GRUPO CORPORACIÓN MASAVEU

(Corporación Masaveu, S.A. y Sociedades Dependientes)

Política sobre la responsabilidad en el ámbito digital

1. Finalidad

La Constitución española garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen. Como derecho fundamental distinto reconoce el derecho a la autodeterminación informativa o libertad informática, que es el derecho a la protección de datos personales, complementario del anterior, pero que no se reduce sólo a los datos íntimos, sino que abarca todos aquellos que identifiquen o permitan la identificación de la persona, pudiendo servir para la confección de su perfil ideológico, racial, sexual, económico o de cualquier otra índole, o que sirvan para cualquier otra utilidad que en determinadas circunstancias constituya una amenaza para el individuo (STC 292/2000).

Los principios de igualdad, dignidad, no discriminación y el derecho a la integridad física y moral son principios jurídicos universales, consagrados en la Constitución Española, que asigna a los poderes públicos la obligatoriedad de promover las condiciones necesarias para que la igualdad y no discriminación sean efectivas.

El artículo 8, apartado 1, de la Carta de los Derechos Fundamentales de la Unión Europea y el artículo 16, apartado 1, del Tratado de Funcionamiento de la Unión Europea establecen que toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan.

El Reglamento General de Protección de Datos -Reglamento (UE) 2016/679 (RGPD)- y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD) configuran conjuntamente el desarrollo del derecho fundamental a la protección de datos de carácter personal. La mayor novedad que presenta el Reglamento europeo es la evolución de un modelo basado en el control, fundamentalmente de carácter formal, del cumplimiento de la normativa de protección de datos a otro que descansa en el principio de responsabilidad activa, que exige una previa valoración del riesgo que pudiera generar el tratamiento de los datos personales para, a partir de esa valoración, adoptar las medidas que procedan.

Mediante la presente política de responsabilidad en el ámbito digital el Grupo Corporación Masaveu manifiesta su compromiso de cumplir con las obligaciones normativas en el ámbito digital detallando las mismas, así como las responsabilidades en que se podría incurrir ante un eventual incumplimiento de las mismas promoviendo de esta forma en el seno de su organización el respeto a la privacidad en el entorno digital.

2. Ámbito de aplicación

Esta política resultará de aplicación a todos los altos directivos, directivos, trabajadores, y, en general a todas las personas que presten servicios en el Grupo Corporación Masaveu, con independencia de cuál sea la modalidad jurídica que determine su relación laboral o de servicios, de la posición que ocupen en la estructura organizativa o del lugar geográfico en el que desempeñen su trabajo. Por consiguiente, afectará a todas las sociedades que integran el Grupo Corporación Masaveu, independientemente del país en el que operen.
A los efectos de esta política, por el Grupo Corporación Masaveu se entenderá el Grupo constituido por la sociedad Corporación Masaveu, S.A. (en adelante, "la Sociedad") y todas las sociedades filiales y participadas que se encuentren, respecto de aquélla, en la situación prevista en el artículo 42 del Código de Comercio.

En el resto de sociedades en la que Corporación Masaveu participe directa o indirectamente sin tener control, Corporación Masaveu promoverá a través de su participación en sus órganos de gobierno, la adopción de políticas de respeto a los derechos humanos.

3. Principios de actuación

Para la consecución de los objetivos señalados, el Grupo Corporación Masaveu asume y se compromete a cumplir con las siguientes obligaciones en materia digital:

Obligaciones generales

Se aplicarán medidas adecuadas y eficaces y que permitan demostrar la conformidad de las actividades de tratamiento con la normativa aplicable (RGPD y LOPDGDD), incluida la eficacia de las medidas adoptadas, que se revisarán y actualizarán cuando sea necesario.

Dichas medidas tendrán en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento, así como el riesgo para los derechos y libertades de las personas físicas (artículos 24.1 RGPD y 28 LOPDGDD).

EL Grupo Corporación Masaveu adopta en el tratamiento de los datos una actitud proactiva, incorporando el valor de la privacidad en su actividad ordinaria, garantizando el cumplimiento de este derecho como un activo de la organización y un elemento distintivo de competitividad en el mercado.

Obligaciones específicas en el ámbito digital

- Informar a los usuarios y usuarias sobre el tratamiento de sus datos y el ejercicio de sus derechos.

  Se informará de forma clara y sencilla sobre los aspectos más importantes del tratamiento que se realice sobre datos personales, identificando quién los trata, con qué base jurídica, para qué finalidad, y sobre la forma de ejercer sus derechos.

