Doc. Ref.	POL-07	Version	2.0
Propietario	DATA PRIVACY OFFICE	Fecha efectiva	Diciembre 2025

Política de Gestión de la Privacidad y la Protección de Datos

MASORANGE

Elaborado por:	Revisado por:	Aprobado por:
Oficina de Privacidad	Comisión de Auditoría y Riesgos	Consejo de Administración

Lista de Distribución
Documento público

Control de versiones

Versión	Fecha de aprobación	Cambio respecto a la última versión
1.0	27/06/2024	*Versión inicial*
2.0	17/12/2025	*Ampliación de datos especialmente sensibles a medios de pago* *Indicación de la vinculación de esta Política con el Sistema de Gestión de la Privacidad alineado con ISO 27701*

Referencias a otros documentos

Doc. Ref.	Documento
L&A.C.02	Código Ético Grupo MASORANGE
POL-06	Política de Control y Gestión de Riesgos
PSG-01	Política de Seguridad Global
POL-10	Política de Seguridad de la Información
POL-15	Política de Uso de la IA

Contenido

1 Introducción y contexto

El Grupo MASORANGE está formado por una serie de sociedades dependientes y asociadas, cuya actividad principal es la prestación de servicios de comunicaciones electrónicas, así como otros servicios tales como energía, asistenciales, mediación de seguros, televisión o alarmas, entre otros, todos ellos destinados tanto a clientes mayoristas como minoristas.

En el ámbito de las telecomunicaciones ofrece servicios de telefonía fija, móvil, e Internet de banda ancha y televisión a clientes residenciales, empresas y operadores, a través de sus marcas principales: Orange, Yoigo, Jazztel, MÁSMÓVIL, Pepephone, Simyo, Lebara y Lycamobile, a través de las marcas regionales Euskaltel, R, Telecable y Guuk.

Establecer, operar, comercializar, prestar y gestionar los servicios que presta el Grupo conlleva la necesidad de tratar gran cantidad de datos personales de muy diferentes interesados: clientes, usuarios, empleados, colaboradores, proveedores, etc. Incluyendo datos especialmente sensibles por el impacto que un uso inapropiado podría tener en los Derechos y Libertades de las personas.

Tanto la Constitución Española como el Derecho Europeo reconocen el derecho fundamental a la protección de datos, entendido como la capacidad que debe tener el ciudadano para disponer y decidir sobre los datos que se refieran a él.

Este derecho se ha regulado jurídicamente, especialmente a través del Reglamento (UE) 2016/679 del Parlamento Europeo y de 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 (RGPD) y de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDyGDD). Aunque también ha de tenerse en cuenta en el ámbito de actuación del Grupo, lo recogido en la Ley 11/2022, de 28 de junio, General de Telecomunicaciones (LGTEL), en la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico, y en la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.

2 Objeto y alcance

El objeto de la presente Política es la de establecer los principios y pautas que se deberán desarrollar en el Grupo para definir e implementar un Sistema de Gestión de la Privacidad alineado con la norma ISO 27701 y la normativa aplicable de protección de datos, que busque asegurar que todo tratamiento de datos personales realizado en el Grupo cumple con la legislación vigente y la normativa interna.

Por su carácter de Política General, va dirigida, en primer lugar, a todas las sociedades que integran el Grupo, así como a las sociedades participadas no integradas en el Grupo sobre las que la este tiene un control efectivo, dentro de los límites legalmente establecidos.

Esta Política, y toda la normativa interna que la desarrolla, obliga a todas las áreas, departamentos y equipos de trabajo dentro de citadas sociedades, tanto en sus relaciones internas como con terceros, así como a toda actividad, producto, servicio o sistema de información con el que se traten en alguna forma datos personales, bien sea en calidad de Responsable o de Encargado del Tratamiento[1].

[1] Todos estos conceptos están definidos en el apartado siguiente para mejor entendimiento

Es necesario destacar que obliga a todos los profesionales, pertenecientes al Grupo o a terceras empresas que colaboren con el mismo, inclusive si en sus tareas actuales no existe un acceso y/o tratamiento de datos personales directo, en cuanto a la transversalidad precisa de ciertas obligaciones a lo largo de toda la organización, como puede ser la confidencialidad, gestión de brechas, etc.

La presente Política y las Políticas, Procedimientos, Procesos y Normas que la desarrollan directamente, así como aquellas más vinculadas a la Seguridad de la Información, sin las que no sería posible desarrollar un proceso de Protección de Datos adecuado, serán comunicados a todos los profesionales del Grupo, y estarán a disposición de todas las partes interesadas.

3 Definiciones

3.1 ¿Qué es un dato personal?

El RGPD define dato personal como toda información sobre una persona física identificada o identificable, considerando como tal toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona.

