UCI

Política de Privacidad

Índice de contenidos

1. Introducción

El 25 de mayo de 2016 entró en vigor el Reglamento Europeo de Protección de Datos (RGPD o GDPR – Reglamento UE 2016/679 de 27 de abril de 2016), por el que se introducen nuevas disposiciones legales que abordan diferentes aspectos de privacidad y protección de datos dentro de un marco único aplicable dentro del Espacio Económico Europeo. Este nuevo Reglamento deroga la Directiva 95/46/CE y es obligatorio en todos sus elementos, y directamente aplicable en cada Estado miembro a partir del 25 de mayo de 2018.

Con posterioridad en diciembre de 2018 se aprobó la Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD): Ley Orgánica 3/2018, de 5 de diciembre, aprobada por las Cortes Generales de España, y que tiene por objeto adaptar el Derecho interno español al Reglamento General de Protección de Datos. Esta ley orgánica deroga a la anterior Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal, y entró en vigor el 7 de diciembre de 2018.

La privacidad y protección de datos tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de datos personales, las libertades públicas y derechos fundamentales de las personas físicas, especialmente a su honor, intimidad y privacidad personal y familiar. Su objetivo es regular el tratamiento de los datos personales, independientemente del soporte en el cual sean tratados, los derechos de los interesados sobre ellos y las obligaciones de aquellos que los crean o tratan.

La adopción de los nuevos requisitos del reglamento y su total cumplimiento por parte de todas las organizaciones es un objetivo clave, para lo cual estas están obligadas a implementar cambios técnicos y organizativos que garanticen la seguridad de los datos personales y reconozcan su protección como derecho fundamental.

2. Objeto

La presente política tiene como objetivo establecer el compromiso del Grupo UCI (en adelante la Compañía), con respecto a la privacidad y protección de datos de carácter personal, de acuerdo con la legislación aplicable de GDPR y LOPDGDD, permitiendo así, la consecución de sus objetivos definidos.

El alcance del presente documento es cubrir los requerimientos sobre privacidad y protección de datos de carácter personal con respecto al GDPR y LOPDGDD, en la Compañía, entendida como entidad jurídica independiente, así como a cualquier empresa perteneciente al Grupo o a empresas que prestan servicios a las anteriores.

La Compañía, a través de esta Política Global de Privacidad, establece un marco único de definición de la privacidad y la protección de datos de carácter personal, donde se compromete a proteger y tratar todos sus datos personales garantizando siempre el cumplimiento de las distintas normativas y leyes aplicables en esta materia.

3. Ámbito de aplicación

El cumplimiento de la presente política es responsabilidad de todo el personal de la Compañía, así como del personal externo al mismo incluido en el ámbito de aplicación. Por tanto, la Dirección de la Compañía espera que todo el personal, tanto interno como externo, esté familiarizado y comprometido con la misma.

4. Definiciones

RGPD o GDPR: Reglamento General de Protección de Datos (General Data Protection Regulation).

LOPDGDD: Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales.

DPO o DPD: Data Protection Officer (Delegado de Protección de Datos).

PIA o EIPD: Privacy Impact Assesment o Evaluación del Impacto en Protección de datos.

Datos personales: Toda información sobre una persona física identificada o identificable («el interesado»); Se considerará persona física identificable a 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.

Tratamiento: Cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción.

Responsable del tratamiento o Responsable: 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 del tratamiento o Encargado: 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.

Consentimiento del interesado: Toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen.

Elaboración de perfiles: Toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física.

Datos biométricos: Datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos.

Datos relativos a la salud: Datos personales relativos a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud.

Tratamiento transfronterizo: El tratamiento de datos personales realizado en el contexto de las actividades de establecimientos en más de un Estado miembro de un Responsable o un Encargado del tratamiento en la Unión, si el Responsable o el Encargado está establecido en más de un Estado miembro; o cuando el tratamiento de datos personales realizado en el contexto de las actividades de un único establecimiento de un Responsable o un Encargado del tratamiento en la Unión, pero que afecta sustancialmente o es probable que afecte sustancialmente a interesados en más de un Estado miembro.

