobre la salud, particularidades académicas y profesionales, datos laborales, económicos y financieros	Prestación de servicios informáticos entre empresas del Grupo PROSEGUR: (i) asistencia técnica; (ii) herramientas/sistemas digitales globales; gestión de incidencias técnicas al sistema de la Fundación.

4. Objeto

- En el marco de las relaciones comerciales entre las distintas entidades que forman parte del Grupo, PROSEGUR tiene el firme compromiso de cumplir y respetar las leyes de privacidad, así como de respetar la protección de los datos personales que sean objeto de tratamiento en el desarrollo de su actividad, con el objetivo principal de proteger los derechos y libertades esenciales de las personas físicas, en particular su derecho a la intimidad y confidencialidad.

- Para dar cumplimiento a este compromiso y a sus obligaciones en materia de protección de datos, PROSEGUR ha establecido las presentes Normas Corporativas Vinculantes (en adelante, las «NCV») como parte integrante del Acuerdo NCV, que tiene por objeto regular las TID que puedan tener lugar en las entidades bajo su ámbito de aplicación y que se especifican en el Anexo 1 de estas NCV.

5. Versión pública

Este documento es la versión pública de las NCV que se publicará en las páginas web de las entidades NCV y se facilitará a cualquier persona que lo solicite.

6. Desarrollo

6.1. Principios del tratamiento de datos personales

6.1.1. Principios aplicables al tratamiento de datos personales

- El tratamiento de datos personales debe llevarse a cabo de conformidad con los siguientes principios:

6.1.1.1 Principio de legalidad

- El tratamiento de datos personales debe ser lícito. El tratamiento solo es lícito si y en la medida en que se cumpla al menos una de las siguientes condiciones:

  a) Los interesados han dado su consentimiento al tratamiento de sus datos personales para uno o más fines específicos.

  b) El tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte, o para tomar medidas a petición del interesado antes de celebrar un contrato;

  c) El tratamiento es necesario para el cumplimiento de una obligación legal a la que está sujeto el responsable del tratamiento.

  d) El tratamiento es necesario para proteger los intereses vitales del interesado o de otra persona física;

  e) El tratamiento es necesario para el cumplimiento de una misión de interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento;

  f) El tratamiento es necesario para los fines de los intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, salvo cuando prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un menor.

6.1.1.2 Imparcialidad y transparencia

- El tratamiento de datos personales debe realizarse de manera imparcial y transparente para los interesados. Los interesados deben ser informados de las circunstancias relativas al tratamiento de sus datos personales de forma accesible y comprensible, utilizando un lenguaje claro y sencillo, de conformidad con lo dispuesto en la Ley Europea de Protección de Datos.

6.1.1.3 Principio de limitación de la finalidad

- Los datos personales deben tratarse con fines determinados, explícitos y legítimos, y no deben tratarse posteriormente de manera incompatible con dichos fines.

6.1.1.4 Principio de reducción al mínimo de los datos

- Datos personales que deben ser adecuados, pertinentes y limitados a lo necesario para los fines para los que se recogen. La minimización de los datos se aplicará teniendo en cuenta la cantidad de datos recogidos, el alcance de su tratamiento y su periodo de conservación. El acceso a los

datos también se reducirá al mínimo, de modo que solo puedan acceder a ellos el personal o los destinatarios que necesiten tener conocimiento de los mismos para cumplir con sus obligaciones («necesidad de conocer»).

6.1.1.5 Principio de precisión

- Los datos personales tratados deben ser exactos y, en su caso, estar actualizados. Se tomarán todas las medidas razonables para garantizar que los datos personales que sean inexactos, teniendo en cuenta los fines para los que fueron tratados, se supriman o rectifiquen sin demora.

6.1.1.6 Principio de limitación del almacenamiento

- Los datos personales deben guardarse en un formato que impida la identificación de los interesados por un período superior al necesario para los fines del tratamiento de dichos datos personales.

6.1.1.7 Principio de integridad y confidencialidad

- Los datos personales se tratarán de forma que se garantice su adecuada seguridad, incluida la protección contra el tratamiento no autorizado o ilícito y contra la pérdida, destrucción o daño accidentales, mediante las correspondientes medidas técnicas u organizativas.

6.1.1.8 Principio de responsabilidad

- Las entidades NCV serán responsables y serán capaces de demostrar que cumplen todos los principios, derechos y obligaciones previstos en estas NCV. También son responsables del cumplimiento de estos principios, derechos y obligaciones, y de poder demostrarlo.

6.1.1.9 Protección de datos por diseño y de manera predeterminada

- Teniendo en cuenta por una parte el nivel tecnológico, el coste de aplicación y, por otra, la naturaleza, el alcance, el contexto y los fines del tratamiento, así como los riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas que entraña el tratamiento, las entidades NCV deberán, tanto en el momento de la determinación de los medios para el tratamiento como en el momento del propio tratamiento aplicar medidas técnicas y organizativas apropiadas, como la seudonimización, destinadas a aplicar de manera efectiva los principios de protección de datos, como la minimización de datos, y a integrar en el tratamiento las garantías necesarias para cumplir los requisitos de la normativa europea de protección de datos y proteger los derechos de los interesados.

- El tratamiento debe incorporar desde el principio las medidas técnicas y organizativas que posibiliten la aplicación efectiva de los principios establecidos en la normativa europea de protección de datos, el cumplimiento de sus requisitos y la protección de los derechos de los interesados.

- Se adoptarán medidas para garantizar que, de forma predeterminada, solo se traten los datos personales que sean necesarios para cada finalidad específica de la actividad de tratamiento. La obligación de aplicar dichas medidas se aplica a la cantidad de datos personales recopilados, el alcance de su tratamiento, el periodo de almacenamiento y su accesibilidad. En particular, las

medidas deben garantizar que, por defecto, los datos personales no sean accesibles, sin intervención de la persona, a un número indeterminado de personas.

- Es decir, desde la concepción de un nuevo proyecto, sistema, herramienta o proceso en el que se prevea el tratamiento de datos personales, las entidades NCV deben tener en cuenta la protección de dichos datos personales, y adoptar decisiones y medidas que garanticen el cumplimiento de la normativa europea de protección de datos y limiten el tratamiento de los datos personales a lo estrictamente necesario.

6.1.2. Tratamiento de categorías especiales de datos personales

- Se prohíbe el tratamiento de categorías especiales de datos personales, a menos que se cumpla una de las siguientes condiciones:

  a) el interesado ha dado su consentimiento explícito al tratamiento de dichos datos personales para uno o varios fines específicos, salvo cuando la legislación europea establezca que el interesado no puede levantar la prohibición de tratamiento de dichos datos;

  b) El tratamiento es necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del interesado en el ámbito del derecho laboral, de la seguridad social y de la protección social, tal y como se establece en la legislación europea o en un convenio colectivo de conformidad con las leyes europeas que prevean garantías adecuadas para los derechos fundamentales y los propósitos del interesado.

  c) El tratamiento es necesario para proteger los intereses vitales del interesado o de otra persona física cuando dicho interesado presenta incapacidad física o jurídica para dar su consentimiento;

  d) El tratamiento es llevado a cabo en el curso de sus actividades legítimas con las garantías adecuadas por una fundación, asociación o cualquier otro organismo sin ánimo de lucro con fines políticos, filosóficos, religiosos o sindicales y a condición de que el tratamiento se refiera únicamente a los miembros o antiguos miembros del organismo o a las personas que tengan contacto habitual con él en relación con sus fines y que los datos personales no se divulguen fuera de dicho organismo sin el consentimiento de los interesados;

  e) El tratamiento se refiere a datos personales que el interesado hace manifiestamente públicos;

  f) El tratamiento es necesario para el establecimiento, ejercicio o defensa de acciones legales o reclamaciones o cuando los tribunales actúan en su capacidad judicial;

  g) El tratamiento resulta necesario debido a la relevancia de un interés público significativo, conforme a las normativas europeas, y debe estar adecuadamente ajustado al propósito perseguido. Esto conlleva respetar la esencia del derecho a la protección de datos y

establecer medidas concretas y apropiadas para garantizar la protección de los derechos fundamentales y propósitos del interesado.

h) El tratamiento es necesario con fines de medicina preventiva o del trabajo o de evaluación de la capacidad laboral del trabajador, de diagnóstico médico, de prestación de asistencia sanitaria o social o de tratamiento o gestión de sistemas y servicios de asistencia sanitaria o social, sobre la base de las leyes europeas o en virtud de un contrato con un profesional de la salud y cuando los datos personales son tratados por un profesional o bajo su responsabilidad o por cualquier otra persona sujeta a una obligación de secreto profesional en virtud de las leyes europeas o de las normas establecidas por los organismos nacionales competentes;

i) El tratamiento es necesario por razones de interés público en el ámbito de la salud pública, como la protección frente a amenazas transfronterizas graves para la salud o la garantía de un alto nivel de calidad y seguridad de la asistencia sanitaria y de los medicamentos o dispositivos médicos, sobre la base de las leyes europeas que prevén medidas apropiadas y específicas para proteger los derechos y libertades del interesado, en particular el secreto profesional;

j) El tratamiento es necesario para fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos basados en leyes europeas que deberán ser proporcionales al fin perseguido, respetar la esencia del derecho a la protección de datos y prever medidas adecuadas y específicas para salvaguardar los derechos fundamentales y los propósitos del interesado.

6.1.3. Medidas para garantizar la seguridad de los datos

- Las entidades NCV implantarán y aplicarán las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado, teniendo en cuenta el estado de la técnica, los costes de aplicación, la naturaleza, el alcance, el contexto y los fines del tratamiento, así como los riesgos a que esté expuesto el tratamiento y los efectos que pueda tener sobre los derechos y libertades de las personas físicas, ya se deriven de la acción humana o del medio físico o natural.

- Las medidas que se aplicarán incluyen, entre otras, las siguientes:

  a) seudonimización y cifrado de datos personales;

  b) capacidad para garantizar la continuidad de la confidencialidad, integridad, disponibilidad y resistencia de los sistemas y servicios de tratamiento;

  c) capacidad para restablecer rápidamente la disponibilidad y el acceso a los datos personales en caso de incidentes físicos o técnicos;

  d) Verificación, evaluación y valoración periódicas de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

- Las entidades NCV también tomarán medidas para garantizar que cualquier persona que actúe bajo su responsabilidad y que tenga acceso a datos personales solo pueda tratar dichos datos

personales siguiendo instrucciones del responsable del tratamiento, salvo que esté obligado a hacerlo en virtud de la legislación europea.

- Al evaluar el nivel adecuado de seguridad se tendrán en cuenta, en particular, los riesgos que presente el tratamiento, en especial los derivados de la destrucción, pérdida, alteración, comunicación o acceso no autorizados, accidentales o ilícitos, a los datos personales transmitidos, conservados o tratados de otra forma.