Datos como nombre y apellidos, número de DNI, dirección postal, correo electrónico, número de teléfono, la voz o la imagen son claramente datos personales. Pero otros muchos datos como una dirección IP, un número de IMEI, una dirección MAC e incluso identificadores únicos o cualquier otro dato o conjunto de datos que permitan al Grupo identificar a una persona física, ya sea directa o indirectamente, o a través de la combinación de información propia, pública o de terceros a la que tenga acceso tiene la consideración de dato personal[2].

Si bien el RGPD no aplica a datos de personas jurídicas, sí incluye en su ámbito los datos de personas físicas que representan a personas jurídicas o de personas físicas que actúan en calidad de empresario individual. Es decir, los datos de contacto empresarial están incluidos dentro del concepto de dato personal.

3.2 Datos especialmente sensibles

Existen datos personales que, por su naturaleza, son particularmente sensibles, ya que su tratamiento podría entrañar importantes riesgos para los derechos y las libertades fundamentales de las personas. Esta tipología de datos requiere especiales medidas de seguridad y control por parte del Grupo. Definiéndose en el alcance de esta Política como datos especialmente sensibles:

- Datos de categorías especiales según lo recogido en el artículo 9 del RGPD: datos que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o la orientación sexual de una persona física.

  Estos datos no pueden ser tratados salvo que concurra alguna de las circunstancias que figuran en el punto 2 del citado artículo 9. De entre las cuales solo dos supuestos pueden tener aplicación

[2] Ver Apéndice I. Ejemplos de Tipos de datos personales

práctica en una empresa: Consentimiento explícito del interesado[3], o que sea necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos de la empresa o del interesado en el ámbito laboral y de la seguridad y protección social[4].

- Datos relativos a condenas e infracciones penales, según el artículo 10 del RGPD.
- Datos de tráfico de telecomunicaciones, metadatos e información relativa al emisor y receptor de toda comunicación electrónica, así como los datos de localización asociados, que en todo caso deberán tratarse conforme lo recogido en la Ley General de Telecomunicaciones.
- Datos de medios de pago, entendidos como aquellos que permitan directamente realizar algún tipo de cargo o puedan suponer riesgos de pérdidas financieras directas para los interesados, como datos de tarjetas de crédito o mandatos SEPA válidos.

3.3 Conceptos importantes

Los siguientes conceptos aparecen en varias ocasiones a lo largo del documento por lo que es importante que se tenga claro su significado:

- **Interesado**: la persona titular de los datos personales.
- **Responsable del tratamiento**: la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento.
- **Encargado de tratamiento**: la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento.
- **Tercero**: Persona física o jurídica, autoridad pública, servicio u organismo distinto del interesado, del responsable del tratamiento, del encargado del tratamiento y de las personas autorizadas para tratar los datos personales bajo la autoridad directa del responsable o del encargado. Por ejemplo, es un tercero la entidad a la que se comunican datos personales del interesado para que sean tratados por esta con sus propios fines, en su caso.
- **Tratamiento u Operación de Tratamiento:** operación o conjunto de operaciones que se realiza con los datos personales, ya sea por medios automáticos o no, como: recopilación, registro, estructuración, almacenamiento, acceso, consulta, uso, transmisión, bloqueo, o borrado. También incluye la transferencia o divulgación de datos personales a terceros.
- **Actividad de tratamiento**: materialización de una finalidad sobre los datos personales de un determinado colectivo de personas. Así, una actividad de tratamiento puede ser la gestión de personal o la prestación de servicios. Cada Actividad de Tratamiento podrá incluir varias operaciones de Tratamiento.
- **Registro de Actividades de Tratamiento**: registro de las actividades de tratamiento de datos personales que lleva a cabo un responsable de tratamiento o un encargado en nombre de un responsable de tratamiento.
- **Conceptos de cesión y acceso a los datos personales**: La cesión de datos implica transferir los datos a un sujeto externo para que los utilice para sus propias finalidades, como por ejemplo los datos de empleados que se comunican a la Seguridad Social o a Hacienda. El acceso se refiere

[3] Salvo que una norma prohíba que el interesado pueda levantar la prohibición general del tratamiento.
4 En la medida en que así lo autorice el Derecho de la Unión, de los Estados miembros o un convenio colectivo.

a transferir los datos a un sujeto externo, para que este nos preste un servicio, bajo las instrucciones y con las finalidades que se le marquen, como por ejemplo comunicar datos de empleados a la empresa que gestiona las nóminas.

- **Evaluación de impacto relativa a la protección de datos:** análisis exhaustivo y documentado realizado por un responsable o un encargado del tratamiento de los riesgos para la privacidad, obligatorio cuando es probable que el tratamiento suponga un alto riesgo para los derechos y libertades del interesado.
- **Transferencia Internacional de datos**: tratamiento de datos llevado a cabo fuera de los territorios incluidos en el Espacio Económico Europeo[5].
- **Sistema de Gestión de la Privacidad (SGPI):** conjunto de elementos y actividades iterrelacionados y coordinados que, estableciendo políticas y objetivos, dirigen y controlan el cumplimiento legal, normativo y de criterios internos en relación a la privacidad y protección de datos personales en el Grupo.