Autoridad de Control: la autoridad pública independiente establecida por un Estado miembro con arreglo a lo dispuesto en el artículo 51 del RGPD:

- En España, la Agencia Española de Protección de Datos, en adelante AEPD.
- En Portugal, la Comissão Nacional de Protecção de Dados, en adelante CNPD.
- En Grecia, la Hellenic Data Protection Authority, en adelante HDPA.

5. Referencias

- Reglamento General de Protección de Datos (GDPR/RGPD): Reglamento (UE) 2016/679 del 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. Este nuevo Reglamento deroga la Directiva 95/46/CE y es obligatorio en todos sus elementos, y directamente aplicable en cada Estado miembro a partir del 25 de mayo de 2018.

- Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD): Ley Orgánica 3/2018, de 5 de diciembre, aprobada por las Cortes Generales de España, y que tiene por objeto adaptar el Derecho interno español al Reglamento General de Protección de Datos. Esta ley orgánica deroga a la anterior Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal, y entró en vigor el 7 de diciembre de 2018.
- ISO 9001:2015, comercialización y gestíón de préstamos hipotecarios y personales.
- ISO 27001:2022 para la gestión de clientes en posventa.

6. Política de Privacidad

6.1. Datos de Carácter Personal

Un “dato de carácter personal” es cualquier información referente a personas físicas identificadas o identificables, pudiendo ser identificable toda persona cuya identidad pueda determinarse mediante un identificador (nombre, número de identificación, datos de localización o identificador en línea) o mediante el uso de elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de las personas.

Dependiendo del tipo de datos que se traten, estos pueden ser: identificativos (nombre, apellidos, número de pasaporte) o referidos a la situación laboral, financiera o de salud. También existen las denominados categorías especiales de datos, en los que además de los datos de salud, se encuentran aquellos que hagan referencia a ideología, religión, origen racial, vida sexual, y comisión de infracciones penales y administrativas.

6.2. Partes Involucradas

La Compañía debe garantizar la seguridad e integridad de todos los datos personales que son de su responsabilidad y que tratan directamente (responsable del tratamiento), mediante la provisión de servicios por parte de terceros (tercero como encargado del tratamiento) o como proveedor de servicios a otra empresa (Grupo UCI como encargado del tratamiento).

En todos estos casos, independientemente de si se actúa como responsable o encargado, los datos persones deben ser controlados y su tratamiento debe cumplir con las obligaciones y garantías legales y contractuales exigidas.

A. Responsable del Tratamiento

La Compañía, como responsable del tratamiento, decidirá sobre el propósito, contenido y uso de los tratamientos de datos personales con respecto a clientes, empleados y otros interesados. Por tanto, en la realización de estas actividades se debe cumplir las siguientes instrucciones:

- Asegurar que los datos sean adecuados y precisos, legítimamente obtenidos y tratados acordes al propósito para el que fueron recogidos.

- Garantizar el cumplimiento de la confidencialidad relativa al tratamiento de datos personales.

- Informar a los interesados de la obtención de su consentimiento así como de los fines del tratamiento.

- Facilitar y garantizar que los interesados puedan ejercer sus derechos.

- Aplicar medidas técnicas y organizativas para garantizar un tratamiento justo y legal, llevar a cabo evaluaciones de impacto sobre la privacidad y mantener un registro de actividades de tratamiento.

- Notificar a la autoridad de control aquellas brechas de seguridad, con impacto en datos personales, cuyo nivel de riesgo supere el umbral establecido por política.

- Garantizar que se respeten las normas de protección de datos en sus relaciones con proveedores de servicios que acceden a datos personales de su responsabilidad.

B. Encargado del Tratamiento

La Compañía tiene acuerdos de servicios con proveedores externos, los cuales pueden tener acceso a datos personales. Estos proveedores deben procesar los datos como encargados del tratamiento en nombre de la Compañía, que es el responsable del tratamiento.

