Política de protección de datos

1. Introducción

El objetivo de esta Política es establecer las directrices que todos los niveles de CONTROL GROUP deberán seguir en materia de Protección de Datos de carácter Personal.

Esta Política contiene una descripción de los elementos clave, tanto humanos como organizativos, tecnológicos y documentales, que CONTROL GROUP aplica para proteger los datos de carácter personal, evitando que se produzcan vulneraciones de los derechos y libertades de los interesados.

En todos los niveles de CONTROL GROUP se velará por la aplicación real y efectiva de las directrices establecidas en esta Política en materia de protección de datos, de manera que este sistema de autorregulación consiga la eliminación de comportamientos que pudieran poner en riesgo los datos personales tratados por CONTROL GROUP.

2. Ámbito de aplicación

- Ámbito Societario. - Esta Política será aplicable al grupo de empresas CONTROL GROUP.

- Ámbito personal. - Esta Política será aplicable a todos los niveles de CONTROL GROUP, incluyendo los órganos de administración, los cargos directivos, los órganos de control y la totalidad del personal.

- Ámbito relacional. - El ámbito de aplicación de esta Política se extenderá, en la medida de lo posible, a los proveedores, asesores, clientes y otros terceros de CONTROL GROUP.

- Ámbito geográfico. - Esta Política se aplicará a las relaciones públicas y privadas que CONTROL GROUP establezca en cualquier ámbito geográfico.

3. Normativa aplicable

Esta Política está adaptada a la siguiente normativa:

- Reglamento General de Protección de Datos de la UE (RGPD)
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales
- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico
- Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen.
- Ley 29/2021, del 28 de octubre, cualificada de Protección de Datos Personales (LCPDP).
- Decreto 391/2022, del 28-9-2022 de aprobación del Reglamento de aplicación de la Ley 29/2021, del 28 de octubre, calificada de protección de datos personales.

Se harán las adaptaciones necesarias de esta Política en función de los cambios legislativos que se produzcan, así como a los criterios establecidos en:

- Las guías, informes y resoluciones de la Agencia Española de Protección de Datos

- Las guías, informes y resoluciones de las autoridades de control de los restantes Estados miembros de la Unión Europea
- El Grupo de Trabajo del Artículo 29
- Las sentencias del Tribunal de Justicia de la Unión Europea
- Las sentencias de la Audiencia Nacional, el Tribunal Supremo y el Tribunal Constitucional

4. Riesgos del negocio en materia de protección de Datos

CONTROL GROUP desarrolla su actividad principal en el sector de servicios; en concreto, sus actividades son las de prestar servicios de implementación tecnológica para entidades.

La especial naturaleza de los datos personales, la complejidad de la normativa aplicable y la cuantía de las sanciones establecidas en ella generan riesgos como el acceso no autorizado, la copia no autorizada, la comunicación o la cesión a terceros y otras infracciones previstas en el RGPD y la normativa local.

Los riesgos derivados del incumplimiento de las obligaciones legales establecidas en materia de protección de datos son los siguientes:

1) Sanciones administrativas
2) Delitos contra la intimidad
3) Indemnizaciones de daños y perjuicios
4) Daños reputacionales

La protección de los datos personales es uno de los valores de CONTROL GROUP y es un objetivo prioritario del grupo que exige una serie de medidas jurídicas, técnicas y organizativas, que se resumen en esta Política y se detallan en sus normas y procedimientos propios.

5. Objetivos de la protección de Datos

Los objetivos de CONTROL GROUP en materia de protección de datos están alineados con los de negocio, dando prioridad al cumplimiento de las obligaciones legales que sean aplicables a la actividad desarrollada.

La protección de dados se considera una ventaja competitiva, ya que permite diferenciar a CONTROL GROUP de sus competidores que no respeten la privacidad de su clientes y colaboradores o que traten inadecuadamente sus datos, asumiendo el riesgo de importantes sanciones económicas con gran impacto reputacional.

Se considerará un objetivo prioritario de la protección de datos el cumplimiento del Reglamento General de Protección de Datos de la Unión Europea y la Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales.

En todos los niveles de CONTROL GROUP existirá el compromiso de cumplir los objetivos fijados en materia de protección de datos y los principios y obligaciones establecidos en esta Política.

CONTROL GROUP podrá elaborar normas y procedimientos que desarrollen, concreten y detallen de la presente política.

6. Principios de la Protección de Datos

La estrategia de CONTROL GROUP en materia de protección de datos cumplirá los principios que se describen a continuación:

- Principio de licitud: el tratamiento de datos personales será lícito si se basa en el consentimiento del interesado o en alguna otra base de legitimación establecida en la Ley.

- Principio de transparencia: el interesado deberá ser informado de todas las circunstancias relativas al tratamiento.

- Principio de lealtad: los datos personales no podrán ser tratados en circunstancias distintas de las informadas.

- Principio de limitación de la finalidad: los datos personales serán recogidos con fines determinados, explícitos y legítimos, y no serán tratados posteriormente de manera incompatible con dichos fines.