4 Principios básicos relativos al tratamiento de datos personales

Según la legislación el tratamiento de datos personales debe regirse, a lo largo de todo su ciclo de vida, por una serie de principios, cuyo incumplimiento lleva aparejadas las sanciones más altas contempladas en la normativa[6]. Estos principios no deben verse como meras declaraciones teóricas, sino que han de tener una aplicación transversal en toda actividad del Grupo que implique datos personales.

A continuación, se explica el contenido de cada principio, sus implicaciones prácticas, así como de las herramientas que se ha dotado el grupo para asegurar el cumplimiento de los mismos:

4.1 Principio de licitud, lealtad y transparencia

Los datos personales deberán ser tratados de manera lícita, leal y transparente en relación con el interesado.

El artículo 6.1 del RGPD establece que una Actividad del Tratamiento solo será lícita si se cumple alguna de las siguientes condiciones: el interesado ha dado su consentimiento; es necesario para la ejecución de un contrato del que el interesado es parte o medidas precontractuales asociadas; es necesario para el cumplimiento de una obligación legal; es necesario para proteger intereses vitales del interesado u otra persona física; se necesario para el cumplimiento de una misión realizada en interés público; o es necesario para la satisfacción de intereses legítimos del Responsable o un tercero.

Con el fin de cumplir con el principio de licitud, a través de esta Política, se establece la prohibición para todas las Sociedades del Grupo de tratar datos personales que no se hayan obtenido de fuentes legítimas o de fuentes que no cuenten con suficientes garantías sobre su origen legítimo.

Así mismo, se definirá y mantendrá un procedimiento de actualización del Registro de Actividades del Tratamiento, que obligará a documentar en este la base de legitimación de cada una de las Operaciones del Tratamiento realizadas, justificar jurídicamente su validez y, en los casos que se

[5] Compuesto por los Estados miembros de la UE, Islandia, Liechtenstein y Noruega.
[6] Sanciones que pueden llegar hasta los 20M€ o el 4% del volumen anual de negocio del Grupo

considere necesario7, realizar una evaluación detallada sobre esta validez.

En cuanto al principio de transparencia, los artículos 13 y 14 del RGPD recogen el contenido mínimo a facilitar a los interesados antes del inicio del tratamiento de sus datos, según hayan facilitado ellos mismos los datos o provengan de terceros, con la obligación de informar en este segundo caso antes de 30 días tras la recepción de los datos personales del interesado.

Esta información debe facilitarse de forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo. Lo que quiere decir, además, que ha de evitarse la fatiga informativa al interesado; pudiendo optarse, con este fin, por un sistema de información por capas, como el recogido en el artículo 11 de la LOPDyGDD.

El principio de transparencia debe entenderse desde la perspectiva de los interesados, comprometiéndose el Grupo en la realización de todos los esfuerzos que sean necesarios para que estos conozcan qué se está haciendo con sus datos, adaptándose a las circunstancias del propio interesado, el contexto de recogida de los datos y al tratamiento o tratamientos concretos.

Para asegurar el cumplimiento del principio de Transparencia, toda Sociedad del Grupo que trate datos personales en calidad de Responsable del Tratamiento implementará un sistema de información para los interesados atendiendo a los siguientes requisitos:

Se informará a través de una Política de Privacidad específica para cada tipología de interesados/contexto del tratamiento. Por ejemplo, y sin ser exhaustivos: empleados, proveedores, clientes, usuarios de web y App.

Se tratará de un modelo por capas, que en la primera capa de información contendrá como mínimo los datos del responsable, la finalidad o finalidades del tratamiento, los derechos que podrá ejercer el interesado, así como una vía para su ejercicio gratuita y sencilla, y la forma directa de acceder a la segunda capa.

La segunda capa de información, recogida en cada Política de Privacidad, se pondrá a disposición de los interesados a través de medios electrónicos, preferiblemente página web, y se informará de la posibilidad de obtener una copia en soporte duradero, como papel.

4.2 Principio de limitación de la finalidad

El RGPD establece que los datos personales deben ser recogidos para finalidades específicas y legítimas y que su uso con fines posteriores diferentes solo se permitirá si es compatible con el fin inicial. Este principio concurre con el de transparencia, ya que se debe ofrecer a los interesados en el momento en que se recogen los datos información sobre la finalidad para la que se pretende utilizarlos.

A nivel práctico este principio supone que el Responsable debe tener documentadas todas las finalidades para las que utilizará datos personales y que debe implantar medidas para asegurar que estos no se utilizarán para finalidades no compatibles con las explicitadas al interesado en el momento de informarle sobre las cuestiones de protección de datos.

Con este objetivo, el Grupo definirá dentro de un procedimiento de actualización del Registro de Actividades del Tratamiento la obligación de mantener documentada toda finalidad, principal o ulterior, para el tratamiento de datos dentro del Registro de Actividades del Tratamiento, así como

[7] El Interés Legítimo requerirá una LIA (o según sus siglas en ingles “Legitimated Interest Assesment”)

de los requisitos de transparencia y claridad que deberá tener la definición de estas finalidades.