  En cumplimiento de los artículos 13 y 14 del RGPD y 11 LOPDGDD no podrá denegarse el ejercicio de estos derechos en el caso de que la persona quiera ejercitarlos por un procedimiento o cauce diferente al que se le ofrezca.
- Aplicar principios relativos al tratamiento
  En el tratamiento de datos de clientes, personal, proveedores, ciudadanos y ciudadanas se aplicarán los principios de licitud, lealtad, transparencia, limitación de la finalidad, minimización, exactitud, limitación del plazo de conservación, integridad, confidencialidad y responsabilidad proactiva, con el alcance dado a los mismos por el artículo 5 del RGPD.
- Garantizar la licitud del tratamiento
  Se garantizará la licitud del tratamiento de los datos de clientes, su personal, ciudadanos y ciudadanas sobre la base de alguna de las causas contempladas en el artículo 6 y también, en caso de categorías especiales de datos personales (datos de salud, de carácter político o sindical, relativos a la vida sexual, etc.), en su artículo 9, ambos del RGPD
- Designación de un Delegado de Protección de Datos (DPD)
  En los supuestos legalmente exigibles se designará a una persona como Delegado/a de Protección de Datos. Esta persona contará con la debida cualificación, garantizándole los medios necesarios para el ejercicio de sus funciones de manera independiente, debiendo comunicar la designación a la Agencia Española de Protección de Datos (artículos 37 a 39 RGPD, y 34 a 36 LOPDGDD).

  Sin perjuicio de lo anterior, si las circunstancias del tratamiento así lo aconsejan y la entidad dispone de recursos para ello, se podrá valorar la designación de un Delegado de Protección de Datos.

  En ambos casos se ofrecerá todo el apoyo necesario al DPD para que pueda atender en las mejores condiciones las reclamaciones que le dirijan los ciudadanos y ciudadanas cuando opten por esta vía antes de plantear una reclamación ante la AEPD, o en los casos en que la AEPD decida su traslado a la persona responsable con carácter previo a su admisión a trámite (artículo 65.4 LOPDGDD)

- Aplicar la privacidad "desde el diseño" y "por defecto
  Tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, es decir, "desde el diseño", se aplicarán medidas técnicas y organizativas apropiadas fin de cumplir eficazmente las obligaciones legales y proteger los derechos de las personas afectadas (artículo 25.1 RGPD).

  Asimismo, se aplicarán las medidas técnicas y organizativas apropiadas para garantizar que, por defecto, sólo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento. Esta obligación se aplicará a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad (artículo 25.2 RGPD).

El incumplimiento de estas obligaciones específicas, podrá dar lugar a las siguientes **responsabilidades en el ámbito digital**.

- **Responsabilidad administrativa por infracción de la normativa de protección de datos**
  Entre los hechos que constituirían una infracción a la normativa de protección de datos y que serían, por tanto, susceptibles de sanción, se encuentran:
  - No facilitar la información que permita a las personas usuarias conocer quién y para qué tratarán sus datos personales. Conseguir los datos personales de una persona de manera ilícita, engañosa o fraudulenta, en particular, mediante la suplantación de la identidad
  - Utilizar los datos de carácter personal de una persona o comunicarlos a terceros sin una base jurídica que lo permita, en particular si se trata de datos sensibles como la ideología, religión, creencias, origen étnico, salud, vida y orientación sexual.
  - Utilizar los datos de carácter personal de una persona para fines distintos e incompatibles de aquellos para los que fueron recogidos.
  - Las víctimas de violencia de género gozan de especial protección que alcanza a la utilización, acceso y difusión de sus datos personales, a fin de evitar verse expuestas a nuevos riesgos de dicha naturaleza. En particular, la difusión de datos especialmente sensibles de una persona física (en contenidos tales como imágenes, audios o videos de carácter sexual o violento que permitan identificarla) publicados a través de los diferentes servicios de internet sin consentimiento, se considera un tratamiento ilícito de datos personales y, por tanto, puede constituir una infracción de la normativa de protección de datos sancionable por la Agencia Española de Protección de Datos con multas que en los casos más graves pueden alcanzar los 20 millones de euros o el 4% del volumen global de facturación de la compañía (art. 83.5 RGPD).

- **Responsabilidad Civil**
  Los ciudadanos y ciudadanas podrían tener que indemnizar a la persona afectada por los daños y perjuicios, materiales y morales, que se deriven de su conducta ilícita en materia de protección de datos personales (artículos 82 RGPD; 1.101 y 1.902 Código civil). Los padres, tutores, acogedores y guardadores legales o de hecho podrían tener que responder igualmente por los daños y perjuicios causados por sus hijos y tutelados menores con sus dispositivos móviles (artículo 1.903 Código Civil).
- **Responsabilidad Penal**
  La evolución de las tecnologías de la información y la comunicación y la extensión de su uso a través de los servicios y aplicaciones de Internet, como redes sociales, mensajería instantánea o correo electrónico en dispositivos inteligentes, ha llevado a que se utilicen como un cauce habitual no sólo para la comisión de infracciones en materia de protección de datos, sino también hechos tipificados como delitos. Expresiones como ciberacoso, ciberbullying, sexting, grooming, phishing, pharming o carding, que cada vez nos resultan más familiares, son términos en inglés que identifican situaciones de acoso, amenazas, coacciones, revelación de secretos, delitos sexuales, violencia de género o estafas.

