Marco de gobierno corporativo sobre la protección de datos personales y la seguridad de la información

Grupo Catalana Occidente

Introducción

El Consejo de Administración de Grupo Catalana Occidente S.A. tiene atribuida la competencia de diseñar, evaluar y revisar con carácter permanente el sistema de gobierno, y específicamente, el establecimiento de una estructura organizativa y una distribución de funciones transparente y apropiada que garantice la gestión sostenible, sana y prudente de la actividad y los mecanismos eficaces de control interno, mediante la aprobación de las políticas y procedimientos que conforman el sistema de gobierno y desarrollan los principios y valores del Grupo Catalana Occidente, tal y como se definen en su Código ético.

El Grupo Catalana Occidente está constituido, a efectos del ámbito y alcance del presente Marco de gobierno corporativo, por Grupo Catalana Occidente, S.A., sus sociedades filiales y agrupaciones de interés económico de las que las mismas formen parte (en adelante, indistintamente, "GCO" o el "Grupo").

La divulgación del Marco de gobierno corporativo sobre la protección de datos personales y la seguridad de la información de GCO tiene como objeto y finalidad el fomento de la transparencia y la contribución al mantenimiento de la confianza de sus grupos de interés, posibilitando que éstos puedan relacionarse con el Grupo sin que el temor a los riesgos en relación con el tratamiento de los datos personales y la seguridad de la información, puedan influir en su capacidad para decidir y actuar libremente, mediante la preservación de la confidencialidad y privacidad de los datos personales y la información, y de un entorno de gestión seguro de los sistemas y servicios de tratamiento que la soportan.

Principios y valores

Entre los principios y valores generales que inspiran el funcionamiento y la actuación del Grupo recogidos en su Código ético, se encuentran la integridad y honestidad, la imparcialidad, la profesionalidad, la sostenibilidad, el compromiso social, el respeto al medioambiente, la marca, imagen y reputación corporativa, el respeto y salvaguarda de los derechos humanos, la transparencia y la confidencialidad, y el cumplimiento de la legalidad y del sistema de gobierno corporativo, esto es, el compromiso del respeto a la privacidad y confidencialidad de las personas que se relacionan con el Grupo, ya tengan la condición de accionistas, empleados, clientes en el sentido amplio del término, proveedores, distribuidores o colaboradores, y, en particular, la protección de los derechos y las libertades fundamentales en relación con el tratamiento de sus datos personales.

GCO siempre ha estado firmemente comprometido con el cumplimiento de la normativa sobre la protección de datos personales, en especial, el 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), la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD) que lo desarrolla, y demás normativa de aplicación; así como también con las directrices y recomendaciones de las autoridades de control sobre la protección de datos personales, tanto nacionales como internacionales, las guías sectoriales a las que las entidades que conforman el Grupo se encuentran adheridas, las mejores prácticas y estándares internacionales, y la normativa interna que les resulta de aplicación conforme a las políticas y procedimientos adoptados por el Grupo.

Como consecuencia de lo anterior, GCO se ha comprometido a realizar un tratamiento de los datos personales de las personas físicas que se relacionan con el Grupo ajustado a los principios siguientes:

- Licitud, lealtad y transparencia en el tratamiento de los datos personales de los interesados, obteniendo dichos datos por medios lícitos y transparentes, facilitándoles toda la información relativa a al tratamiento de forma transparente y en un lenguaje claro y sencillo, y recabando el consentimiento explícito de los mismos en su caso cuando sea necesario.
- Limitación de la finalidad; esto es, los datos personales serán recogidos y tratados con fines determinados, explícitos y legítimos, de conformidad con la finalidad y propósito informados al interesado en el momento de la obtención de los mismos.
- Minimización de los datos, esto es, los tratamientos de los datos personales serán adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados.
- Exactitud, esto es, los datos personales objeto de tratamiento deberán ser exactos y si fuera necesario actualizados, suprimiendo o rectificando aquellos inexactos.
- Limitación del plazo de conservación, esto es, los datos personales objeto de tratamiento serán mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento.
- Integridad y confidencialidad, esto es, los datos personales serán tratados de tal manera que se garantice una seguridad adecuada de los mismos, protegiéndolos contra su tratamiento no autorizado o ilícito, y contra su pérdida o destrucción mediante la aplicación de medidas técnicas u organizativas apropiadas.
- Responsabilidad proactiva y rendición de cuentas, esto es, no solo deberá velarse por el cumplimiento de los anteriores principios relativos al tratamiento de datos personales, sino que, además, deberá ser posible demostrarlo.