De igual forma, la Compañía puede actuar como encargado del tratamiento en la provisión de servicios a otra entidad que actúa como responsable de tratamiento.

En ambos casos, el encargado del tratamiento debe asegurar a su responsable el cumplimiento de sus obligaciones, ofreciendo garantías de un tratamiento acorde con las reglamentaciones correspondientes y de las salvaguardas pertinentes para los derechos de los interesados. La adhesión del encargado del tratamiento a un código de conducta o mecanismo de certificación aprobado puede usarse como elemento para demostrar su cumplimiento.

El tratamiento de datos por parte de un encargado de tratamiento debe estar regido por un contrato con el responsable del tratamiento, en el cual se establezcan los siguientes puntos:

- Garantizar la confidencialidad de los tratamientos.
- Implementar medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad de los datos, teniendo en cuenta las finalidades del tratamiento y los riesgos.
- Autorización previa del responsable antes de contratar a otro encargado y garantizar que se cumplen con las mismas condiciones para el tratamiento de datos personales.

- Permitir y cooperar en todas las auditorías e inspecciones realizadas por el responsable.
- Asistir al responsable en la respuesta del ejercicio de derechos de los interesados y a garantizar el cumplimiento de las obligaciones relacionadas con las medidas de seguridad y las evaluaciones de impacto de privacidad.
- Suprimir o devolver los datos personales al responsable al finalizar los servicios, y eliminar las copias existentes.

C. Autoridad de Control

La Compañía notificará directamente a la autoridad de control correspondiente en caso de cualquier infracción de protección de datos que pueda ocurrir o consultará antes de procesar ciertos datos personales.

Con respecto a la responsabilidad legal y contractual de los encargados, como en el caso de los responsables, cualquier incumplimiento de los mismos puede estar sujeto a sanciones emitidas por la autoridad de control hacia los propios responsables.

D. Delegado de Protección de Datos (DPO)

En el RGPD y en la LOPDGDD se establece la obligación de designar, en ciertos casos, un delegado de protección de datos (DPO) encargado de tareas, responsabilidades y deberes profesionales particulares.
En el RGPD se indica que las entidades deben designar un DPO en los siguientes casos:

- Cuando las actividades principales consisten en operaciones de tratamiento que, en virtud de su naturaleza, su alcance y/o sus finalidades, requieren una supervisión regular y sistemática de los sujetos de datos a gran escala.
- Cuando las actividades secundarias consisten en procesar a gran escala categorías especiales de datos.

La Compañía, por tanto, ha optado por la designación de un único DPO global integrado internamente y ubicado dentro de la Unión Europea, y por la designación de unos representantes divididos por países que reportarán directamente al DPO global. A continuación, se exponen los datos de contacto del DPO global:

Delegado de Protección de Datos – Oficina del DPO

Correo electrónico: **dpo@uci.com**

6.3. Principios Fundamentales

La regulación de protección de datos aplicable afecta directamente a las operaciones de la Compañía, ya que los datos personales se procesan en su actividad diaria. Al procesar estos datos, se deben cumplir una serie de principios y medidas:

A. Legalidad, proporcionalidad y transparencia:

La Compañía debe procesar los datos de acuerdo con los siguientes principios:

- Legalidad: los datos deben obtenerse lícitamente y conforme a los reglamentos y leyes aplicables.

- Proporcionalidad: los datos sólo se deben procesar para fines necesarios, apropiados y pertinentes.

- Transparencia: la información debe ser clara, exacta y no ambigua.

B. Finalidades compatibles con la recogida inicial:

La Compañía debe garantizar que los datos personales se procesen sólo para los fines específicos, explícitos y legítimos para los que se recopilaron.

En los casos donde los datos se procesen para otros fines posteriores a los iniciales, salvo con el debido consentimiento del interesado, sólo se permiten cuando son compatibles con los propósitos iniciales.