- La Política de Seguridad de la Información del Grupo PROSEGUR, adjunta como Anexo 3, constituye el marco para la definición, gestión, administración e implantación de los mecanismos y procedimientos necesarios para establecer niveles adecuados de seguridad de los activos de información del Grupo PROSEGUR y de sus clientes.

6.1.4. Modelo de gobernanza y cumplimiento en materia de protección de datos

- Las entidades NCV designarán un Delegado de Protección de Datos cuando: (i) sus actividades principales consistan en operaciones de tratamiento que, en virtud de su naturaleza, su alcance o sus fines, requieren un seguimiento habitual y sistemático de los interesados a gran escala; o (ii) sus actividades principales consistan en el tratamiento a gran escala de categorías de datos especiales con arreglo a la Cláusula 6.1.2 o de datos personales relativos a condenas e infracciones penales.

- Los Delegados de Protección de Datos tendrán como mínimo las siguientes funciones:

  a) informar y asesorar a las entidades NCV y al personal que lleva a cabo el tratamiento de sus obligaciones en virtud de estas NCV y de la legislación europea o de los Estados miembros en materia de protección de datos;

  b) supervisar el cumplimiento de estas NCV, de la legislación europea o de las disposiciones de los Estados miembros en materia de protección de datos y de las políticas de las entidades NCV en relación con la protección de datos personales, incluida la asignación de responsabilidades, la sensibilización y la formación del personal implicado en las operaciones de tratamiento, así como las auditorías correspondientes;

  c) proporcionar asesoramiento cuando se le solicite en relación con la Evaluación del impacto de la protección de datos y supervisar su ejecución de acuerdo con la Cláusula 6.1.8;

  d) colaborar con la autoridad de supervisión;

  e) actuar como punto de contacto para la autoridad en cuestiones relacionadas con el tratamiento, incluida la consulta previa de conformidad con las leyes europeas, y consultar, en su caso, con respecto a cualquier otro asunto.

- PROSEGUR ha designado (i) un Delegado de Protección de Datos corporativo del Grupo PROSEGUR («Delegado de Protección de Datos del Grupo») con la responsabilidad, entre otras, de supervisar el cumplimiento de las NCV con del máximo apoyo de la dirección para el cumplimiento de esta tarea; y (ii) Delegados de Protección de Datos Locales en los países del Espacio Económico Europeo en los que está presente el Grupo PROSEGUR, así como en Brasil y Uruguay [«Delegados de protección de datos locales»]. Los Delegados de Protección de Datos del Grupo y locales dependerán directamente del más alto nivel directivo de las entidades NCV.

- PROSEGUR también ha designado Oficiales de Cumplimiento locales de cumplimiento en aquellos países en los que no es obligatorio un Delegado de Protección de Datos Local en virtud de esta cláusula o de la legislación local. Estos Oficiales de Cumplimiento son responsables de la protección de datos a escala local, actúan como contactos y gestores en la gestión de cuestiones de protección de datos (incluidas, entre otras, las reclamaciones vinculadas a NCV) a escala local, informando a los equipos de gestión locales y al Delegado de Protección de Datos del Grupo.

- Tanto los Delegados de Protección de Datos como los Oficiales de Cumplimiento locales forman parte y reciben apoyo (i) del Comité Corporativo de Protección de Datos; (ii) del Comité de Privacidad (ejecutivo); (iii) del Responsable funcional de tratamiento y (iv) de los comprobadores de control, como se establece en el Modelo de gobernanza y cumplimiento en materia de protección de datos.

- El Anexo 4 proporciona información sobre la estructura del Modelo de gobernanza y cumplimiento en materia de protección de datos en el Grupo PROSEGUR, así como las responsabilidades de los equipos.

6.1.5. Encargados y subencargados del tratamiento de datos

- Cuando una entidad NCV que actúe como encargado del tratamiento desee subcontratar la prestación de servicios a un encargado del tratamiento (sea o no una entidad NCV), deberá recurrir en primer lugar solo a encargados del tratamiento que ofrezcan garantías suficientes para aplicar las medidas técnicas y organizativas apropiadas, de forma que el tratamiento cumpla los requisitos de las NCV y garantice la protección de los derechos de los interesados. Lo mismo es válido cuando una entidad NCV que actúa como encargada del tratamiento desea subcontratar a otra encargada del tratamiento, sea o no una entidad NCV (en lo sucesivo, las «subencargada» o las «subencargadas»).

- Dicho tratamiento por parte del encargado en nombre del responsable del tratamiento, se regirá por un contrato u otro acto jurídico con arreglo a la legislación europea, que sea vinculante para el encargado frente al responsable del tratamiento y que establezca el objeto y la duración del tratamiento, la naturaleza y la finalidad de este, el tipo de datos personales y las categorías de interesado, así como las obligaciones y los derechos del responsable del tratamiento («Acuerdo del encargado del tratamiento de datos»). El Acuerdo del encargado del tratamiento de datos, que podrá basarse, total o parcialmente, en cláusulas contractuales tipo, estipulará, en particular, que el encargado del tratamiento:

  a) trata los datos personales siguiendo solo instrucciones documentadas del responsable del tratamiento, incluso con respecto a las transferencias de datos personales a un tercer país o a una organización internacional, a menos que así lo exija la ley a la que está sujeto el responsable del tratamiento; en tal caso, el responsable del tratamiento informará al responsable del tratamiento de dicho requisito legal antes del tratamiento, a menos que dicha ley prohíba dicha información por motivos importantes de interés público;

  b) garantiza que las personas autorizadas a tratar los datos personales se han comprometido a mantener la confidencialidad o están sometidas a una obligación legal adecuada de confidencialidad;

  c) adopta todas las medidas exigidas en virtud de la Cláusula 6.1.3;

d) cumple las condiciones siguientes: (i) El encargado del tratamiento no contratará a otro encargado del tratamiento sin la previa autorización específica o general por escrito del responsable del tratamiento. En el caso de una autorización general por escrito, el encargado del tratamiento informará al responsable del tratamiento de cualquier cambio previsto en relación con la adición o sustitución de otros encargados del tratamiento, dando así al responsable del tratamiento la oportunidad de oponerse a dichos cambios; y (ii) cuando un encargado del tratamiento contrate a otro para llevar a cabo actividades específicas de tratamiento en nombre del responsable del tratamiento, se impondrán a ese otro encargado las mismas obligaciones en materia de protección de datos que las establecidas en el Acuerdo del encargado del tratamiento de datos entre el responsable y el encargado mediante un contrato u otro acto jurídico con arreglo a la ley, en particular proporcionando garantías suficientes para aplicar las medidas técnicas y organizativas adecuadas de tal modo que el tratamiento cumpla los requisitos de estas NCV. Si ese otro Encargado incumple sus obligaciones en materia de protección de datos, el Encargado inicial seguirá siendo plenamente responsable ante el responsable del tratamiento del cumplimiento de las obligaciones de ese otro encargado.

e) habida cuenta de la naturaleza del tratamiento, asiste al responsable del tratamiento con medidas técnicas y organizativas apropiadas, en la medida en que ello sea posible, para el cumplimiento de la obligación del responsable del tratamiento de responder a las solicitudes de ejercicio de los derechos del interesado establecidos en la Cláusula 6.3;

f) ayuda al responsable del tratamiento a garantizar el cumplimiento de las obligaciones previstas en las cláusulas 6.1.3. y 6.1.6 a 6.1.8., teniendo en cuenta la naturaleza del tratamiento y la información de que dispone el encargado del tratamiento;

g) a elección del responsable del tratamiento, suprime o devuelve todos los datos personales al responsable del tratamiento una vez finalizada la prestación de servicios relacionados con el tratamiento, y elimina las copias existentes, a menos que la ley exija la conservación de los datos personales;

h) pone a disposición del responsable del tratamiento toda la información necesaria para demostrar el cumplimiento de las obligaciones establecidas en la presente cláusula y permita y contribuya a las auditorías, incluidas las inspecciones, realizadas por el responsable del tratamiento u otro auditor encargado por el responsable del tratamiento.

i) el encargado del tratamiento informará inmediatamente al responsable del tratamiento si, en su opinión, una instrucción infringe estas NCV o cualquier disposición de la legislación europea en materia de protección de datos.

- Cuando una entidad NCV desee subcontratar con un subencargado la totalidad o parte de los servicios contratados, deberá obtener previamente la autorización escrita, específica o general, del responsable del tratamiento. Cuando los representantes del responsable del tratamiento le autoricen a recurrir a otro encargado del tratamiento, el subencargado del tratamiento estará sujeto contractualmente, como mínimo, a las mismas obligaciones que las estipuladas en el Acuerdo del encargado del tratamiento de datos, de conformidad con lo dispuesto en estas NCV.

- El encargado del tratamiento responde ante el responsable del tratamiento y debe asegurarse de que el subencargado del tratamiento satisface correctamente las obligaciones de protección de datos.

- El encargado del tratamiento se compromete a notificar al responsable del tratamiento, con antelación y por medio fehaciente, cualquier cambio previsto en cuanto a la incorporación o sustitución de encargados del tratamiento, dando al responsable del tratamiento la oportunidad de oponerse a dichos cambios.

- A los efectos anteriores, las entidades NCV deberán observar y cumplir la Política de selección y evaluación de proveedores del Grupo PROSEGUR, que se adjunta como Anexo 5. Asimismo, se observará lo dispuesto en la Cláusula 6.2 de estas NCV.

6.1.6. Fallos de seguridad de los datos personales

- Si se produce, o se sospecha que se ha producido, un fallo de seguridad que pueda afectar a los datos personales, la persona que lo detecte informará inmediatamente al Delegado de Protección de Datos Local/Oficial de Cumplimiento Local; y este informará inmediatamente a PROSEGUR (a través del Delegado de Protección de Datos del Grupo), de acuerdo con el Protocolo de gestión y notificación de fallos de seguridad de datos personales, que se adjunta como Anexo 6.

- Entre otras obligaciones, debe conservarse un registro escrito que documente los hechos relativos al fallo de seguridad de los datos personales, sus efectos y las medidas correctoras adoptadas, y debe ponerse a disposición de las autoridades competentes a petición de estas.

- Las entidades NCV que actúen como responsables del tratamiento deberán notificar a la autoridad supervisora competente cualquier fallo de seguridad de datos personales, salvo que sea improbable que dichos fallos supongan un riesgo para los derechos y libertades de los interesados. La notificación deberá efectuarse sin dilación y, a ser posible, en un plazo de 72 horas a partir del momento en que el responsable del tratamiento tenga conocimiento del fallo de seguridad en los datos personales. También se informará a los interesados, sin dilaciones indebidas, cuando sea probable que el fallo de seguridad de los datos personales entrañe un alto riesgo para sus derechos y libertades.