4.3 Principio de minimización de datos

Los datos personales deben ser adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados, es decir, solo se recogerán aquellos datos personales que sean necesarios para cumplir con la finalidad para la que se recogen. Este principio exige que el Grupo emprenda una labor de reflexión sobre los datos personales que trata para desarrollar las actividades de tratamiento, y sea responsable y coherente a la hora de pedir información.

Su cumplimiento se canalizará a través del un procedimiento de verificación del cumplimiento de protección de datos del Grupo, que establece la obligación de realizar el análisis de necesidad de cada categoría de datos que se pretenda utilizar en un tratamiento y dejar documentado este análisis, asociado al Registro de Actividades del Tratamiento. De forma que cualquier dato cuya necesidad no se pueda acreditar, será eliminado de la Actividad del Tratamiento.

4.4 Principio de Exactitud

Los datos personales deben ser exactos y, por tanto, deberán ser puestos al día cuando resulte preciso. Si bien ha de tenerse en cuenta que el Responsable del Tratamiento no será responsable de la inexactitud de datos facilitados directamente del interesado, ni de los suministrados por un mediador o intermediario en los casos en los que su participación sea legalmente posible, ni los provenientes de otro Responsable en virtud del ejercicio del derecho a la portabilidad.

Para asegurar el cumplimiento de este principio, por una parte, se incluirá en la información facilitada al interesado su obligación de facilitar datos exactos, y que cualquier inexactitud o modificación en los datos deberá ser comunicada al Responsable inmediatamente a través de las vías de contacto puestas a su disposición.

Por otra parte, se pondrán en marcha medidas que permitan la actualización periódica de datos personales, definidas en función de las circunstancias concretas de cada categoría de interesado y/o tratamiento. Estas medidas podrán implicar contactar con el interesado a través de medios eficaces, como el correo electrónico o notificaciones en su espacio privado en el caso de clientes, de forma periódica, pero sin resultar molestos por periodicidad.

4.5 Principio de limitación del plazo de conservación

Los datos personales no serán tratados más allá del plazo de tiempo necesario para alcanzar la finalidad por la cual se recabaron, salvo en los supuestos previstos legalmente. Además, el artículo 32 de la LOPDyGDD recoge la obligación de bloquear los datos cuando proceda su rectificación o supresión, consistiendo el boqueo en la adopción de las medidas técnicas y organizativas necesarias para impedir su tratamiento, incluyendo su visualización, excepto para la puesta a disposición de los jueces y tribunales, Ministerio Fiscal o las Administraciones públicas competentes, durante los plazos de prescripción de las obligaciones legales asociadas.

Los periodos de conservación, incluyendo los de bloqueo y destrucción, van a depender del tipo de datos personales y de la finalidad para la que se lleva a cabo el tratamiento. Los criterios generales en cuanto a definición de plazos y metodología para cumplir con esta obligación se definirá en un procedimiento relativo a los plazos de conservación, bloqueo y supresión de datos conforme al artículo 32 de la LOPDGDD. Mientras que los plazos concretos que aplican a cada Actividad del Tratamiento se documentarán y mantendrán actualizados en el Registro de Actividades del Tratamiento, siguiendo el procedimiento correspondiente.

4.6 Principio de integridad y confidencialidad

El Responsable del Tratamiento tiene que asegurar que los datos personales son 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. Este principio se ve complementado con la obligación recogida en el artículo 32 del RGPD, sobre las medidas de seguridad que el Responsable o el Encargado deben implantar para garantizar un nivel de seguridad adecuado al riesgo para los derechos y libertades de las personas físicas.

De acuerdo con este enfoque, será necesario realizar, con carácter previo al inicio de todo tratamiento y periódicamente o ante cambios sustanciales en el estado de la técnica, costes, naturaleza y alcance del tratamiento o su contexto, una identificación y evaluación de riesgos que cada Actividad del Tratamiento puede conllevar para los Derechos y Libertades de los Interesados. Y en base a este análisis definirse las medidas técnicas y organizativas apropiadas para mantener este nivel de riesgo en valores que puedan considerarse aceptables.

Por una parte, todo tratamiento de datos llevado a cabo por alguna Sociedad del Grupo, deberá contar con un análisis de riesgos para la seguridad de los datos y para los derechos y libertades de los interesados. Además, aquellos tratamientos que presenten un riesgo inherente alto o muy alto deberán contar con una Evaluación de Impacto en Protección de Datos.

Con el fin de asegurar el cumplimiento de estas obligaciones, el Grupo se ha dotará de un proceso documentado de gestión de riesgos para los derechos y libertades alineado con el artículo 32 del RGPD, que incluirá la documentación y evidencia de su ejecución asociado al Registro de Actividades del Tratamiento.