C. Minimización y exactitud de los datos personales:

Los datos personales deben ser adecuados, relevantes y estar limitados a los fines para los que se procesan. Además, se deben tomar todas las medidas razonables para garantizar que, si son inexactos, teniendo en cuenta los fines para los que se procesan, se borren o rectifiquen.

D. Almacenamiento de los datos personales:

La Compañía debe almacenar los datos personales permitiendo la identificación de los interesados por un período no superior al necesario para los fines para los que se procesan.

No obstante, pueden almacenarse por períodos más largos, siempre que se procesen únicamente con fines de archivo de interés público, de investigación científica o histórica o con fines estadísticos, sujeto a la implementación de medidas técnicas y organizativas apropiadas.

E. Integridad, confidencialidad y disponibilidad de los datos personales:

La Compañía debe asegurar que los datos recopilados se procesan garantizando una adecuada seguridad (protección contra tratamientos no autorizados o ilegales, y contra la pérdida, destrucción o daño accidental) y utilizando medidas técnicas u organizativas (cifrado o pseudonimización). Con este fin, se debe garantizar un nivel de seguridad

apropiado para el riesgo, así como la confidencialidad, integridad, disponibilidad de los sistemas y servicios.

En particular, la Compañía debe garantizar que sus empleados, los terceros que prestan servicios y los empleados de dichos terceros que, en el desempeño de sus funciones, tengan acceso a datos personales, se comprometan a tratar estos datos como confidenciales y a abstenerse de divulgarlos a otras partes.

F. Protección de los datos desde el diseño y por defecto:

La Compañía debe aplicar medidas para salvaguardar y demostrar el cumplimiento de los requisitos legales de protección de datos, mediante la definición de políticas adecuadas, adaptadas a las circunstancias particulares de la organización y que estén completamente implementadas y funcionen adecuadamente en la práctica. En este sentido, un aspecto clave a implementar es la protección de datos desde el diseño y por defecto:

- **Privacidad desde el diseño:** Cuando se diseña un producto o servicio, la Compañía debe tener en cuenta desde su inicio cuestiones tales como requisitos de información u obtención de consentimiento apropiado para procesar los datos personales de los clientes.

- **Privacidad por defecto:** De forma predeterminada, sólo deben procesarse los datos personales necesarios para alcanzar el objetivo legal perseguido, garantizando siempre la confidencialidad y seguridad de los datos personales.

6.4. Responsabilidad de los Datos y Tratamientos

La Compañía, como responsable del tratamiento, debe adoptar políticas y procedimientos apropiados, así como implementar medidas técnicas y organizativas adecuadas y verificables, que permitan garantizar y evidenciar que los datos personales se procesan de acuerdo con la regulación aplicable. Este marco regulatorio aborda las siguientes medidas principales a aplicar:

- Designación de un DPO.
- Requisitos del deber de información y recopilación de consentimiento.
- Registro de actividades de tratamiento.
- Protección de datos por diseño y por defecto, y evaluaciones de impacto de privacidad.
- Medidas de seguridad y mecanismos de notificación de brechas de seguridad.

6.5. Deber de Información

Antes de recopilar cualquier tipo de datos de carácter personal, se debe informar a los interesados de una manera simple, clara y fácil de entender, sobre los diferentes aspectos relacionados con sus datos personales y los tratamientos.

De igual forma, cuando los datos personales se obtienen a través de terceros, también se debe informar a los interesados.

6.6. Legitimidad del Tratamiento

Los aspectos a tener en cuenta para garantizar que el tratamiento sea legal, según establece el art. 6.1. del RGPD son:

a) Consentimiento del interesado para uno o varios fines específicos;

b) el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de éste de medidas precontractuales;

c) el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento;

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

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

f) el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un menor.