- Cuando una Entidad NCV que actúe como Encargado del Tratamiento se vea involucrada en un fallo de datos personales, dicha Entidad informará inmediatamente a PROSEGUR (a través del Delegado de protección de datos del Grupo), que será el encargado de notificarlo a la entidad NCV que actúe como responsable del tratamiento, sin dilaciones indebidas, para que se efectúen, en su caso, las notificaciones exigidas por estas NCV.

6.1.7. Registro de las actividades de tratamiento

- Las entidades NCV que actúen como responsables del tratamiento deberán mantener, por escrito (incluido, pero no limitado a un formulario electrónico), un registro de las actividades de tratamiento (RAT) de datos personales llevadas a cabo bajo su responsabilidad, y mantenerlo actualizado y facilitarlo a las autoridades de supervisión cuando estas lo soliciten. El RAT deberá contener la siguiente información:

a) nombre y datos de contacto del responsable del tratamiento; y si procede, los del corresponsable del tratamiento, del representante del responsable del tratamiento y del Delegado de Protección de Datos Local o del Grupo;

b) la finalidad del tratamiento;

c) una descripción de las categorías de interesados y las categorías de datos personales;

d) las categorías de destinatarios a los que se han comunicado o se comunicarán los datos personales, incluidos los destinatarios de terceros países y organizaciones internacionales;

e) en su caso, las transferencias de datos personales a un tercer país u organización internacional, incluida la identificación del tercer país u organización internacional destinatarios de los datos y, en su caso, la documentación de las garantías adecuadas;

f) cuando sea posible, los plazos previstos para la eliminación de las distintas categorías de datos;

g) cuando sea posible, una descripción general de las medidas de seguridad técnicas y organizativas mencionadas en la Cláusula 6.1.3 de estas NCV.

- Las entidades NCV que actúen como encargados del tratamiento y, en su caso, el representante del encargado, mantendrán un RAT de todas las categorías de actividades de tratamiento realizadas en nombre de un responsable, que contenga:

a) el nombre y los datos de contacto del encargado o encargados del tratamiento y de cada uno de los responsables del tratamiento en nombre de los cuales actúe el encargado, así como, en su caso, del representante del encargado o encargados del tratamiento y del Delegado de Protección de Datos Local o del Grupo;

b) las categorías de tratamiento efectuadas en nombre de cada responsable;

c) cuando proceda, las transferencias de datos personales a un tercer país o a una organización internacional, incluida la identificación de dicho tercer país u organización internacional y, en el caso de las transferencias mencionadas en el segundo párrafo de la Cláusula 6.2.1 de estas NCV, la documentación de las garantías adecuadas;

d) cuando sea posible, una descripción general de las medidas de seguridad técnicas y organizativas mencionadas en la Cláusula 6.1.3 de estas NCV.

6.1.8. Evaluaciones de impacto de la protección de datos

- Las entidades NCV llevarán a cabo una Evaluación del impacto de la protección de datos (en adelante, «EIPD») antes de iniciar el tratamiento de datos personales, cuando un determinado tipo de tratamiento implique un alto riesgo para los derechos y libertades de los interesados.

- Dichas evaluaciones se prepararán de acuerdo con la metodología establecida por el Grupo PROSEGUR, con el asesoramiento del Delegado de Protección de Datos del Grupo o Local,

cuando haya sido designado. Su finalidad es evaluar la necesidad y proporcionalidad del Tratamiento, identificar los riesgos y establecer las medidas necesarias para mitigarlos.

- A tal efecto, las entidades NCV deberán observar y cumplir el Protocolo de gestión de la EIPD del Grupo PROSEGUR, que se adjunta como Anexo 7.

- Cuando, tras realizar una EIPD, una entidad NCV identifique un riesgo elevado que no pueda mitigarse, consultará a la autoridad de supervisión pertinente antes de llevar a cabo el tratamiento previsto.

6.2. Requisitos para la divulgación de datos personales

6.2.1. Transferencias internacionales de datos

- Los datos personales no podrán transferirse fuera del EEE si no se cumplen los siguientes requisitos:

  a) la entidad importadora de datos está sujeta a estas NCV y puede cumplirlas. Para mayor claridad, estas NCV solo son aplicables a las TID entre entidades del Grupo PROSEGUR que se hayan adherido a ellas; o

  b) la Comisión Europea ha decidido que el tercer país en el que se encuentra la importadora de datos garantiza un nivel de protección adecuado; o bien

  c) si el país en el que se encuentra la importadora de datos no dispone de un nivel de protección adecuado en virtud de una decisión de adecuación de la Comisión Europea, las entidades NCV adoptarán las medidas de salvaguardia apropiadas, y a condición de que los interesados dispongan de derechos exigibles y de recursos legales efectivos. Se considerarán salvaguardias adecuadas los siguientes mecanismos:

     i. Cláusulas contractuales tipo

     ii. Código de conducta aprobado de conformidad con el RGPD, junto con compromisos vinculantes y exigibles del responsable o encargado del tratamiento en el tercer país de aplicar las salvaguardias adecuadas, incluso en lo que respecta a los derechos de los interesados.

     iii. Mecanismo de certificación aprobado de conformidad con el RGPD, junto con compromisos vinculantes y exigibles del responsable o encargado del tratamiento en el tercer país de aplicar las salvaguardias adecuadas, incluso en lo que respecta a los derechos de los interesados.

     iv. Instrumento jurídicamente vinculante y ejecutorio entre autoridades u organismos públicos.

- Si no se cumple ninguno de esos requisitos, una transferencia o un conjunto de transferencias de datos personales fuera del EEE solo tendrá lugar en una de las siguientes condiciones:

a) la transferencia ha sido previamente autorizada por la autoridad supervisora competente sobre la base de la aplicación de las garantías adecuadas mediante cláusulas contractuales entre el responsable o el encargado y el responsable, el encargado o el destinatario de los datos personales en el tercer país u organización internacional.

b) existe una sentencia de un juzgado o tribunal o una decisión de una autoridad administrativa de un tercer país que obligue al responsable o al encargado del tratamiento a transferir o revelar datos personales en virtud de un acuerdo internacional, como un tratado de asistencia judicial mutua, vigente entre el tercer país solicitante y la Unión Europea o un Estado miembro;

c) el interesado ha dado su consentimiento explícito a la transferencia propuesta, tras haber sido informado de los posibles riesgos de dichas transferencias para el interesado debido a la ausencia de una decisión de adecuación y de garantías apropiadas;

d) la transferencia es necesaria (i) para la ejecución de un contrato entre el interesado y el responsable o para la aplicación de medidas precontractuales adoptadas a petición del interesado; (ii) para la celebración o ejecución de un contrato celebrado en interés del interesado entre el responsable y otra persona física o jurídica; (iii) por motivos importantes de interés público reconocidos por el derecho de la Unión Europea o de los Estados miembros; (iv) para la formulación, el ejercicio o la defensa de reclamaciones judiciales; o (v) para proteger los intereses vitales del interesado o de otras personas, cuando el interesado esté física o jurídicamente incapacitado para dar su consentimiento;

e) solo si la transferencia (i) no es repetitiva, (ii) afecta solo a un número limitado de interesados, (iii) es necesaria para la satisfacción de intereses legítimos imperiosos perseguidos por el responsable del tratamiento sobre los que no prevalezcan los intereses o los derechos y libertades del interesado, y (iv) el responsable del tratamiento ha evaluado todas las circunstancias que concurren en la transferencia de datos y, sobre la base de dicha evaluación, ha previsto garantías adecuadas con respecto a la protección de los datos personales. En este caso, el responsable del tratamiento informará de la transferencia a la autoridad de supervisión. El responsable del tratamiento, además de facilitar la información a que se refiere la Cláusula 6.3.1, informará al interesado de la transferencia y de los intereses legítimos apremiantes que se persiguen.

6.2.2. Transferencias a terceros

6.2.2.1 Cuando el destinatario es una entidad NCV

En general, deberán cumplirse y respetarse los requisitos establecidos en la Cláusula **6.2.1** anterior. En caso de duda, la importadora de datos deberá informar a la exportadora de datos y obtener su autorización expresa.

6.2.2.2 Cuando el destinatario no es una entidad NCV

La importadora de datos informará a la exportadora de datos, verificará si alguno de los mecanismos o excepciones contenidos en la sección 5.8.4 del Anexo 5 del presente documento es aplicable a la transferencia a terceros y obtendrá la autorización de la exportadora de datos.

6.2.3. Relaciones con el encargado del tratamiento

Cuando la comunicación de datos se base en una relación de encargado del tratamiento, esta relación se formalizará por escrito, según la plantilla de Acuerdo del encargado del tratamiento de datos del Grupo PROSEGUR y teniendo en cuenta la Política de selección y evaluación de proveedores, que se adjunta como Anexo 5.

6.3. Derechos de los interesados

6.3.1. Información:

- Los responsables del tratamiento están obligados a facilitar información a los interesados, según se detalla en el presente documento:

a) En el momento en que se recaben los datos personales del interesado, este deberá recibir toda la información indicada a continuación:

(i) la identidad y los datos de contacto del responsable y, en su caso, del representante del responsable;

(ii) los datos de contacto del Delegado de Protección de Datos, si procede;

(iii) los fines del tratamiento a que se destinan los datos personales, así como la base jurídica del tratamiento;

(iv) cuando el tratamiento se base en un interés legítimo, los intereses legítimos perseguidos por el responsable del tratamiento o por un tercero;

(v) los destinatarios o categorías de destinatarios de los datos personales, en su caso;

(vi) cuando proceda, el hecho de que el responsable del tratamiento tiene la intención de transferir datos personales a un tercer país o a una organización internacional y la existencia o ausencia de una decisión de adecuación o la referencia a las garantías apropiadas o adecuadas y los medios para obtener una copia de estas o si están disponibles.

Además de la información anterior, el responsable del tratamiento, en el momento de la obtención de los datos personales, facilitará al interesado la siguiente información adicional necesaria para garantizar un tratamiento leal y transparente:

(i) el periodo durante el cual se almacenarán los datos personales o, si esto no fuera posible, los criterios utilizados para determinar dicho periodo;

(ii) la existencia del derecho a solicitar al responsable del tratamiento el acceso y la rectificación o borrado de los datos personales o la limitación del tratamiento en

relación con el interesado o a oponerse al tratamiento, así como el derecho a la portabilidad de los datos;

(iii) cuando el tratamiento se base en el consentimiento del interesado, la existencia del derecho a retirar el consentimiento en cualquier momento, sin que ello afecte a la licitud del tratamiento basado en el consentimiento previo a su retirada;

(iv) el derecho a presentar una reclamación ante una autoridad de supervisión;

(v) si el suministro de datos personales es un requisito legal o contractual, o un requisito necesario para la celebración de un contrato, así como si el interesado está obligado a facilitar los datos personales y las posibles consecuencias de no facilitarlos;

(vi) cuando proceda, la existencia de una toma de decisiones automatizada, incluida la elaboración de perfiles y, al menos en tales casos, información significativa sobre la lógica implicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado.