Además, dentro de los procedimientos relativos a la gestión de incidentes de seguridad y violación de de datos personales, se establecerán los procedimientos y obligaciones relacionados con la gestión de brechas de datos personales, notificación a la Autoridad de control y a nos interesados, en caso de que sea necesario.

4.7 Principio de Responsabilidad Proactiva

Las sociedades del Grupo que actúen como Responsable o Encargado del Tratamiento deberán dotarse de medios para cumplir con todo lo estipulado en la legislación de protección de datos, en esta Política y la normativa interna relacionada, y además deberán ser capaces de demostrarlo.

Para ello será obligatorio, tal y como recogerá en un procedimiento de verificación de cumplimiento de protección de datos del Grupo, que se analice para cada nuevo tratamiento o ante cambios sustanciales de su alcance, naturaleza o contexto, cómo se van a cumplir las obligaciones en materia de Protección de Datos a lo largo de todo el ciclo de vida de la este. Quedando documentado en el Registro de Actividades del Tratamiento tanto la Verificación como las tareas periódicas que se realicen sobre cada Actividad del Tratamiento.

5 Otras obligaciones

5.1 Principio de privacidad desde el diseño y por defecto

La privacidad desde el diseño consiste en incorporar la protección de los datos personales a lo largo de todo el ciclo de vida de un sistema, producto, servicio o proceso que implique el tratamiento de datos personales, con la finalidad de establecer las medidas y estrategias necesarias para asegurar el cumplimiento de todos los principios y requisitos legales que han de cumplirse con respecto al tratamiento de datos desde las primeras fases de la concepción de este.

Para aplicar correctamente la Privacidad desde el diseño y por defecto han de tenerse en cuenta las siguientes consideraciones: ha de ser proactivo no reactivo, la privacidad como configuración predeterminada (por defecto), integrar la privacidad desde la fase inicial de diseño, buscar siempre un equilibrio entre los diferentes intereses en juego, asegurar la privacidad durante todo el ciclo de vida, fomentar la transparencia y visibilidad del tratamiento para el interesado, y mantener un enfoque centrado el este.

Para asegurar el correcto cumplimiento de este principio, el Grupo se dotará de una política que asegure que se cumplen los principios de privacidad desde el diseño y por defecto recogidos en el art. 25 del RGPD, en la que se recogerán los objetivos que se establecen como línea base de privacidad para todos los proyectos que se lleven a cabo dentro del Grupo y que impliquen o puedan implicar el tratamiento de datos personales, las estrategias generales para alcanzar citados objetivos, así como los procesos asociados que se tendrán que implantar en todas las Sociedades para asegurar su cumplimiento.

5.2 Principios sobre la contratación de encargados del tratamiento

Si fuese preciso contratar a terceras empresas la realización de cualquier tipo de servicio o tarea que implique la necesidad de que traten, entendiendo que el mero acceso ya supone un tratamiento, datos personales de los que sea Responsable o Encargado cualquier empresa del Grupo, ha de tenerse en cuenta todas las obligaciones que establece el artículo 28 del RGPD.

En primer lugar, deberán seleccionarse exclusivamente proveedores que ofrezcan garantías suficientes para aplicar medidas técnicas y organizativas apropiadas en función del tratamiento de datos que vayan a realizar. Para ello en el proceso de evaluación de proveedores se tendrá en cuenta su capacidad para aplicar medidas de ciberseguridad y otras medidas directamente relacionadas con las obligaciones recogidas en el artículo 28 y en las Directrices para la elaboración de contratos entre Responsables y Encargados del Tratamiento de la Agencia Española de Protección de Datos[8].

Por otra parte, se establece la obligación para toda Sociedad de Grupo de regular la relación con este tipo de proveedores mediante la formalización de un contrato por escrito que deberá incluir tanto obligaciones en materia de protección de datos como un acuerdo de medidas técnicas de seguridad que se obligan a implantar en su tratamiento. El Grupo se dotará de contratos tipo que sigan las citadas Directrices de la Agencia, y que se adaptarán a aquellos casos que por sus especiales características lo requieran.

Y finalmente, se establecerán procedimientos y medidas para proceder a la verificación del

[8] Directrices accesibles aquí: https://www.aepd.es/documento/guia-directrices-contratos.pdf

cumplimiento por parte de los proveedores con acceso a datos personales de sus obligaciones contractuales y legales, tanto en el ámbito de las obligaciones legales en materia de protección de datos como en el de medidas de seguridad. Entre otras medidas, deberá incluirse un proceso de control y auditoría recurrente sobre las obligaciones de los proveedores que incluyan las mencionadas verificaciones.

5.3 Principios sobre la Corresponsabilidad

El artículo 26 del RGPD define la Corresponsabilidad como aquella situación en la que dos o más responsables determinan conjuntamente los objetivos y los medios del tratamiento. Fijando además la obligación de que se firme un acuerdo entre los Corresponsables con las obligaciones de cada uno respecto al tratamiento, sobre todo las relativas al ejercicio de derechos y el deber de información, que debe estar a disposición de los interesados.