6.7. Derechos de los Interesados

La Compañía debe informar a todas las personas de las que se recopilan datos personales sobre los riesgos, salvaguardas y derechos en relación con el tratamiento de datos personales. También se debe garantizar que los interesados puedan ejercer fielmente sus derechos, y que la Compañía responda diligentemente a las solicitudes de ejercicio de cualquiera de los derechos del interesado:

- **Derecho de acceso:** Los interesados tienen derecho a acceder a los datos personales que se han recopilado sobre ellos (ya sea en la propia Compañía o en sus proveedores), a fin de conocer y verificar la legalidad del tratamiento.

- **Derecho de rectificación:** Los interesados tienen derecho a la rectificación de cualquier dato personal inexacto o incompleto que les concierna (ya sea en la propia Compañía o en sus proveedores), a fin de garantizar su exactitud y el tratamiento adecuado.

- **Derecho de supresión (o derecho al "olvido"):** Los interesados tienen derecho a la supresión de los datos personales que les conciernan.

- **Derecho de oposición:** Los interesados tienen derecho a oponerse en todo momento al tratamiento de sus datos personales para un uso específico, si la Compañía los trata sobre la base de un interés legítimo, o para una actividad de interés público. La Compañía estará obligada a dejar de tratar los datos personales del interesado, salvo que acredite motivos legítimos imperiosos para el tratamiento que prevalezcan sobre los intereses, los derechos y las libertades del interesado, o para la formulación, el ejercicio o la defensa de reclamaciones. Aparte, cuando el tratamiento de datos personales tenga por objeto la mercadotecnia directa, el interesado tendrá derecho a oponerse en todo momento al tratamiento de los datos personales que le conciernan, incluida la elaboración de perfiles en la medida en que dicho perfilado esté relacionado con la mencionada mercadotecnia. En este caso, los datos personales deberán dejar de ser tratados para dichos fines de manera inmediata.

- **Derecho de limitación:** Los interesados tienen derecho a la limitación del tratamiento de sus datos personales mientras se determina si el interés legítimo de la Compañía prevalece sobre su interés individual. No obstante, en caso de fines comerciales directos, la Compañía siempre tiene la obligación de dejar de tratar los datos personales si lo solicita el interesado.

- **Derecho a la portabilidad:** Los interesados tienen derecho a recibir los datos personales que les conciernan, y a que dichos datos sean transmitidos a otro responsable, en un formato estructurado, de uso común y legible automáticamente.

- **Derecho a no ser objeto de decisiones individuales automatizadas:** Los interesados tienen derecho a no ser objeto de decisiones automatizadas que produzcan sobre ellos efectos jurídicos, o les afecte significativamente de forma similar. Esto también incluye aquellos tratamientos en los que la Compañía utiliza cookies como una herramienta técnica para evaluar clientes y predecir su comportamiento, desempeño o preferencias, comparando su perfil con el de usuarios o clientes similares.

6.8. Registro de Actividades de Tratamiento

La Compañía debe mantener un Registro de las Actividades de Tratamiento (RAT) llevadas a cabo bajo su responsabilidad. La obligación de mantener dicho registro recae tanto en el

responsable como en el encargado del tratamiento, aunque la información que debe mantenerse en los registros del responsable difiere de la requerida para el encargado.

El tratamiento de datos personales se entiende como cualquier procedimiento u operación técnica, automatizada o no, que permita la recopilación, registro, conservación, preparación, modificación, consulta, uso, cancelación, bloqueo o eliminación de datos, así como las transferencias de datos procedentes de comunicaciones, consultas, combinación y transferencias de datos que identifiquen o puedan señalar directa o indirectamente a una persona física.

6.9. Evaluación de Impacto en la Privacidad (PIA o EIPD)

El tratamiento de datos personales está expuesto a riesgos durante todo su ciclo de vida. Estos riesgos deben ser gestionados y reducidos, en la medida de lo posible, a un nivel razonable.