Cuando el responsable del tratamiento tenga la intención de seguir tratando los datos personales con una finalidad distinta de aquella para la que se recogieron, el responsable del tratamiento facilitará al interesado, antes de ese tratamiento posterior, información sobre esa otra finalidad y cualquier otra información pertinente a la que se ha hecho referencia anteriormente.

b) Cuando no se hayan obtenido los datos personales del interesado, el responsable del tratamiento le facilitará la siguiente información:

(i) la identidad y los datos de contacto del responsable y, en su caso, del representante del responsable;

(ii) los datos de contacto del Delegado de Protección de Datos, si procede;

(iii) los fines del tratamiento a que se destinan los datos personales, así como la base jurídica del tratamiento;

(iv) las categorías de datos personales de que se trate;

(v) los destinatarios o categorías de destinatarios de los datos personales, en su caso;

(vi) cuando proceda, el hecho de que el responsable del tratamiento tiene la intención de transferir datos personales a un tercer país o a una organización internacional y la existencia o ausencia de una decisión de adecuación o la referencia a las garantías apropiadas o adecuadas y los medios para obtener una copia de estas o si están disponibles.

Además de la información anterior, el responsable del tratamiento, en el momento de la obtención de los datos personales, facilitará al interesado la siguiente información adicional necesaria para garantizar un tratamiento leal y transparente:

(i) el periodo durante el cual se almacenarán los datos personales o, si esto no fuera posible, los criterios utilizados para determinar dicho periodo;

(ii) cuando el tratamiento se base en un interés legítimo del responsable, los intereses legítimos perseguidos por el responsable del tratamiento o por un tercero;

(iii) la existencia del derecho a solicitar al responsable del tratamiento el acceso y la rectificación o borrado de los datos personales o la limitación del tratamiento en relación con el interesado o a oponerse al tratamiento, así como el derecho a la portabilidad de los datos;

(iii) cuando el tratamiento se base en el consentimiento del interesado, la existencia del derecho a retirar el consentimiento en cualquier momento, sin que ello afecte a la licitud del tratamiento basado en el consentimiento previo a su retirada;

(v) el derecho a presentar una reclamación ante una autoridad de supervisión;

(vi) de qué fuente proceden los datos personales y, en su caso, si proceden de fuentes de acceso público;

(vii) cuando proceda, la existencia de una toma de decisiones automatizada, incluida la elaboración de perfiles y, al menos en tales casos, información significativa sobre la lógica implicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado.

El responsable del tratamiento facilitará la información mencionada en los párrafos anteriores: (a) en un plazo razonable tras la obtención de los datos personales, pero a más tardar en el plazo de un mes, teniendo en cuenta las circunstancias específicas en las que se tratan los datos personales; (b) si los datos personales van a utilizarse para la comunicación con el interesado, a más tardar en el momento de la primera comunicación a dicho interesado; o (c) si está prevista una comunicación a otro destinatario, a más tardar en el momento de la primera comunicación de los datos personales.

Cuando el responsable del tratamiento tenga la intención de seguir tratando los datos personales con una finalidad distinta de aquella para la que se recogieron, el responsable del tratamiento facilitará al interesado, antes de ese tratamiento posterior, información sobre esa otra finalidad y cualquier otra información pertinente a la que se ha hecho referencia en el párrafo 2 de la Cláusula 6.3.1(b).

Los párrafos anteriores de esta Cláusula 6.3.1(b) no se aplicarán siempre y cuando:

(i) el interesado ya dispone de la información;

(ii) el suministro de dicha información resulte imposible o suponga un esfuerzo desproporcionado, en particular para el tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, o en la medida en que la obligación mencionada en el párrafo primero del presente apartado (b) pueda imposibilitar o perjudicar gravemente la consecución de los fines de dicho tratamiento. En tales casos, el responsable del tratamiento adoptará las medidas adecuadas para proteger los derechos y libertades y los intereses legítimos del interesado, incluida la puesta a disposición del público de la información;

(iii) la recogida o divulgación está expresamente prevista por la legislación europea o de los Estados miembros a la que está sujeto el responsable del tratamiento y que establece medidas adecuadas para proteger los intereses legítimos del interesado; o bien,

(iv) cuando los datos personales deban permanecer confidenciales sujetos a una obligación de secreto profesional regulada por la legislación europea o de los Estados miembros, incluida una obligación legal de secreto.

6.3.2. Otros derechos

- Los interesados podrán ejercer los siguientes derechos:

(i) **Acceso**: confirmar si se están tratando o no datos personales que les conciernen y solicitar información sobre qué datos personales concretos se están tratando y, en tal caso, acceder a los datos personales y a la siguiente información:

a) la finalidad del tratamiento;
b) las categorías de datos personales de que se trate;
c) los destinatarios o categorías de destinatarios a los que se han comunicado o se comunicarán los datos personales, en particular destinatarios de terceros países u organizaciones internacionales. Cuando los datos personales se transfieran a un tercer país o a una organización internacional, el interesado tendrá derecho a ser informado de las garantías adecuadas de conformidad con la Cláusula 6.2.1. relativa a la transferencia.
d) cuando sea posible, el periodo previsto durante el cual se almacenarán los datos personales o, cuando no lo sea, los criterios utilizados para determinar dicho periodo;
e) la existencia del derecho a solicitar al responsable del tratamiento la rectificación o borrado de los datos personales o la limitación del tratamiento de los datos personales que conciernan al interesado o a oponerse a dicho tratamiento;
f) el derecho a presentar una reclamación ante una autoridad de supervisión;
g) cuando los datos personales no se recaben del interesado, cualquier información disponible sobre su origen;
h) la existencia de una toma de decisiones automatizada, incluida la elaboración de perfiles y, al menos en tales casos, información significativa sobre la lógica implicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado.

El responsable del tratamiento facilitará una copia de los datos personales objeto de tratamiento. Por cualquier otra copia solicitada por el interesado, el responsable podrá cobrar una tasa razonable basada en los costes administrativos. Cuando el interesado realice la solicitud por medios electrónicos, y salvo que solicite lo contrario, la información se facilitará en un formato electrónico de uso común.

El derecho a obtener una copia no afectará negativamente a los derechos y libertades de los demás.

(ii) **Rectificación**: obtener del responsable del tratamiento, sin dilación indebida, la rectificación de los datos personales inexactos que le conciernan. Teniendo en cuenta los fines del tratamiento, el interesado tendrá derecho a que se completen los datos personales, incluso mediante la presentación de una declaración complementaria.

(iii) **Borrado (derecho al olvido)**: El interesado tendrá derecho a obtener del responsable del tratamiento el borrado de los datos personales que le conciernan sin dilación indebida, y el responsable tendrá la obligación de suprimir los datos personales sin dilación indebida cuando concurra uno de los motivos siguientes:

a) los datos personales ya no son necesarios en relación con los fines para los que fueron recogidos o tratados de otro modo;
b) el interesado retira el consentimiento en el que se basa el tratamiento de acuerdo con la Cláusula 6.1.1.1., o la Cláusula 6.1.2., y cuando no exista otro fundamento jurídico para el tratamiento;
c) el interesado se opone al tratamiento de conformidad con el punto (vi);
d) los datos personales han sido objeto de un tratamiento ilícito;
e) los datos personales tienen que ser borrados para cumplir con una obligación legal de la legislación europea a la que está sujeto el responsable;
f) los datos personales se han recogido en relación con la oferta de servicios de la sociedad de la información directamente a un niño.

Cuando el responsable del tratamiento haya hecho públicos los datos personales y esté obligado a borrarlos, el responsable del tratamiento, teniendo en cuenta la tecnología disponible y el coste de su aplicación, adoptará medidas razonables, incluidas medidas técnicas, para informar a los responsables que estén tratando los datos personales de que el interesado ha solicitado que dichos responsables borren cualquier enlace a esos datos personales o cualquier copia o réplica de ellos.

El derecho al borrado de los datos no se aplicará en la medida en que el tratamiento sea necesario:

a) por ejercer el derecho a la libertad de expresión e información;
b) para el cumplimiento de una obligación legal que requiera el tratamiento por parte de la legislación europea a la que esté sujeto el responsable del tratamiento o para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento;
c) por razones de interés público en el ámbito de la salud pública, de conformidad con la Cláusula 6.1.2.

d) para fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos de conformidad con la legislación europea, en la medida en que este derecho pueda hacer imposible o perjudicar gravemente la consecución de los objetivos de dicho tratamiento; o bien
e) para el establecimiento, ejercicio o defensa de reclamaciones legales.

(iv) **Restricción del tratamiento**: El interesado tendrá derecho a obtener del responsable del tratamiento la limitación del tratamiento cuando concurra alguna de las siguientes circunstancias:

a) el interesado impugne la exactitud de los datos personales, durante un plazo que permita al responsable verificar la exactitud de los datos personales;
b) el tratamiento es ilícito y el interesado se opone al borrado de los datos personales y solicita en su lugar la limitación de su uso;
c) el responsable ya no necesita los datos personales para los fines del tratamiento, pero el interesado los necesita para el reconocimiento, el ejercicio o la defensa de un derecho en un procedimiento judicial;
d) el interesado se ha opuesto al tratamiento a la espera de que se verifique si los motivos legítimos del responsable prevalecen sobre los del interesado.

Cuando se haya restringido el tratamiento, dichos datos personales, con excepción del almacenamiento, solo se tratarán con el consentimiento del interesado o para el reconocimiento, ejercicio o defensa de un derecho en un procedimiento judicial o para la protección de los derechos de otra persona física o jurídica, o por razones de interés público importantes de la Unión Europea o de un Estado miembro.

El interesado que haya obtenido la limitación del tratamiento será informado por el responsable antes de que se levante dicha limitación.

(v) **Portabilidad de los datos**: Los interesados tendrán derecho a recibir los datos personales que les conciernan, que hayan facilitado a un responsable del tratamiento, en un formato estructurado, de uso común y lectura por ordenador, y tendrán derecho a transmitir dichos datos a otro responsable del tratamiento sin impedimentos por parte del responsable al que se hayan facilitado los datos personales, cuando: a) el tratamiento se basa en el consentimiento o en un contrato de conformidad con las cláusulas 6.1.1.1. y 6.1.2.; y b) el tratamiento se lleva a cabo por medios automatizados.

En el ejercicio de su derecho a la portabilidad de los datos, los interesados tendrán derecho a que los datos personales se transmitan directamente de un responsable del tratamiento a otro, siempre que sea técnicamente posible.

El ejercicio del derecho a la portabilidad de los datos deberá (a) entender sin perjuicio del derecho al borrado de los datos. Este derecho no se aplicará al tratamiento necesario para el cumplimiento de una misión de interés público o inherente al ejercicio del poder público conferido al responsable del tratamiento, y b) no afectar negativamente a los derechos y libertades de terceros.