Dentro de un Grupo empresarial como el nuestro existen situaciones en las que son varias empresas del Grupo las que deciden de forma conjunta las finalidades para que los datos son utilizados, y se emplean a su vez medios (sistemas, plataformas, servicios, etc) conjuntos para su ejecución. Por ejemplo, los tratamientos relativos a los Empleados están centralizados, participando en las decisiones asociadas a estos todas las sociedades que conforman el Grupo.

Ha de distinguirse esta situación de otras ocasiones en las que una sociedad del grupo contrata a otra para que le preste un servicio, para el que sea necesario que la segunda sociedad trate datos personales, pero que lo hará siguiendo exclusivamente las instrucciones de la primera; como, por ejemplo, contratar el uso de un sistema de información propiedad de otra empresa del Grupo. En este caso se tratará de un Encargo del Tratamiento y aplicarán las obligaciones del punto anterior.

Cuando se detecte que un tratamiento tiene dos o más sociedades del grupo como Responsables, se deberá firmar un acuerdo entre todas ellas que recogerá explícitamente las responsabilidades de cada una sobre el tratamiento y se introducirá un resumen del citado acuerdo en la Política de Privacidad correspondiente, para poner su contenido a disposición de los interesados.

5.4 Principios sobre Transferencias Internacionales de Datos

El tratamiento de información y/o datos personales que realice cualquier sociedad del Grupo como Responsable o como Encargada del Tratamiento, que implique una transferencia de los mismos fuera del Espacio Económico Europeo, deberá llevarse a cabo dentro del estricto cumplimiento de los requisitos establecidos en la legislación origen y en esta Política.

El RGPD exige que estas transferencias se realicen solo si se han tomado previamente garantías adecuadas (art. 46 RGPD) para que los datos transferidos se mantengan bajo un entorno de seguridad equivalente al de la Unión Europea o que la transferencia se realice al amparo de alguna de las situaciones que enumera el art. 49 RGPD, entre ellas, que el interesado haya dado su consentimiento explícito tras ser informado de los posibles riesgos de la transferencia.

Con el fin de asegurar el cumplimiento de estas obligaciones se desarrollará un procedimiento que regule la realización de transferencias internacionales de datos personales, que ha de incluir tanto la obligación de existencia de una base legitimadora de la transferencia, artículo 49 del RGPD, como la realización de un análisis de riesgos para los Derechos y Libertades de los afectados por causa de la propia transferencia, con el fin de definir, si fuese menester, medidas mitigadoras o atenuantes de estos riesgos.

Cumpliendo con el deber de transparencia se informará de lo que resulte pertinente en cuanto estas transferencias internacionales a los interesados a través de las políticas de privacidad.

5.5 Principios sobre los derechos de los interesados

El RGPD recoge la potestad de toda persona física cuyos datos estén siendo tratados por un responsable para ejercer sus derechos de acceso (conocer qué datos se tienen de él), rectificación (pedir su modificación), cancelación y oposición (pedir su baja total o parcial o restringir su utilización o posibles comunicaciones a terceros), limitación del tratamiento (conservándolos sólo para el ejercicio o defensa de reclamaciones), revocación (dejar sin efecto el consentimiento otorgado) y, en su caso, solicitar la portabilidad de sus datos.

Con el fin de asegurar que todo ejercicio de derechos que se ejerza ante alguna sociedad del Grupo es respondido en forma y plazo, y atendido adecuadamente, se establecerá un procedimiento de gestión de derechos de protección de datos, que, a su vez, se complementará con los Procedimientos operativos que cada Responsable o Encargado debe desarrollar atendiendo al contexto concreto de los tratamientos que realiza.

5.6 Principios obligatorios para los empleados y colaboradores

Dentro de los principios éticos que rigen todas las actividades del Grupo Empresarial, se espera que todos sus empleados y colaboradores no solo cumplan con la presente Política, sino que realicen un uso legal, transparente y adecuado de los datos personales a los que tengan acceso.

Con el fin de asegurar este tratamiento leal y lícito, se implantarán varias medidas asociadas a los profesionales que trabajen para el grupo. Por una parte, todo contrato laboral o de colaboración implicará un acuerdo de confidencialidad que no se extinguirá con el fin de la relación contractual, y que hará hincapié en todo lo referido a datos personales. Así mismo, se definirá una normativa que regule el uso de equipamiento y seguridad, de obligado cumplimiento para todos los profesionales, contemplará especialmente las normas en cuanto al tratamiento seguro de datos personales, incluyendo las medidas disciplinarias previstas a nivel laboral para cualquier incumplimiento.

Y, por último, la formación en materia de protección de datos de los empleados es crucial para el Grupo, por lo que se establecerán acciones formativas periódicas para asegurar los conocimientos, habilidades y actitudes necesarias en los empleados, con el objetivo de mejorar los tratamientos de información que contengan datos personales. Esta formación periódica se actualizará en función de los cambios legales y/o de contexto que sufran los tratamientos, para asegurar que los conocimientos de los empleados nunca se quedan obsoletos en este ámbito.