Asimismo, GCO promueve que dichos principios intrínsecos a la protección de datos personales y la seguridad de la información estén presentes en los procesos y procedimientos siguientes:

- En el diseño e implementación de los procedimientos que impliquen el tratamiento de datos personales, asegurando la integración de la seguridad y la privacidad en los procesos de negocio, contribuyendo así a la calidad y sostenibilidad de los mismos.
- En el diseño, distribución y comercialización de los productos y servicios ofrecidos por las entidades que conforman el Grupo, implementando las medidas de seguridad adecuadas al nivel de riesgo, en los sistemas y plataformas que impliquen el tratamiento de datos personales, esto es, la denominada protección de datos personales desde el diseño y por defecto.
- En el análisis del riesgo sobre la protección de datos de los procesos de las entidades que conforman el Grupo que impliquen el tratamiento de datos personales, realizándose, en aquellos que entrañen un alto riesgo, evaluaciones de impacto relativas a la protección de datos, con la finalidad de mitigar dicho riesgo y garantizar la protección de los datos personales, adecuando las medidas de seguridad organizativas y técnicas al nivel de riesgo.
- En la transparencia informativa a los interesados, la publicación y difusión de la Política de Privacidad del Grupo actualizada y la incorporación del documento informativo sobre la protección de datos personales en los procesos de contratación de los productos y servicios comercializados por las entidades que conforman el Grupo.
- En la cumplimentación de los derechos de acceso, rectificación, supresión y derecho al olvido, oposición, limitación del tratamiento y portabilidad que sean ejercitados por los

interesados, así como la comunicación a los mismos de las brechas de seguridad cuando puedan suponer un perjuicio para el derecho a la protección de sus datos personales.

- En la evaluación de los criterios de privacidad en los procesos de selección de los proveedores con los que las entidades que conforman el Grupo establecen relaciones de negocio y en los procesos de contratación que impliquen el tratamiento de datos personales.
- En la consideración de los datos personales como activos estratégicos de la información y de los sistemas y servicios de tratamiento que la soportan, a efectos de dotarlos de ciber-resiliencia y garantizar la confidencialidad, integridad, disponibilidad, y resiliencia de la información y minimizar los riesgos que les afectan, en especial, en el ámbito de la ciberseguridad.

Estructura organizativa y funciones

La estrategia de sostenibilidad del Grupo orienta su marco de actuación hacia la creación de valor para la sociedad, la ética, la transparencia y el compromiso con la legalidad, integrando voluntariamente en la misma una gestión responsable, bajo los criterios de sostenibilidad, teniendo en consideración los factores ambientales, sociales y de gobierno corporativo, fomentando un comportamiento ético con sus grupos de interés, aplicando con rigor los principios de buen gobierno y contribuyendo al bienestar de la sociedad a través de la creación de valor social sostenible como consecuencia de su integración no sólo en el corto sino también en el medio y largo plazo.