(vi) **Derecho a oposición**: Los interesados tendrán derecho a oponerse en cualquier momento, por motivos relacionados con su situación particular, al tratamiento de los datos personales que les conciernan basado en las letras e) o f) de la Cláusula 6.1.1.1., incluida la elaboración de perfiles basada en dichas disposiciones. El responsable del tratamiento dejará de tratar los datos personales a menos que demuestre motivos legítimos imperiosos para el tratamiento que prevalezcan sobre los intereses, derechos y libertades del interesado o para la interposición, el ejercicio o la defensa de acciones judiciales.

Cuando se traten datos personales con fines de comercialización directa, el interesado tendrá derecho a oponerse en cualquier momento al tratamiento de los datos personales que le conciernan para dicha comercialización, lo que incluye la elaboración de perfiles en la medida en que esté relacionada con dicha comercialización directa.

Cuando el interesado se oponga al tratamiento con fines de comercialización directa, los datos personales dejarán de tratarse con dichos fines.

A más tardar en el momento de la primera comunicación con el interesado, el derecho al que se hace referencia se pondrá explícitamente en conocimiento del interesado y se presentará de forma clara y separada de cualquier otra información.

En el contexto de la utilización de los servicios de la sociedad de la información, el interesado podrá ejercer su derecho de oposición por medios automatizados utilizando especificaciones técnicas. Cuando los datos personales sean tratados con fines de investigación científica o histórica o con fines estadísticos, el interesado, por motivos relacionados con su situación particular, tendrá derecho a oponerse al tratamiento de los datos personales que le conciernan, salvo que dicho tratamiento sea necesario para el cumplimiento de una misión realizada por razones de interés público.

- El responsable del tratamiento comunicará cualquier rectificación o borrado de datos personales o restricción del tratamiento llevada a cabo de conformidad con la presente cláusula a cada destinatario al que se hayan revelado los datos personales, salvo que ello resulte imposible o implique un esfuerzo desproporcionado. El responsable informará al interesado sobre dichos destinatarios si el titular así lo solicita.

6.3.3. Derecho a oponerse ante una toma de decisiones individual automatizada

- Los interesados tienen derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado de sus datos personales, como la elaboración de perfiles, que tenga efectos jurídicos sobre ellos o les afecte de forma similar de manera significativa («decisiones individuales automatizadas»), a menos que se aplique alguna de las siguientes excepciones: (i) la decisión es necesaria para celebrar o ejecutar un contrato entre el titular de los datos y un responsable del tratamiento; (ii) la decisión está autorizada por la legislación europea a la que está sujeto el responsable del tratamiento y que también prevé medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado; o (iii) la decisión se basa en el consentimiento explícito del interesado.

- En las excepciones mencionadas en los puntos (i) y (iii) anteriores, el responsable del tratamiento aplicará las medidas adecuadas para salvaguardar los derechos y libertades y

los intereses legítimos del interesado, al menos el derecho a obtener la intervención humana del responsable del tratamiento, a expresar su punto de vista y a impugnar la decisión.

- Además, las decisiones en virtud de las excepciones (i) a (iii) no se basarán en categorías especiales de datos personales, a menos que se apliquen las condiciones de la Cláusula 6.1.2 y existan medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado.

6.3.4. Derecho a presentar una reclamación

- Los interesados tienen derecho a presentar una reclamación ante la autoridad de supervisión competente si consideran que el tratamiento de sus datos personales infringe estas NCV. En particular, ante la autoridad de supervisión (i) del Estado miembro de su residencia habitual; (ii) del Estado miembro en el que tenga un lugar de trabajo; o (iii) del Estado miembro en el que se haya producido la presunta infracción.

6.3.5. Derecho a un recurso judicial efectivo

- Los interesados tienen derecho a un recurso judicial efectivo en relación con los encargados del tratamiento o los responsables del tratamiento cuando los interesados consideren que se han vulnerado sus derechos en virtud de las presentes NCV como consecuencia del tratamiento de sus datos personales y sin perjuicio de cualquier recurso administrativo o extrajudicial disponible. Las acciones contra un responsable o un encargado del tratamiento se ejercitarán, a elección del interesado, ante los tribunales del Estado miembro en el que el responsable o el encargado del tratamiento estén establecidos o ante los tribunales del Estado miembro en el que el interesado tenga su residencia habitual.

- Cuando la infracción haya sido causada por una entidad NCV establecida fuera del EEE, se aplicará la Cláusula 6.7.

6.3.6. Procedimiento para el ejercicio de los derechos del interesado

- Los interesados podrán ejercitar los derechos previstos en los apartados 6.3.2 y 6.3.3 o presentar una reclamación dirigiendo una solicitud por escrito a la dirección postal de la entidad NCV que actúe como responsable del tratamiento, a las direcciones de correo electrónico indicadas en las políticas de privacidad de las entidades NCV o a la siguiente dirección de correo electrónico oficina.privacidad@prosegur.com. Si la entidad NCV tiene dudas razonables sobre la identidad del interesado que formula la solicitud, la entidad NCV podrá solicitar la información adicional necesaria para confirmar la identidad del interesado.

- Los interesados deben recibir una respuesta a los derechos que ejercen sin demora y, en cualquier caso, en el plazo de un (1) mes a partir de la recepción de la solicitud. Este plazo podrá prorrogarse otros dos (2) meses, cuando sea necesario, en función de la complejidad y el número de solicitudes recibidas. Se informará al interesado de dicha prórroga en el plazo de un (1) mes a partir de la recepción de la solicitud, con la indicación de los motivos del retraso.

- Los interesados recibirán una respuesta, en la que se acepte o rechace la solicitud o la reclamación. También se informará a los interesados de que, si no están satisfechos con la respuesta recibida, tienen derecho a presentar una reclamación ante la autoridad de

supervisión competente, así como a interponer un recurso judicial efectivo, de conformidad con las cláusulas 6.3.4 y 6.3.5 anteriores.

6.4. Derechos de terceros beneficiarios

- Las entidades NCV acuerdan y aceptan expresamente que los interesados tienen derecho a hacer valer esta cláusula y las cláusulas 6.1.1, 6.1.2, 6.1.3, 6.1.6, 6.2, 6.3, 6.4, 6.5, 6.6.6, 6.7 y 6.8 de estas NCV como terceros beneficiarios.

6.5. Reclamaciones y quejas

- Con independencia de lo dispuesto en la Cláusula 7 de estas NCV, los interesados podrán ejercitar sus derechos o presentar una reclamación en relación con el tratamiento de sus datos por las entidades NCV y su aplicación de las NCV, siguiendo el procedimiento establecido en la Cláusula 6.3.6.

- Las entidades NCV deberán cumplir lo dispuesto en la Cláusula 6.3.6 y en el Protocolo de tramitación de quejas y reclamaciones de las NCV, que se adjunta como Anexo 8.

6.6. Medidas para aplicar las NCV

6.6.1. Formación del personal

- Como parte del compromiso del Grupo PROSEGUR con la privacidad y el cumplimiento de la protección de datos, anualmente se imparten cursos de formación y sensibilización del personal.

- Las entidades NCV y los Oficiales de Cumplimiento /Delegados de Protección de Datos locales, con el apoyo del Delegado de Protección de Datos del Grupo, son responsables de definir el formato de los cursos de formación y sensibilización (que pueden ser presenciales u online), así como la frecuencia de los cursos de formación.

- En concreto, anualmente se celebran las sesiones de formación y sensibilización siguientes: (i) una sesión general sobre privacidad y protección de datos; y (ii) una sesión específica sobre las NCV.

  La sesión general sobre temas de privacidad cubre, entre otros, cómo la privacidad afecta a la actividad del Grupo PROSEGUR y su personal y las políticas y normas adoptadas dentro del Grupo PROSEGUR.

  La sesión específica sobre cuestiones relativas a las NCV abarca el contenido de estas NCV, incluidos los correspondientes anexos.

- Las sesiones de formación y sensibilización se desarrollan a través de la plataforma online de la Universidad Prosegur, a la que se accede desde la intranet del Grupo PROSEGUR. El contenido de las sesiones de formación y sensibilización es una combinación de teoría y práctica, que incluye un cuestionario de evaluación que debe superarse (por ejemplo, respuestas correctas 7 sobre 10) para considerar la formación como «cursada y completada». La Universidad Prosegur utiliza la plataforma online para gestionar las solicitudes del personal para asistir al curso, los recordatorios, los asistentes y los que han finalizado cada curso.

- El personal también tiene acceso a las políticas internas del Grupo PROSEGUR sobre protección de datos personales y seguridad de la información, así como al contenido de estas NCV. La información se incluye en los materiales entregados al personal en el momento de la incorporación, se publica en la intranet del Grupo PROSEGUR y de las entidades NCV y se promueve mediante notificaciones.

6.6.2. Control del cumplimiento de las NCV

- El Delegado de Protección de Datos del Grupo y el Comité Corporativo de Protección de Datos son responsables de supervisar la aplicación de estas NCV, con el apoyo de los responsables locales de protección de datos o cumplimiento y los órganos de dirección de las entidades NCV.

- El Delegado de Protección de Datos Local/Oficial de Cumplimiento Local designado tendrá, entre otras, las siguientes funciones:

  (i) Informar y asesorar a las entidades NCV y al personal encargado del tratamiento sobre sus obligaciones en virtud de las NCV y de la legislación europea de protección de datos. El Delegado de Protección de Datos Local/ Oficial de Cumplimiento Local depende directamente del nivel más alto de la jerarquía de las entidades NCV.

  (ii) supervisar el cumplimiento de las disposiciones de la NCV y de la Ley Europea de Protección de Datos, así como de las políticas de PROSEGUR, incluida la asignación de responsabilidades, la sensibilización y la formación del personal involucrado en las operaciones de tratamiento.

  (iii) actuar como punto de contacto con las autoridades de supervisión en cuestiones relacionadas con las operaciones de tratamiento de datos y la aplicación de las NCV, así como cooperar con las investigaciones practicadas por las citadas autoridades.

  (iv) revisar los informes de auditoría sobre protección de datos y supervisar la aplicación de las medidas correctoras propuestas en ellos.

  (v) atender las peticiones y reclamaciones de los interesados.

- El Delegado de Protección de Datos del Grupo es responsable de mantener actualizadas estas NCV y de comunicar las actualizaciones a las autoridades de supervisión pertinentes, así como de informar anualmente sobre el estado de aplicación de las NCV. Los Oficiales de Cumplimiento/Delegados de Protección de Datos locales informarán trimestralmente al Delegado de Protección de Datos del Grupo sobre las medidas de protección de datos adoptadas a nivel local.