- Principio de minimización de datos: los datos personales deberán ser adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados. Este principio y el anterior se desarrollan en los principios de necesidad y proporcionalidad que se aplican a las evaluaciones de impacto.

- Principio de exactitud: los datos personales deberán ser exactos y, si fuera necesario, actualizados, adoptándose todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan.

- Principio de limitación del plazo de conservación: los datos personales deberán ser mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales.

- Principio de integridad y confidencialidad: los datos personales deberán ser tratados de tal manera que se garantice una seguridad adecuada, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas. Los datos personales sólo serán accesibles para los usuarios autorizados a acceder a ellos y no podrán ser comunicados a terceros sin la correspondiente autorización.

- Principio de responsabilidad proactiva: CONTROL GROUP será responsable del cumplimiento de lo dispuesto en la normativa de protección de datos, y deberá ser capaz de demostrar dicho cumplimiento.

- Protección de datos desde el diseño y por defecto: en los nuevos tratamientos, proyectos, servicios y productos se hará una evaluación previa de su impacto en materia de protección de datos.

7. Roles y responsabilidades

Todos los roles y responsabilidades estarán diferenciados y, en la medida de lo posible, serán asignados de manera individualizada en la descripción del puesto de trabajo. Además de esta asignación individualizada, todas las personas que pertenezcan a CONTROL GROUP, fuera cual fuera su nivel, estarán obligadas a cumplir las normas, procedimientos y controles establecidos en materia de seguridad de la información.

La máxima responsabilidad del control en materia de protección de datos corresponderá al Delegado de Protección de Datos.

CONTROL GROUP dispone de normas y procedimientos donde se establecen las obligaciones del personal en materia de protección de datos.

CONTROL GROUP adoptará las medidas necesarias para que el personal conozca de manera comprensible las obligaciones en materia de protección de datos que afecten al desarrollo de sus funciones, así como las consecuencias de su incumplimiento.

8. Registro de Actividades del Tratamiento

CONTROL GROUP dispondrá de un registro de tratamientos en el constarán los detalles de los tratamientos autorizados como Responsable del Tratamiento; así como otro registro de los tratamientos realizados como Encargado del Tratamiento.

De acuerdo con el principio de privacidad desde el diseño y por defecto, y dada la imposibilidad de que los órganos de control conozcan todas y cada una de las actividades relacionadas con datos personales que se llevan a cabo en cada departamento, cada nuevo tratamiento o cada tratamiento que modifique los atributos y características asignados al mismo en el registro de tratamientos, deberá ser comunicado al Comité de Protección de Datos con el fin de que lo evalúe y lo autorice en el caso de que no suponga un riesgo para los derechos y libertades de los interesados.

Asimismo, CONTROL GROUP informará del tratamiento de los datos personales a todos los interesados a través de las cláusulas informativas y de consentimiento de conformidad con el art. 13 y 14 RGPD.

9. Análisis de riesgos

Todos los tratamientos sujetos a esta Política de Seguridad deberán pasar por un análisis de riesgos, evaluando las amenazas y los riesgos a los que están expuestos. Este análisis se repetirá periódicamente.

CONTROL GROUP hará periódicamente un análisis de los riesgos y amenazas que afecten a la protección de datos.

El análisis de riesgos se hará a través de un mapa de riesgos inherentes, en el que se evalúen los riesgos brutos existentes antes de la aplicación de los controles de prevención, detección y mitigación, tras lo cual se hará un mapa de riesgos residuales, en el que se evalúen de forma automatizada los riesgos netos existentes después de la aplicación de los controles.

En esta línea, se informa que la matriz dispone del certificado de la ISO 27001, garantizando así la aplicación de las medidas de seguridad técnicas y organizativas para garantizar un nivel adecuado de seguridad, teniendo en cuenta la naturaleza, alcance, contexto y finalidad del tratamiento, así como los riesgos para los derechos y libertades de las personas físicas, así como

garantizar la confidencialidad, integridad, disponibilidad y resiliencia continuas de los sistemas y servicios de procesamiento.

10. Obligaciones contractuales

Además de las exigencias legales en materia de protección de datos, CONTROL GROUP estará obligada también a cumplir los requisitos específicos de protección de datos que le exijan sus clientes y proveedores en relación a los datos de carácter personal a lo que accedan en virtud de sus relaciones contractuales con ellos.

CONTROL GROUP prestará especial atención a las obligaciones contractuales de las que se deriven tratamiento de datos personales.

CONTROL GROUP hará y mantendrá actualizado un registro en el que identificará y priorizará las obligaciones relacionadas con la protección de los datos personales a los que acceda o trate.

CONTROL GROUP comprobará periódicamente que las obligaciones contractuales asumidas en materia de protección de datos sean conocidas en todos los niveles de CONTROL GROUP.

11. Control de Proveedores desde el punto de vista de privacidad

CONTROL GROUP elaborará un registro de todos los proveedores que traten datos personales por cuenta de CONTROL GROUP o que tengan acceso directo o indirecto a datos personales gestionados por CONTROL GROUP

En el caso de que fuera necesario contratar un nuevo servicio que exigiera tratamiento de datos, CONTROL GROUP efectuará una selección de proveedores y un proceso de evaluación teniendo en cuenta las garantías exigidas en la Ley en materia de protección de datos.