En línea con su estrategia de sostenibilidad, el Grupo ha identificado como un punto clave de su organización la protección de datos personales y la seguridad de la información, en especial, la ciberseguridad y, en aras al cumplimiento de tales objetivos de desarrollo de su actividad bajo criterios de responsabilidad, ética, transparencia y compromiso con la legalidad, maximización de la creación de valor sostenible para sus grupos de interés en todas sus dimensiones, la prevención y mitigación de los eventuales impactos negativos sobre la materia y la contribución a la mejora de la reputación del Grupo y las entidades que lo componen; se ha dotado de la estructura organizativa, funciones, políticas de sistema de gobierno y mecanismos de control necesarios y adecuados para su consecución, establecidos por el Consejo de Administración del Grupo, y de cuya adecuada implementación de conformidad con las directrices definidas se asegura su Comité de Dirección, y en especial, los siguientes:

- GCO dispone de la función clave de verificación del cumplimiento, que forma parte del sistema integral de control interno y del de gobernanza del Grupo, se encuentra enmarcada en la segunda línea de defensa, en coordinación con el resto de funciones fundamentales y apoyada en el conjunto de la organización y comprende el asesoramiento a los órganos de administración de las entidades que conforman el Grupo, acerca del cumplimiento de las disposiciones legales, reglamentarias y administrativas que les afecten, así como acerca del cumplimiento de su normativa interna, la evaluación de las posibles repercusiones de cualquier modificación del entorno legal en las operaciones del Grupo, y la determinación y evaluación del riesgo de cumplimiento, especialmente, en lo relativo a la protección de datos personales y la seguridad de la información. En este sentido, el Responsable de la función de verificación del cumplimiento del Grupo se encuentra certificado de conformidad con el Esquema de Certificación de Delegados de Protección de Datos de la Agencia Española de Protección de Datos, al amparo de las previsiones del artículo 42 del Reglamento General de Protección de Datos.

- GCO cuenta con un Comité de Verificación del Cumplimiento, para la coordinación, supervisión y el establecimiento de criterios comunes para todas las entidades que conforman el Grupo en relación con la aplicación de la legislación que les afecta, el cual es responsable de velar por el cumplimiento de la normativa interna desarrollada en relación con el sistema de prevención y detección de delitos en los que pueden incurrir las personas jurídicas del Grupo, incluida la normativa sobre protección de datos personales y la seguridad de la información, cuya composición, funciones y periodicidad de sus reuniones se regulan en el Código ético de Grupo y sus protocolos de desarrollo, en particular, en el Protocolo del Responsable de Cumplimiento Penal.
- GCO dispone de la figura del delegado de protección de datos, de conformidad con lo previsto en el artículo 37 del Reglamento General de Protección de Datos en relación con el artículo 34 de la LOPDGDD que la desarrolla, para velar por el cumplimiento de la normativa sobre protección de datos aplicable, supervisando y asesorando a los responsables del tratamiento del Grupo, y actuar como interlocutor y contacto ante las autoridades de control competentes. En este sentido, la delegada de protección de datos del Grupo se encuentra certificada de conformidad con el Esquema de Certificación de Delegados de Protección de Datos de la Agencia Española de Protección de Datos, al amparo de las previsiones del artículo 42 del Reglamento General de Protección de Datos. Asimismo, las entidades del Grupo englobadas bajo el negocio del seguro de crédito disponen también de dicha figura, de conformidad con la legislación que les aplique en cada caso. En idéntico sentido, el negocio funerario del Grupo también dispone de la figura del delegado de protección de datos.
- GCO cuenta con un Comité de Protección de Datos Personales, como órgano ejecutivo responsable de la aplicación de la normativa relativa a la protección de datos personales y al uso de los recursos de las tecnologías de la información y comunicaciones, asumiendo las funciones del Comité de Verificación del Cumplimiento en esta materia, cuya composición, funciones y periodicidad de sus reuniones se regulan en la Política de Protección de Datos Personales y de uso de recursos TIC del Grupo. En el caso del negocio de crédito, cuyo establecimiento principal (Atradius N.V.) se encuentra en los Países Bajos a efectos de la determinación de la autoridad de control competente, cuenta también con un Comité Asesor de Protección de Datos, del que forman parte su delegado de protección de datos y los directores de diversas unidades de negocio y, en cada uno de los países en los que opera existe un representante para velar en esos territorios por el cumplimiento de las normativas de protección de datos personales aplicables.
- Asimismo, GCO dispone de la figura del Responsable de Seguridad tecnológica, con las funciones, entre otras, de coordinar y controlar las medidas de seguridad técnicas de los sistemas de información del Grupo exigidas por el Reglamento General de Protección de Datos, ponderándolas según el estado de la técnica y el coste de su aplicación, con la finalidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento. De igual forma, las entidades del Grupo englobadas bajo el negocio del seguro de crédito disponen de su propio Responsable de Seguridad tecnológica.
- GCO dispone de la función clave de control de gestión de riesgos, que se encuentra enmarcada en la segunda línea de defensa, en coordinación con el resto de funciones fundamentales y apoyada en el conjunto de la organización y a la cual corresponde, la identificación, evaluación, control y gestión de los riesgos actuales y emergentes, con el objetivo de garantizar la eficacia y eficiencia de las operaciones que se realizan en el Grupo y las entidades que lo conforman.