6.6.3. Verificación del cumplimiento de las NCV

- El Grupo PROSEGUR cuenta también con un Programa de auditoría, descrito en el Anexo 9, para verificar el cumplimiento de estas NCV por parte de las entidades NCV. Este programa establece la frecuencia y los periodos de las revisiones y auditorías, su alcance, las acciones implicadas y los medios, entre otros aspectos.

- Los resultados de las revisiones y auditorías deben comunicarse al Delegado de Protección de Datos del Grupo, al Delegado de Protección de Datos Local/Oficial de Cumplimiento Local, al Comité Corporativo de Protección de Datos y al consejo de la entidad NCV afectada.

- Los resultados de las auditorías deben comunicarse también al consejo de PROSEGUR.

- En caso de incumplimiento de las NCV, los informes incluyen recomendaciones y medidas correctoras que debe aplicar la entidad NCV afectada, en un plazo determinado. Si las recomendaciones y medidas correctoras no se aplican debidamente, este hecho se comunica al consejo de PROSEGUR, para que tome las decisiones oportunas; incluyendo, entre otras, la exclusión de la entidad NCV del ámbito de aplicación de las NCV.

- Las autoridades de supervisión podrán exigir el acceso a los informes de auditoría y efectuar auditorías de protección de datos de cualquier entidad NCV.

- También se llevarán a cabo auditorías a petición expresa del Delegado de Protección de Datos del Grupo o del Delegado de Protección de Datos Local/Oficial de Cumplimiento Local y en caso de cambios o hechos que afecten significativamente a las NCV.

6.6.4. Actualizaciones de las NCV

- Las NCV se revisan y actualizan cuando se producen cambios en la legislación europea sobre protección de datos o en cualquiera de sus contenidos (incluidos sus anexos). El Delegado de Protección de Datos del Grupo es responsable de revisar periódicamente las NCV y de introducir los cambios necesarios para mantenerlas actualizadas, y para ello debe hacer lo siguiente:

  (i) Mantener un registro actualizado de las entidades NCV y de las actualizaciones de las NCV, así como mostrar dichos datos en las NCV;

  (ii) supervisar los cambios normativos, registrándolos y añadiéndolos a las NCV;

  (iii) facilitar la información necesaria a los interesados o a las autoridades de control, según proceda.

- Las modificaciones de las NCV (que incluyen, entre otras cosas, la lista de entidades NCV) se comunican a todas las entidades NCV sin demora injustificada.

- Los cambios en las NCV o en la lista de entidades NCV se comunican a las autoridades de supervisión, a través de la autoridad de supervisión principal, una vez al año, junto con una explicación de los motivos. Cuando las modificaciones de las NCV puedan afectar al nivel de protección ofrecido por las NCV o afectar significativamente a las NCV, dichas modificaciones deberán notificarse previamente a las autoridades de supervisión competentes, a través de la autoridad de supervisión principal, con una breve explicación de los motivos de la actualización. En este caso, las autoridades de supervisión también evaluarán si los cambios realizados requieren una nueva aprobación.

- No se efectuará ninguna transferencia a una nueva entidad NCV hasta que esta quede efectivamente vinculada por las NCV y pueda dar cumplimiento a lo dispuesto en ellas.

6.6.5. Incumplimiento de las NCV

- Las entidades NCV informarán sin demora a la exportadora de datos en caso de que no puedan cumplir las NCV, cualquiera que sea el motivo, incluidas las situaciones descritas en la Cláusula 6.8.2.

- En caso de que la importadora de datos (o cualquier otra entidad NCV que sea destinataria en una transferencia a terceros) incumpla las NCV o no pueda cumplirlas, la exportadora de datos suspenderá la TID.

- Las entidades NCV, a elección de la exportadora de datos, devolverán o borrarán inmediatamente los datos personales que hayan sido transferidos en virtud de las NCV en su totalidad cuando:

  (i) la entidad exportadora de datos ha suspendido la TID y no se restablece el cumplimiento de estas NCV en un plazo razonable y, en cualquier caso, en el plazo de un mes desde la suspensión; o bien,

  (ii) la entidad NCV incumple de forma sustancial o persistente las obligaciones de las NCV; o

  (iii) la entidad NCV incumple una decisión vinculante de un tribunal competente o de una autoridad de supervisión en relación con sus obligaciones en virtud de las NCV.

- Lo mismo se aplicará a las copias de los datos y a las transferencias a terceros. Las entidades NCV certificarán el borrado de los datos a la entidad exportadora de datos. Hasta que los datos sean borrados o devueltos, las entidades NCV seguirán garantizando el cumplimiento de las NCV. En caso de que la legislación local aplicable a las entidades NCV prohíba la devolución o el borrado de los datos personales transferidos, las entidades NCV garantizan que seguirán velando por el cumplimiento de las NCV y que solo tratarán los datos en la medida y durante el tiempo que exija dicha legislación local.

6.6.6. Información a los interesados

- Los interesados serán informados de las NCV por los siguientes medios:

  (i) publicación en los sitios web oficiales de PROSEGUR y de las entidades NCV;

  (ii) publicación en la intranet de PROSEGUR y de las entidades NCV;

  (iii) inserción de referencias a las NCV en las cláusulas informativas sobre protección de datos en relación con contratos, formularios, políticas, manuales y avisos.

  La información facilitada a los interesados figura en el Anexo 0. Versión pública de las NCV.

- Además, los interesados podrán solicitar por escrito una copia de las NCV en la siguiente dirección: oficina.privacidad@prosegur.com.

6.7. Responsabilidad

- PROSEGUR será responsable y se compromete a adoptar las medidas necesarias para remediar los actos de las entidades NCV situadas fuera del EEE y a indemnizar por los daños materiales o morales que resulten de la infracción de las NCV por dichas entidades NCV situadas fuera del EEE.

- PROSEGUR quedará exenta, total o parcialmente, de dicha responsabilidad cuando acredite que el hecho causante del daño no es, en modo alguno, responsabilidad de la entidad importadora de datos ni de otras entidades NCV en el caso de una transferencia a terceros. Corresponderá a PROSEGUR la carga de la prueba de que no se han infringido las NCV o de

que el hecho causante del daño no es, en modo alguno, responsabilidad de la entidad o entidades NCV de que se trate.

- En los casos en que la infracción de estas NCV haya sido cometida por una entidad NCV establecida en un tercer país, serán competentes los tribunales u otras autoridades de la Unión Europea, y el interesado dispondrá de los derechos y recursos apropiados contra PROSEGUR como si la infracción se hubiera producido en el Estado miembro donde PROSEGUR está establecida y no en el país de la entidad importadora de datos o entidad NCV fuera del EEE.

  En este caso, la acción contra PROSEGUR se ejercitará, a elección del interesado, ante los tribunales españoles o ante los tribunales del Estado miembro en el que el interesado tenga su residencia habitual.

6.8. Relación con la normativa y las autoridades

6.8.1. Comunicación y cooperación con las autoridades de supervisión

- Las entidades NCV se comprometen a cooperar con las autoridades de supervisión competentes en todos los asuntos relacionados con la aplicación de estas NCV y, en particular, a:

  (i) facilitar toda la información requerida por las autoridades de supervisión en relación con las NCV y el tratamiento regulado por ellas;

  (ii) permitir que sean auditadas por las autoridades de supervisión;

  (iii) aplicar las recomendaciones formuladas por las autoridades de supervisión;

  (iv) proporcionar los informes de verificación/auditorías de cumplimiento de las NCV requeridos por las autoridades de supervisión;

  (v) comunicar a la autoridad de supervisión las modificaciones de las NCV.

6.8.2. Relación con la legislación local

6.8.2.1 Compatibilidad con la legislación local

- Los datos personales deben ser tratados por las entidades NCV de conformidad con las leyes que les son aplicables. En ausencia de una ley local de protección de datos, o cuando dicha ley establezca un nivel de protección inferior al previsto en estas NCV, prevalecerán los derechos y obligaciones estipulados en las NCV. Cuando la legislación local exija un mayor nivel de protección de los datos personales, prevalecerá sobre la NCV.

- Las entidades NCV garantizan que no tienen motivos para creer que las leyes y prácticas de los terceros países de destino previstos aplicables al tratamiento de los datos personales por parte de las entidades importadoras de datos pertinentes, incluidos los requisitos de revelación de los datos personales o las medidas que autorizan el acceso por parte de las autoridades públicas, impidan a las entidades importadoras de datos cumplir sus obligaciones en virtud de estas NCV.

- Las NCV se basan en el entendimiento de que las leyes y prácticas que respetan la esencia de los derechos y libertades fundamentales y no exceden de lo necesario y proporcionado en una sociedad democrática para salvaguardar uno de los objetivos enumerados a continuación, no están en contradicción con estas NCV:

  a) seguridad nacional;

  b) defensa;

  c) orden público;

  d) la prevención, investigación, detección o persecución de infracciones penales o la ejecución de sanciones penales, incluida la protección y prevención de amenazas para el orden público;

  e) otros objetivos importantes de interés público general de la Unión Europea o de un Estado miembro, en particular un interés económico o financiero importante de la Unión Europea o de un Estado miembro, incluidos los asuntos monetarios, presupuestarios y fiscales, la salud pública y la seguridad social;

  f) la protección de la independencia judicial y de los procedimientos judiciales;

  g) la prevención, investigación, detección y persecución de las infracciones deontológicas de las profesiones reguladas;

  h) una función de control, inspección o reglamentación vinculada, incluso ocasionalmente, al ejercicio del poder público en los casos contemplados en las letras a) a e) y g);

  i) la protección del interesado o de los derechos y libertades de terceros;

  j) la ejecución de reclamaciones de derecho civil.

- Al evaluar las leyes y prácticas del tercer país que puedan afectar al respeto de los compromisos contenidos en las NCV, las entidades NCV deberán tener debidamente en cuenta, en particular, los siguientes elementos:

  (i) las circunstancias específicas de la TID o conjunto de TID, y de cualquier transferencia a terceros prevista dentro del mismo tercer país o a otro tercer país, incluyendo:

    - los fines para los que se transfieren y tratan los datos personales (por ejemplo, marketing, recursos humanos, almacenamiento, soporte informático, etc.);
    - tipos de entidades que intervienen en el tratamiento (la importadora de datos y cualquier otro destinatario de cualquier transferencia a terceros);
    - sector en el que se produce la TID o el conjunto de TID;
    - categorías y formato de los datos personales transferidos;
    - ubicación del tratamiento, incluido el almacenamiento;
    - canales de transmisión utilizados.

(ii) las leyes y prácticas del tercer país de destino que sean pertinentes a la luz de las circunstancias de la transferencia, incluidas las que exigen revelar los datos a las autoridades públicas o autorizan el acceso de dichas autoridades, incluidas las que prevén el acceso a estos datos durante el tránsito entre el país de la entidad exportadora de datos y el país de la entidad importadora de datos, así como las limitaciones y salvaguardias aplicables;

(iii) cualquier garantía contractual, técnica u organizativa pertinente establecida para complementar las garantías de las NCV, incluidas las medidas aplicadas durante la transmisión y el tratamiento de datos personales en el país de destino.