  El código penal tipifica determinadas conductas en el ámbito digital como delitos, como los que atentan a la integridad moral, de descubrimiento y revelación de secretos, de amenazas, coacciones, acoso; calumnias e injurias, de violencia de género, suplantación de identidad, o de daños informáticos, entre otros.
- **Responsabilidad disciplinaria por infracción en el entorno laboral para la empresa:**
  - **En materia de relaciones laborales**
    La Ley sobre Infracciones y Sanciones en el Orden Social tipifica como infracciones muy graves:
    - "Los actos del empresario que fueren contrarios al respeto de la intimidad y consideración debida a la dignidad de los trabajadores" (artículo 8.11).
    - "El acoso sexual, cuando se produzca dentro del ámbito a que alcanzan las facultades de dirección empresarial, cualquiera que sea el sujeto activo de la misma" (artículo 8.13).
    - "El acoso por razón de origen racial o étnico, religión o convicciones, discapacidad, edad y orientación sexual y el acoso por razón de sexo, cuando se produzcan dentro del ámbito a que alcanzan las facultades de dirección empresarial, cualquiera que sea el sujeto activo del mismo, siempre que, conocido por el empresario, éste no hubiera adoptado las medidas necesarias para impedirlo" (artículo 8.13 bis).

      Las infracciones muy graves se sancionan por la Inspección de Trabajo y Seguridad Social con multas que van desde 6.251 a 187.515 euros.

- **Infracciones en materia de prevención de riesgos laborales**
  Asimismo, se tipifican como infracciones graves: "No llevar a cabo las evaluaciones de riesgos y, en su caso, sus actualizaciones y revisiones, así como los controles periódicos de las condiciones de trabajo y de la actividad de los trabajadores que procedan, o no realizar aquellas actividades de prevención que hicieran necesarias los resultados de las evaluaciones, con el alcance y contenido establecidos en la normativa sobre prevención de riesgos laborales" (artículo 12.1.b). Las infracciones graves se sancionan por la Inspección de Trabajo y Seguridad Social con multas que van desde 626 a 6.250 euros.
- **Infracciones en materia de igualdad:**
  Responsabilidad que se deriva en virtud de lo que establece la Ley Orgánica 3/2007, de 22 de marzo, para la igualdad efectiva de mujeres y hombres que, en sus artículos 45 y 46, establece la obligación de que las empresas que reúnan ciertos requisitos (más de 50 trabajadores, cuando así lo establezca el convenio colectivo o lo acuerde la autoridad laboral en un procedimiento sancionador) dispongan de un plan de igualdad que contenga un conjunto de medidas tendentes a alcanzar la igualdad de trato y oportunidades entre mujeres y hombres, así como a eliminar la discriminación por razón de sexo.
  Mediante el Real Decreto-Ley 6/2019, de 1 de marzo, se establecieron nuevas obligaciones, en especial en lo relativo a la constitución, características y condiciones para la inscripción y acceso al Registro de Planes de Igualdad.
- **Responsabilidad disciplinaria por infracción en el entorno laboral para los empleados y empleadas:**
  Los trabajadores podrán ser sancionados por incumplimientos laborales, de acuerdo con la graduación de faltas y sanciones establecidas en las disposiciones legales o en los convenios colectivos aplicables, que, en caso de faltas muy graves, pueden llegar incluso al despido disciplinario (artículo 58 del Estatuto de los Trabajadores).

4. Mecanismos de supervisión, control y aplicación de las Políticas Corporativas

Las sociedades del Grupo adoptarán los mecanismos de control necesarios para asegurar, dentro de una adecuada gestión empresarial, el cumplimiento de la normativa en materia de protección de datos, así como de los principios y las buenas prácticas enunciadas en esta política. La estructura organizativa de la que se ha dotado el Grupo es la siguiente:

- Delegado de Protección de Datos ("DPD") en la división de medicina: Figura que ejerce, entre otras, la función de supervisar el cumplimiento de la normativa, informar y asesorar a estas sociedades en materia de protección de datos, además de servir de punto de contacto con la Autoridad de Control competente.
- Comité Interno de Seguridad y Protección de Datos: Órgano integrado por los responsables de Tecnologías de la Información y el de Recursos Humanos, cuyo cometido es abordar los asuntos de privacidad y seguridad del Grupo desde una perspectiva integrada y conjunta. Este órgano puede contar, si así lo precisa, con el apoyo de expertos en la materia y también de la Unidad de Cumplimiento Normativo.

5. Aprobación y revisión de esta política

Esta Política fue aprobada inicialmente por el Consejo de Administración el 22 de junio de 2021 y modificada por última vez el 18 de junio de 2024.