En esta evaluación se dará prioridad a los proveedores que ofrezcan mayores garantías en materia de protección de datos.

La relación con los proveedores que traten o que tengan acceso directo o indirecto a datos personales estará regulada siempre en un contrato que incluirá una sección específica sobre las obligaciones que deberá cumplir el proveedor. Estas obligaciones incluirán, como mínimo, las establecidas en el artículo 28 del RGPD.

12. Plazos de conservación de Datos

CONTROL GROUP conservará los datos personales de tal forma que se permita la identificación de los interesados solamente durante el tiempo necesario para los fines del tratamiento de dichos datos. Por ello, CONTROL GROUP elaborará y mantendrá actualizada una tabla en la que establecerá el plazo de conservación de los datos que deba o que considere conveniente conservar.

En la elaboración de esta tabla se tendrán en cuenta los plazos de prescripción de las infracciones y las limitaciones que establece el RGPD y Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales. También se tendrá en cuenta las obligaciones legales,

sectoriales y contractuales que puedan exigir plazos superiores de conservación.

CONTROL GROUP deberá tener en cuenta también los plazos indicados a los interesados en el momento de informarles de sus derechos.

En relación a la destrucción de la documentación, se deberá realizar de forma que se garantice la confidencialidad durante todo su proceso.

13. Gestión de las brechas e incidentes de seguridad

Cualquier situación que pueda comprometer la confidencialidad, integridad, disponibilidad, autenticidad o trazabilidad de la información de CONTROL GROUP se considerará una brecha de seguridad.

Por ello, CONTROL GROUP deberá establecer las medidas oportunas en materia de ciberseguridad, que incluirán la protección frente a amenazas que provengan de las redes de comunicaciones, tales como los ciberataques, los ataques de denegación de servicios, los accesos no autorizados y el secuestro de sistemas o ransomware, entre otros.

Cualquier persona que tuviera conocimiento o sospecha de algún incidente que pudiera afectar a la protección de los datos deberá comunicarlo inmediatamente a través de los canales establecidos para ello.

En el supuesto que la brecha o el incidente de seguridad pudieran suponer un riesgo para los derechos y libertades para las personas físicas, se deberá notificar, a más tardar 72 horas después de que hubiera constancia de ella, a la Autoridad de Control competente, esto es, la Agencia Española de Protección de Datos.

CONTROL GROUP dispone de un protocolo en el cual se define la sistemática seguida por la entidad para la notificación y la gestión de incidentes y vulnerabilidades de seguridad con el propósito de asegurar que los incidentes de seguridad y las debilidades asociadas con los sistemas de información se registren y se traten convenientemente, mediante las oportunas actividades de reparación y resolución, y de la restauración de los niveles normales de funcionamiento de los servicios afectados, pudiendo adoptar acciones correctoras para eliminar sus causas y prevenirlos en un futuro.

14. Formación y concienciación

Todo el personal de CONTROL GROUP tiene la obligación de conocer y cumplir la Política de Protección de Datos. Por ello, CONTROL GROUP promoverá una actividad constante de formación y concienciación en todos los niveles de CONTROL GROUP en materia de protección de datos.

La formación podrá basarse en sesiones presenciales o en cursos de e-Learning.

La concienciación podrá basarse en cualquier tipo de materiales e instrumentos de comunicación y formación que permitan concienciar sobre los riesgos de infracción a todos los niveles de CONTROL GROUP.

Cada trabajador será responsable de cumplir con esta política y los protocolos que se deriven según su puesto de trabajo, así como de notificar las incidencias de seguridad que se detecten.

15. Prevención de Infracciones

El principal objetivo de CONTROL GROUP con esta Política y sus normas, procedimientos y controles que la desarrollan, es prevenir infracciones de los derechos y libertades de los interesados y cumplir con la normativa de protección de datos de carácter personal.

El principal marco de referencia que se tendrá en cuenta para cumplir este objetivo será el RGPD, que establece dos grupos de infracciones: las graves y las muy graves.

A las infracciones graves se podrán aplicar sanciones de hasta 10 millones de Euros o el 2% de la cifra de negocio anual global de CONTROL GROUP. En este grupo se incluirían, por ejemplo, medidas técnicas u organizativas inadecuadas, contratación de encargados de tratamiento sin garantías suficientes, falta de notificación de una violación de datos, etc. A las infracciones muy graves se podrán aplicar sanciones de hasta 20 millones de Euros o el 4% de la cifra de negocio anual global de CONTROL GROUP. En esta categoría se incluirían los casos de tratamiento ilícito, consentimiento ilícito, vulneración del deber de confidencialidad, etc.

16. Actualización y mejora de esta Política

Esta Política será actualizada periódicamente con el fin de reflejar los cambios y mejoras en materia de protección de datos. CONTROL GROUP realizará una verificación periódica de la aplicación de las medidas de prevención y control, y propondrá las oportunas modificaciones que se requieran en caso de detectar infracciones relevantes de esta política, cambios significativos, o cambios en los sistemas de información de la entidad.