- Las entidades NCV se comprometen a que, cuando deban establecerse salvaguardias adicionales a las previstas en las NCV, PROSEGUR, el Delegado de Protección de Datos del Grupo y el Delegado de Protección de Datos/Oficial de Cumplimiento local pertinente serán informados y participarán en la evaluación.

- Las entidades NCV deberán documentar adecuadamente dicha evaluación, así como las medidas complementarias seleccionadas y aplicadas, y pondrán dicha documentación a disposición de la autoridad supervisora competente a petición de esta.

- Las entidades exportadoras de datos deberán supervisar de forma permanente, y en su caso en colaboración con las entidades importadoras de datos y los destinatarios, la evolución de la situación en los terceros países a los que las entidades exportadoras de datos hayan transferido datos personales que pudiera afectar a la evaluación inicial del nivel de protección y a las decisiones adoptadas en consecuencia sobre dichas transferencias.

6.8.2.2 Incompatibilidad con la legislación local

- Cualquier entidad NCV que actúe como importadora o destinataria de datos deberá notificar sin demora a la entidad exportadora de datos si, al utilizar estas NCV como instrumento para la TID, y mientras dure su adhesión a las NCV, tiene motivos para creer que está o ha pasado a estar sujeta a leyes o prácticas que le impedirían cumplir sus obligaciones en virtud de las NCV, incluso a raíz de un cambio en la legislación del tercer país o de una medida (como una solicitud de divulgación). Esta información también deberá facilitarse a PROSEGUR y al Delegado de Protección de Datos del Grupo.

- Una vez verificada dicha notificación, la entidad NCV que actúe como exportadora de los datos, junto con PROSEGUR, el Delegado de Protección de Datos del Grupo y el Delegado de Protección de Datos Local/Oficial de Cumplimiento correspondiente, se comprometen a identificar con prontitud las medidas apropiadas (por ejemplo, medidas técnicas u organizativas para garantizar la seguridad y confidencialidad) que deberá adoptar la entidad NCV que actúe como exportadora de los datos o la entidad NCV que actúe como importadora de los datos para que puedan cumplir con sus obligaciones en el marco de las NCV. Lo mismo es válido si una entidad NCV que actúa como exportadora de datos tiene motivos para creer que una entidad NCV que actúa como su importadora de datos o destinataria de una transferencia a terceros ya no puede cumplir sus obligaciones en virtud de estas NCV.

- Cuando la entidad NCV que actúe como exportadora de datos, junto con PROSEGUR, el Delegado de Protección de Datos del Grupo y el Delegado de Protección de Datos Local/Oficial de Cumplimiento pertinente, evalúe que no pueden adoptarse salvaguardias adecuadas para la TID o el conjunto de TID, o si así se lo ordena las autoridades de supervisión competentes, se compromete a suspender la TID o el conjunto de TID en cuestión, así como todas las transferencias de datos para las que la misma evaluación y el mismo razonamiento llevarían a una consecuencia similar.

- PROSEGUR, el Delegado de Protección de Datos del Grupo y el Delegado de Protección de Datos Local/Oficial de Cumplimiento correspondiente informarán a todas las demás entidades NCV de la evaluación efectuada y de sus resultados, de modo que se apliquen las medidas complementarias identificadas en caso de que otras entidades NCV efectúen el mismo tipo de transferencias o, en caso de que no pudieran aplicarse medidas complementarias eficaces, se suspenda o finalice la TID en cuestión.

- Tras dicha suspensión, la entidad NCV que actúa como exportadora de los datos puede optar por finalizar la TID o conjunto de TID. En este sentido, los datos personales que hayan sido transferidos con anterioridad a la suspensión, así como cualquier copia de ellos deberán, a elección de la entidad NCV que actúe como exportadora de datos, serle devueltos o destruidos en su totalidad.

- Cuando exista alguna incompatibilidad con las leyes locales que pueda tener como consecuencia efectos adversos sustanciales en la aplicación de las garantías proporcionadas por la NCV, PROSEGUR lo notificará a las autoridades de supervisión competentes, incluyendo cualquier solicitud o requerimiento legalmente vinculante para la divulgación de datos personales por parte de una autoridad u organismo de seguridad estatal del país en cuestión. Se informará claramente a las autoridades de supervisión competentes sobre la solicitud, en particular sobre los datos solicitados, el organismo solicitante y el fundamento jurídico de la divulgación, a menos que una prohibición legal impida que se realice dicha notificación.

- Si en casos concretos se prohíbe la suspensión o la notificación, las entidades NCV requeridas harán todo lo posible para obtener el derecho a renunciar a esta prohibición de divulgación a las autoridades de supervisión competentes con la mayor cantidad de información posible, lo antes posible, y poder demostrarlo. Cuando en estos casos, a pesar de los esfuerzos desplegados, las entidades NCV no puedan notificarlo a las autoridades de supervisión competentes, las entidades NCV se comprometen a proporcionar anualmente a las autoridades de supervisión competentes un informe general sobre las solicitudes recibidas, que incluya el número de solicitudes de divulgación, los tipos de datos solicitados y las autoridades u organismos solicitantes, siempre que sea posible.

- En cualquier caso, la revelación de datos personales por parte de una entidad NCV a las autoridades públicas no debe ser masiva, desproporcionada o indiscriminada, de modo que se limite a lo que sea necesario en una sociedad democrática para proteger intereses específicos importantes, como el orden público y la prevención, investigación, detección y enjuiciamiento de delitos o la ejecución de sanciones penales, con la protección contra amenazas al orden público y su prevención.

6.9. Vigencia

- Las NCV entrarán en vigor el día de su adopción y serán válidas por tiempo indefinido.

ANEXOS

7. Anexos

7.1. Anexo 1. Entidades NCV

El listado de entidades del Grupo PROSEGUR que se encuentran adheridas a estas NCV está disponible a través del siguiente enlace: Política de Privacidad: Normas Corporativas Vinculantes | Prosegur.com.

7.2. Anexo 2. Mapa de transferencia internacional de datos

En la **Cláusula 3.2.2.** de las NCV se incluye un resumen de la transferencia internacional de datos actualmente prevista o ejecutada.

Allí podrá encontrar información relevante sobre los países desde los que se exportan o se exportarán datos personales, los terceros países de destino actuales o previstos, los grupos de interesados afectados y los tipos de datos que se transferirán, así como las finalidades de su tratamiento.

7.3. Anexo 3. Política de seguridad de la información

La Política de seguridad de la información del Grupo PROSEGUR es interna y confidencial. En la **Cláusula 6.1.3** de las NCV puede encontrar la información relevante y pública relativa a las medidas de seguridad implantadas en el Grupo PROSEGUR.

7.4. Anexo 4. Modelo de gobernanza para el cumplimiento en materia de protección de datos

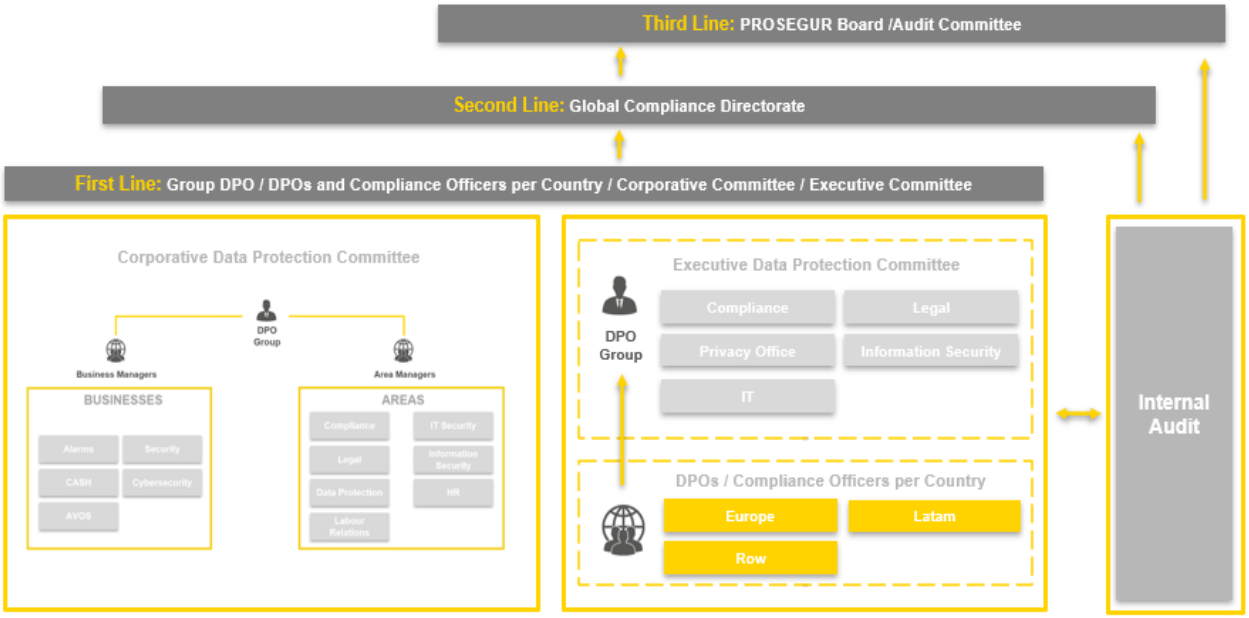
El Modelo de Gobernanza y Cumplimiento en materia de protección de datos es una política interna y confidencial por la que el Grupo PROSEGUR establece las bases de su sistema interno de protección de datos personales y sus políticas y procedimientos asociados. Esta política establece:

i. Los principios de protección de datos que deben ser respetados por todas las entidades que forman parte del Grupo PROSEGUR y su personal. Estos principios se indican en la **Cláusula 6.1.1.** de las NCV.

ii. Las funciones y responsabilidades de las principales áreas y de todo el personal del Grupo PROSEGUR para la protección de los datos personales, que incluyen las relativas a la aplicación de las NCV.

iii. Las funciones y responsabilidades de los delegados de protección de datos globales y locales y de los oficiales de cumplimiento locales se resumen en la **Cláusula 6.1.4** de las NCV.

iv. La composición de los órganos corporativos de protección de datos personales, sus funciones y responsabilidades, a quién informan y con qué frecuencia, así como su posición como líneas de defensa de la privacidad y la protección de datos. A continuación, le ofrecemos un resumen:



- **Comité corporativo de protección de datos**

  El Comité Corporativo de Protección de Datos, liderado y presidido por el Delegado de Protección de Datos del Grupo (DPO), se reunirá semestralmente y estará integrado por un miembro de las principales áreas y negocios de PROSEGUR, denominado Responsable funcional de tratamiento, que será el encargado del seguimiento de las acciones que se hayan definido para garantizar el cumplimiento en materia de protección de datos en su ámbito de competencia, y deberá informar a los DPO/Oficiales de Cumplimiento locales o del Grupo sobre el grado de cumplimiento de las acciones emprendidas. Este comité tiene las funciones siguientes:

  - Informar sobre las actuaciones llevadas a cabo por cada una de las áreas/departamentos y empresas en materia de protección de datos, así como cualquier asunto que estime oportuno en dicha materia.
  - Informar sobre posibles riesgos en el ámbito de la protección de datos.
  - Notificar cualquier fallo o incidente identificado en relación con los datos personales.
  - Informar sobre nuevas iniciativas que conlleven el tratamiento de datos personales.
  - Informar de los resultados de las evaluaciones objetivas de los riesgos, así como de las nuevas actividades de tratamiento identificadas en relación con su ámbito de competencia, (empresa/área/departamento), que incorporen las nuevas actividades de tratamiento implantadas.
  - Informar sobre el acceso a los datos del Grupo PROSEGUR por parte de terceros recientes.
  - Identificar las nuevas transferencias internacionales de datos realizadas.
  - Informar de las nuevas necesidades detectadas en el ámbito de la protección de datos.
  - Preparar materiales para cursos y sesiones de formación sobre el tratamiento de datos personales y definir el formato de los cursos de formación y su frecuencia.