Si bien la citada normativa incluirá las obligaciones de los empleados en materia de tratamiento de datos personales, seguidamente se incluyen aquellas más importantes que siempre deberán tenerse en cuenta:

El usuario recibirá instrucciones sobre los tratamientos de datos personales para los que está autorizado, el tipo de acceso permitido (lectura, escritura, etc.) y su finalidad.

Solo tratará y accederá a aquellos datos para los que está autorizado, e informará inmediatamente a través del área de ciberseguridad o de su responsable, de cualquier acceso posible por su parte que considere excede sus necesidades profesionales.

El usuario sólo podrá utilizar los datos para la finalidad estipulada, que estará recogida en el

Registro de Actividades del Tratamiento, procurando además que los datos personales estén siempre actualizados y cancelándolos cuando ya no sean necesarios o pertinentes para la finalidad para la cual hubieran sido recabados.

En caso de que vaya a subcontratar terceras empresas para algún servicio o producto y que pueda producirse acceso por parte de esta a datos personales, deberá proceder según el los procedimientos establecidos, e informar, por los canales pertinentes, para que se pueda producir esta contratación siguiendo las obligaciones correspondientes.

Nunca comunicará datos personales a un tercero (proveedor, cliente u órgano administrativo) si no cuenta con la autorización de la organización. De forma que, si la comunicación no está embebida en los procesos de negocio, es decir, es puntual, deberá solicitar autorización previa a través del Responsable de Protección de Datos de su área de actuación.

En todo caso, la transmisión de datos personales a través de medios públicos, como correo electrónico o Internet, están prohibidas. De ser necesarias se contactará previamente con el área de ciberseguridad para determinar las medidas de seguridad que han de aplicarse. Siendo responsabilidad del área de ciberseguridad comunicarlo a la Oficina de Privacidad si considera que es necesario evaluar el nivel de riesgo del caso concreto de forma específica.

El usuario comunicará inmediatamente y sin dilación alguna, a través del área de ciberseguridad, cualquier sospecha, indicio o evidencia de que se ha producido un incidente de seguridad, especialmente si puede conllevar afectación a datos personales.

En el supuesto de que el usuario desee realizar alguna nueva Operación del Tratamiento, incluso si es de carácter temporal, deberá solicitar autorización a través del Responsable de Protección de Datos de su área de actuación, quien le informará de cualquier posible medida legal, técnica u organizativa que haya que adoptar.

6 Gobierno de la Protección de Datos

Con el fin de asegurar el cumplimiento riguroso por parte de todas las Sociedades que conforman en Grupo mercantil de sus obligaciones en materia de protección de datos el Grupo se dotará de una organización específica en materia de Protección de Datos.

Esta organización, junto con las funciones y obligaciones que a cada sujeto se le asignan en la misma, deberá estar recogida y desarrollada, en la que se recogen las siguientes figuras o puestos relativos a la Gestión diaria de todo lo relativo al tratamiento de datos personales:

- Consejo de Administración: La determinación de las Políticas del Grupo es responsabilidad del Consejo de Administración de MASORANGE como facultad indelegable.
- Comisión de Auditoría y Riesgos: en su función asesora e informativa, brinda asistencia al Consejo de Administración con respecto a la supervisión del cumplimiento de las Políticas del Grupo MASORANGE.
- Delegado de Protección de Datos (DPO): El Grupo ha decido nombrar un DPO de grupo, que tiene asignadas las atribuciones legalmente establecidas y con el que se podrá

contactar a través del correo electrónico

- Oficina de Privacidad: El Delegado de Protección de Datos contará con una oficina de apoyo para la realización de sus funciones.
- Comité de privacidad: El Comité de Privacidad es el órgano responsable de la toma de decisiones operativas relacionadas con el Sistema de Gestión de la Privacidad y de Protección de Datos, así como de monitorizar el cumplimiento de la legislación en este ámbito por parte del Grupo.
- Comité de Seguridad Global: Como principal órgano en materia de gestión de riesgos de seguridad, será el encargado de la aprobación de las evaluaciones de riesgos y planes de tratamiento, así como el órgano de la dirección en cuanto al reporte del SGPI.
- Responsable de protección de datos de área: punto de contacto del área que se le asigne con la Oficina de Privacidad y tendrá asignada la responsabilidad de ciertas tareas que la legislación asigna al Responsable del Tratamiento, de las que podrá delegar su realización, pero ostentando siempre la responsabilidad sobre las mismas.
- Responsable de recursos: punto de contacto con la Oficina de Privacidad en relación a cuestiones técnicas de los sistemas que soportan los tratamientos de datos: Funcionalidades, Accesos, Segregación de Funciones, Autorizaciones y demás medidas de seguridad.