- Finalmente, GCO cuenta con un Comité de Dirección, en quien el Consejo de Administración ha delegado la gestión ordinaria del Grupo que, entre otras funciones, monitoriza el perfil de riesgos del Grupo, para garantizar el sistema de gestión de todos los riesgos del Grupo incluida la ciberseguridad, apoyado en el conjunto de la organización a través de los Comités de Negocio de Seguros Generales y Vida y del Seguro de Crédito, del Comité de Inversiones y del Comité de Operaciones, que controla la actualización y valoración de los riesgos y realiza un seguimiento periódico de los mismos, y del que es miembro el Responsable de los sistemas de tecnologías de la información (CIO) del Grupo. El negocio del seguro de crédito cuenta asimismo con un Comité de Riesgo Operacional, con la finalidad de identificar, evaluar y gestionar los riesgos operacionales, del cual es miembro el Director de los servicios IT.

Los referidos comités internos, funciones clave y responsables del Grupo cooperan en el desempeño conjunto y coordinado de las actividades tendentes a asegurar y garantizar en el seno de la organización el cumplimiento de la normativa sobre la protección de datos personales y la seguridad de la información; colaborando de forma permanente con las autoridades de control competentes sobre la materia en los territorios donde operan las entidades que conforman el Grupo; y participando activamente en los grupos de trabajo y órganos consultivos sobre la materia de las asociaciones sectoriales más representativas a las que se encuentran adheridas.

Políticas y procedimientos

GCO ha aprobado, en relación con la protección de datos personales y la seguridad de la información, a cuyo cumplimiento están obligados todos los consejeros, empleados, distribuidores y colaboradores de las entidades que conforman el Grupo, entre otras, las políticas y procedimientos siguientes:

- Política de privacidad, publicada en las páginas web de las entidades del Grupo.
- Política de protección de datos personales y de uso de los recursos TIC, que regula, entre otras cuestiones, los análisis de riesgos y las evaluaciones de impacto relativas a la protección de datos personales.
- Política de cookies, adaptada a la Guía sobre el uso de las cookies emitida por la Agencia Española de Protección de Datos y publicada en las páginas web de las entidades del Grupo, donde el usuario puede administrar y modificar en todo momento sus preferencias sobre el uso de cookies.
- Política de Seguridad de la Información Corporativa, normas de desarrollo y Modelo de gobierno de seguridad.
- Protocolo de conservación, supresión y bloqueo de datos personales.
- Procedimiento de atención de los derechos de acceso, rectificación, supresión y derecho al olvido, limitación del tratamiento, portabilidad y oposición de datos personales.
- Procedimiento de gestión y notificación de brechas de seguridad, adaptado a la Guía para la notificación de brechas de datos personales emitida por la Agencia Española de Protección de Datos y a la Guía nacional de notificación y gestión de ciberincidentes emitida por el Consejo Nacional de Ciberseguridad.