- **Comité Ejecutivo de Protección de Datos**

  - El Comité Ejecutivo de Protección de Datos está representado por el DPO del Grupo y los responsables de las áreas de cumplimiento, jurídica, protección de datos, seguridad informática y seguridad de la información, y tiene como principal objetivo tratar los asuntos de mayor relevancia en el ámbito de la protección de datos, de acuerdo con los criterios de prioridad, gravedad y urgencia.

7.5. Anexo 5. Política de selección y evaluación de proveedores

La selección y evaluación de proveedores es una política interna y confidencial en la que Grupo PROSEGUR establece los requisitos para la contratación de un encargado de tratamiento de datos. Esta política establece, en resumen, que:

- Las entidades NCV solo podrán contratar encargados de tratamiento que ofrezcan garantías suficientes para implementar las medidas técnicas y organizativas apropiadas, con el fin de asegurar que la actividad de tratamiento de datos personales se desarrolla de conformidad con los requisitos establecidos por las NCV al respecto y garantizando la protección de los derechos de los interesados. Lo mismo sucede cuando una entidad NCV que actúa como encargada del tratamiento desea contratar a un subencargado del tratamiento, sea o no una entidad NCV.

- Estas salvaguardas están contenidas, entre otros elementos, en la experiencia, la fiabilidad y los recursos, con objeto de aplicar las medidas técnicas y organizativas correspondientes para cumplir los requisitos de las NCV, incluida la seguridad del tratamiento. A este respecto, la adhesión del encargado a un código de conducta aprobado o a un mecanismo de certificación aprobado puede utilizarse como medio para demostrar la existencia de garantías suficientes en cuanto al cumplimiento de sus obligaciones en materia de protección de datos.

- El proceso de selección de un proveedor que actúe como encargado del tratamiento de datos se iniciará con la presentación de un cuestionario de evaluación del proveedor, que deberá cumplimentarse antes de llevar a cabo la contratación. El cuestionario y las respuestas facilitadas deberán ir acompañados de las pruebas pertinentes. El cuestionario también incluye preguntas relacionadas con las medidas técnicas de seguridad, que el proveedor debe responder para evaluar el grado de cumplimiento y determinar así si las medidas de seguridad aplicadas son adecuadas para el nivel de riesgo que se ha identificado. Si los resultados del proceso de evaluación no son satisfactorios una vez finalizado el proceso de evaluación, el proveedor en cuestión no podrá ser contratado a menos que subsane las deficiencias detectadas en la evaluación y certifique la corrección presentando las pruebas pertinentes.

- Las entidades NCV también tienen derecho a auditar las instalaciones y sistemas del encargado del tratamiento y solicitar el acceso a determinada documentación que acredite el cumplimiento de las NCV, como sus registros de actividades de tratamiento, compromisos de confidencialidad firmados con sus empleados y colaboradores, certificados de haber recibido formación en materia de protección de datos, certificados de haber sido asesorado en la materia o de haber sido auditado, etc.

- La relación con el encargado del tratamiento se regirá por un contrato u otro acto jurídico con arreglo a las leyes europeas, que sea vinculante para el encargado frente al responsable. Los requisitos mínimos de este contrato se describen en la **Cláusula 6.1.5.** de las NCV.

7.6. Anexo 6. Protocolo de gestión y notificación de fallo de seguridad de los datos personales

El Protocolo de gestión y notificación de fallos de seguridad de los datos personales de PROSEGUR es interno y confidencial. En la **Cláusula 6.1.6** de las NCV puede encontrar la información relevante y pública relativa al procedimiento de fallo de seguridad de los datos personales en el Grupo PROSEGUR.

7.7. Anexo 7. Protocolo de gestión de la EIPD

El protocolo de Evaluación del impacto de la protección de datos (EIPD) de PROSEGUR es un protocolo interno y confidencial por el que el Grupo PROSEGUR establece los requisitos para la contratación de un encargado del tratamiento. Este protocolo establece, en resumen, que:

- La EIPD es un análisis detallado de una o varias operaciones similares de tratamiento de datos personales que tiene por objeto identificar y evaluar los riesgos asociados al tratamiento y especificar las medidas que deben adoptarse para prevenirlos o mitigarlos.

- Este proceso de evaluación debe llevarse a cabo antes de iniciar cualquier operación de tratamiento de datos personales, de forma que se determinen y apliquen desde el principio los medios necesarios para garantizar el cumplimiento de los principios, derechos y obligaciones establecidos por la legislación de protección de datos personales. No obstante, nada impide que se lleve a cabo una EIPD para un tratamiento que ya esté en pleno funcionamiento.

- Las entidades NCV deben llevar a cabo una EIPD cuando sea probable que la naturaleza, el alcance, el contexto o los fines de un tipo de tratamiento, en particular si utiliza nuevas tecnologías, entrañen un alto riesgo para los derechos y libertades de las personas físicas.

- La EIPD debe incluir como mínimo:

    - una descripción sistemática de las operaciones de tratamiento previstas y de los fines de este, incluido, en su caso, el interés legítimo perseguido por las entidades NCV;

    - una evaluación de la necesidad y proporcionalidad de las operaciones de tratamiento en relación con su finalidad;

    - una evaluación de los riesgos para los derechos y libertades de los interesados; y

    - las medidas previstas para hacer frente a los riesgos, incluidas las salvaguardias, las medidas de seguridad y los mecanismos para garantizar la protección de los datos personales y demostrar el cumplimiento de las leyes, teniendo en cuenta los derechos y los intereses legítimos de los interesados y de otros sujetos de datos afectados.

7.8. Anexo 8. Protocolo de tramitación de quejas y reclamaciones de las NCV

El protocolo de tramitación de quejas y reclamaciones de PROSEGUR NCV es un protocolo interno y confidencial. En la **Cláusula 6.3.6** de las NCV puede encontrar la información pertinente y pública al respecto.

7.9. Anexo 9. Programa de auditoría

El Programa de Auditoría es un protocolo interno y confidencial por el que el Grupo PROSEGUR define la frecuencia y periodicidad de las revisiones y auditorías, su alcance, acciones implicadas y medios, entre otros aspectos, con el fin de verificar el cumplimiento de las NCV por parte de las entidades NCV.

El programa de auditoría establece, en resumen, que:

- El cumplimiento por parte de las entidades NCV de las leyes locales de protección de datos y de las políticas y códigos internos del Grupo PROSEGUR es analizado constantemente por el Delegado de Protección de Datos del Grupo a través de los informes del sistema de protección de datos, que contiene toda la información relacionada con la protección de datos a escala local (es decir, registros de las actividades de tratamiento, sistemas asociados a este, quejas y solicitudes recibidas, etc.), así como el grado de cumplimiento de los controles de protección de datos del Grupo PROSEGUR. Asimismo, los DPO/Oficiales de Cumplimiento locales informarán trimestralmente al Delegado de Protección de Datos del Grupo y este al consejo de PROSEGUR, que es el máximo nivel de dirección del Grupo.

- Además de esos análisis generales de cumplimiento de la protección de datos, el Grupo PROSEGUR ha creado un programa de auditoría para verificar específicamente el cumplimiento de las NCV por parte de las entidades NCV, que consiste en:

    - **Revisiones anuales**: Cada año, todas las entidades NCV cumplimentarán un cuestionario sobre cómo están cumpliendo las NCV. Estos cuestionarios medirán el nivel de aplicación de las entidades NCV y su grado de eficacia. A partir de la información facilitada, auditoría interna elaborará un informe que remitirá al Delegado de Protección de Datos del Grupo y a los Delegados de Protección de Datos/Oficiales de Cumplimiento locales del país correspondiente, para que este lo presente a su vez al Comité Corporativo de Protección de Datos. Se propondrán recomendaciones y medidas correctivas para cualquier incumplimiento o deficiencia detectada.

    - **Auditorías trienales:** Trienalmente, auditoría interna llevará a cabo una auditoría en la que se analizarán las respuestas al cuestionario de la última revisión anual y su informe, y se recopilarán pruebas sobre el cumplimiento de los requisitos de las NCV. La auditoría interna elaborará un informe de auditoría que remitirá al Delegados de Protección de Datos del Grupo y a los Delegados de Protección de Datos/ Oficiales de Cumplimiento locales del país correspondiente, para que a su vez lo remitan al Comité Corporativo de Protección de Datos. Los informes de auditoría resultantes también se comunicarán al órgano administrativo y de gestión de la entidad NCV en cuestión y al consejo de PROSEGUR.

      En caso de incumplimiento de las NCV, los informes incluirán recomendaciones y medidas correctoras que debe aplicar la entidad NCV afectada, en un plazo determinado. Si las recomendaciones y medidas correctoras no se aplican debidamente, este hecho se comunica al consejo de PROSEGUR, para que tome las decisiones oportunas; incluyendo, entre otras, la exclusión de la entidad NCV del ámbito de aplicación de las NCV.

    - **Auditorías solicitadas:** Las autoridades de supervisión podrán exigir el acceso a los informes de auditoría y efectuar auditorías de protección de datos de cualquier entidad NCV. También se llevarán a cabo auditorías de protección de datos a petición específica del Delegado de Protección de Datos del Grupo o del Delegado de Protección de Datos/Oficial de Cumplimiento local, siempre que lo consideren necesario. También se requerirán auditorías en caso de (i) cambios en la estructura/políticas de la entidad NCV o en las leyes locales de protección de datos; o bien, (ii) cualquier hecho denunciado o detectado, que afecte significativamente a las NCV o que ponga en duda la capacidad de la entidad NCV para cumplir con las NCV.

PROSEGUR