7 Adhesión a códigos de conducta y certificaciones

Los códigos de conducta y las certificaciones en materia de RGPD facilitan la correcta aplicación del RGPD, de manera que permitan evaluar con mayor rapidez el nivel de protección de datos de productos y servicios. Si bien no limitará la responsabilidad de los responsables o encargados en cuanto al cumplimiento del RGPD, con arreglo a las competencias de la Autoridad de Control, sí se tienen en cuenta a la hora de graduar la posible sanción.

En caso de que MASORANGE tenga conocimiento de la existencia de un Código de Conducta relacionado con su sector de actividad, ésta debe tener en cuenta la posibilidad de adherirse al mismo, puesto que la adhesión a códigos de conducta y la obtención de certificaciones pueden ser utilizados como elementos para demostrar el cumplimiento de la normativa de protección de datos y puede utilizarse como elemento para demostrar que las empresas del Grupo MASORANGE, en la medida que presten un servicio a otra entidad o AAPP como encargados o subencargados, ofrecen garantías suficientes.

8 Control y evaluación

8.1 Mejora continua

El Grupo MASORANGE está firmemente comprometido con la mejora continua, y más concretamente en el caso del Sistema de Gestión de la Privacidad alineado y basado en la ISO

27701 así como en la normativa relativa a la protección de datos personales, se implantarán las medidas necesarias para asegurar que este es revisado periódicamente, ante cambios sustanciales del sistema o la legislación vigente.

La presente Política será revisada con una periodicidad al menos anual y en caso de que se produzcan cambios sustanciales en el contexto de la privacidad y protección de datos del Grupo MASORANGE. Por otra parte, el Sistema de Gestión de la Privacidad incluirá un calendario documentado del proceso periódico de revisiones de todos los estándares, procedimientos, normas, procesos y metodologías que la desarrollen. Estas revisiones buscarán actualizar y mejorar los citados elementos del SGPI, pudiendo establecerse a raíz de estas un plan de mejora que deberá ser aprobado por el Comité de Privacidad.

Por otra parte, el propio Sistema incluirá la realización de auditorías tanto internas como externas, que serán de carácter anual en relación con la certificación de la ISO 27701.

De las citadas auditorías se extraerá un plan de acción que será aprobado por parte del Comité de Privacidad y/o el Comité de Seguridad Global, según su impacto, e incluirá los puntos de mejora detectados.

8.2 Responsabilidades sobre la presente Política

Será responsabilidad de la Oficina de Privacidad mantener actualizada la presente política, así como de asegurarse que es puesta a disposición de todos los profesionales del Grupo. Igualmente, será responsable de verificar que el resto de normativa interna que la desarrolla está correctamente actualizada y mantenida por parte de las áreas responsables.

Todo profesional del Grupo es responsable de asegurarse que tiene acceso, conoce y aplican, la presente Política, y todos los documentos que la desarrollan en la medida que lo precisen en sus actividades profesionales. Además, en caso de detectar la necesidad de modificación de cualquiera de estos documentos, ante cambios legales, de contexto, tratamiento o riesgos, será su obligación escalarlo a la Oficina de Privacidad, que revisar y, en su caso, propondrá su actualización.

8.3 Resolución de conflictos

En caso de que se produzcan conflictos de intereses o de interpretación de la presente Política, será el Comité de Privacidad como máximo órgano en cuanto a la Gestión de la Protección de Datos en el Grupo, quien tendrá la responsabilidad de su resolución, apoyándose para ello en el asesoramiento del Delegado de Protección de Datos.

Apéndice I. Ejemplos de Tipos de datos personales

Datos especialmente sensibles	**Información familiar**	**Información de contacto**
Historial criminal	Nombre de hijos, padres o compañeros sentimentales	Dirección
Antecedentes penales	**Información laboral**	Email
Citaciones de tráfico	Departamento	Número de teléfono
Resultados del "Test de Drogas"	Tipo de contrato	**Información de cuentas de usuario**
Opinión política	Acciones disciplinarias	Fecha de creación de la cuenta
Religión	Fecha de extinción laboral y motivos	Identificador de la cuenta
Origen racial o étnico	Información de salud y seguridad	Contraseña de la cuenta
Orientación sexual	Detalles del puesto de trabajo	**Información de navegación web**
Identificación personal	Salario	Tiempo de navegación
Número de identificación personal	Fecha de inicio de la relación laboral	Información de cookies
Nombre completo	**Experiencia profesional y afiliaciones**	Historial de webs visitadas
Fecha de nacimiento	Experiencia profesional	**Biométrica**
Género	Membresía profesional	Reconocimiento facial
Estado civil	Cualificaciones/certificaciones	Huella dactilar
Imagen	Afiliación sindical	Reconocimiento por voz
Firma	Formación y habilidades	**Redes sociales**
Grabación de voz	Títulos académicos e Historial educativo	Cuentas de redes sociales
Productos y Servicios	**Financiero**	Contactos
Número de teléfono	Información cuenta bancaria (IBAN)	Historial de redes sociales
Identificador de cliente	Número de tarjeta de crédito	**Información comercial**
Datos de facturación	Ingresos	Perfiles comerciales
Localización		Comunicaciones y campañas recibidas