Asimismo, GCO se asegura de la actualización permanente de las políticas y procedimientos en relación con cualquier modificación del entorno legal y la evaluación del riesgo de cumplimiento mediante sus revisiones periódicas objeto de difusión entre los sujetos obligados

a su cumplimiento, para su debido conocimiento y aplicación, y promueve una cultura de cumplimiento relativa a la protección de datos personales y la seguridad de la información mediante acciones de concienciación y formación continuas dirigidas a los mismos.

Medidas de seguridad

GCO aplica las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado a los riesgos en el tratamiento de los datos personales, teniendo en consideración el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y las finalidades del tratamiento de datos personales, y los riesgos de probabilidad y gravedad o impacto para los derechos y libertades de las personas físicas, en especial, su derecho a la protección de datos personales, y que pueden incluir, entre otras, las siguientes:

- La seudonimización y el cifrado de datos personales.
- La capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento.
- La capacidad de restaurar la disponibilidad y el acceso a los datos personales con celeridad en caso de incidente físico o técnico.
- La implementación de procesos de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento de datos personales, teniendo en consideración los riesgos del tratamiento de los datos personales derivados de su destrucción, pérdida, alteración accidental o ilícita y de su comunicación o acceso no autorizados.

Asimismo, el Grupo se asegura la adopción de medidas de seguridad para garantizar que los sujetos obligados que actúen bajo su autoridad y tengan acceso a datos personales los traten siguiendo sus instrucciones, de conformidad con la Política de protección de datos personales y de uso de los recursos del TIC de GCO o, en los casos de los negocios de crédito y funerario del Grupo, las Políticas de protección de datos personales correspondientes y legislación aplicable.

Mecanismos de control y supervisión

GCO dispone de un sistema de control interno que abarca la supervisión de todos los procesos de las actividades de las entidades que conforman el Grupo, con el objetivo de proporcionar un grado de seguridad razonable en cuanto a la consecución de objetivos dentro de las siguientes categorías:

- La eficacia y eficiencia de las operaciones.
- La fiabilidad de la información financiera.
- La protección de activos, considerando como activos estratégicos la información y los sistemas y servicios de tratamiento que la soportan.
- El cumplimiento de las leyes y normas aplicables, en especial, la normativa sobre la protección de datos personales y la seguridad de la información.
- Los mecanismos adecuados respecto a su solvencia que permitan identificar y medir todos los riesgos significativos existentes y cubrir adecuadamente esos riesgos con fondos propios admisibles.

Complementariamente, GCO dispone de un sistema de control de gestión de riesgos, que tiene por objetivo principal identificar, medir, controlar, gestionar e informar sobre los riesgos a los

que está o pudiera estar expuesto el Grupo, incluido el riesgo de ciberseguridad, y en particular, el riesgo operacional entendido éste como el riesgo de pérdida derivado de la inadecuación o de la disfunción de procesos internos, del personal, de los sistemas, o de sucesos externos. El referido sistema tiene como elementos principales el gobierno del riesgo, el proceso de gestión de riesgos y la estrategia de negocio, alineada con la estrategia de riesgos, al objeto de cumplir con el apetito y la tolerancia al riesgo definido por el Consejo de Administración del Grupo, fomentando así una cultura común de los riesgos dentro del Grupo y asegurando la eficiencia del sistema de control de gestión de riesgos.

Adicionalmente a las labores de supervisión y control, GCO se somete regularmente a auditorías; de carácter interno, a través de la función fundamental de auditoría interna de Grupo, configurada como tercera línea de defensa y con la misión de mejorar y proteger el valor de las entidades que conforman el Grupo, proporcionándoles aseguramiento objetivo, asesoría y conocimiento basado en riesgos; y de carácter externo, a través del sometimiento voluntario a auditorías externas por parte de consultores de reconocido prestigio; que supervisan, controlan y evalúan periódicamente la eficacia y eficiencia de los sistemas de control interno y de gestión del riesgo operacional, así como los procesos y procedimientos del Grupo sobre la protección de datos personales y la seguridad de la información.

Versión 4ª, aprobada en fecha 20 de septiembre de 2023, con fecha de efecto 1 de enero de 2024.

* * * * *