El GDPR introduce el concepto de Evaluación de Impacto en la Privacidad (EIPD o PIA) como una nueva herramienta de análisis de riesgos destinada a salvaguardar los datos personales. Por tanto, se establecen las bases para los requisitos relacionados, los casos en los que se debe llevar a cabo una EIPD, la información que se expondrá, la participación del DPO y otros aspectos relacionados. Sin embargo, debido a la naturaleza subjetiva de la necesidad de realizar una EIPD, se debe contar con una metodología para garantizar un enfoque más objetivo, estableciendo los pasos mínimos y los requisitos de información que deben tener. El GDPR prevé tres casos en los que debe realizarse una EIPD:

a. Evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se basen en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas físicas o que les afecten significativamente de modo similar.

b. Tratamiento a gran escala de las categorías especiales de datos, o de datos personales relativos a condenas e infracciones penales.

c. Monitorización/Observación sistemática a gran escala de una zona de acceso público.

Sin embargo, la preparación de una EIPD no puede limitarse sólo a estos tres casos, por lo que se deben definir los criterios utilizados para determinar su realización. Además, la autoridad de control competente establecerá y hará pública una lista del tipo de operaciones de tratamiento que están sujetas al requisito de una evaluación de impacto de privacidad y, opcionalmente, establecerá y hará pública una lista del tipo de operaciones de tratamiento para las cuales no será necesario realizar una evaluación de impacto.

La AEPD ha publicado ambas listas en su Web, y pueden ser consultadas en los dos siguientes enlaces:

1. Listas de tratamientos de datos que requieren EIPD (no es exhaustiva)

2. Lista orientativa de tratamientos de datos que no requieren EIPD

6.10. Notificaciones de Incidentes de Seguridad

En caso de violación de la seguridad de los datos personales, el responsable del tratamiento realizará una notificación a la autoridad de control competente sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, a menos que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas. Si la notificación a la autoridad de control no tiene lugar en el plazo de 72 horas, deberá ir acompañada de indicación de los motivos de la dilación.

Como norma general, en el Grupo UCI, se notificarán a la autoridad de control competente aquellas violaciones de seguridad que superen el umbral de nivel de riesgo establecido en la política interna de gestión de brechas de seguridad.

En cualquier caso, siempre que se supere dicho umbral, se convocará de manera inmediata al Comité de Evaluación de Brechas de Seguridad, que es el órgano interno que analiza toda la información recopilada, y es quien decide en última instancia si se realiza la comunicación del incidente a la autoridad de control competente, y/o a los interesados, además de solicitar medidas urgentes de seguridad, adicionales a las ya establecidas, para prevenir que se reproduzca el incidente de seguridad.
Si el tratamiento lo lleva a cabo un proveedor, el encargado debe notificar al responsable de cualquier violación de datos personales del que tenga conocimiento. Posteriormente, el responsable debe notificar a la autoridad de control, como lo haría con cualquier otra violación de datos personales.

En el caso de violaciones de datos personales que impliquen un alto riesgo, los interesados también deben ser notificados del incumplimiento.

6.11. Cuerpo Normativo de Privacidad

Como parte de esta política se ha generado documentación que hace referencia a políticas y procedimientos que aplican a las distintas áreas de la privacidad y protección de datos personales. Dicha documentación será distribuida por los canales adecuados dentro de la Compañía, y en base a la necesidad del conocimiento, a todas las partes interesadas.

El presente documento está a disposición de todos los colaboradores en la aplicación corporativa de gestión documental.

6.12. Sanciones

El incumplimiento de las obligaciones de protección de datos puede dar lugar a multas administrativas que oscilan entre 10 y 20 millones de euros, o de una cuantía equivalente al

2% y 4% del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía.

Las multas previstas en el GDPR afectan a toda la Compañía en su conjunto y no se asignan a una filial o país específico. En consecuencia, el pleno cumplimiento de este marco de protección de datos es fundamental, ya que representa los requisitos mínimos de protección de datos que la Compañía debe cumplir al tratar datos de carácter personal.

6.13. Cumplimiento Legal y Estatutario

La presente política establece las necesidades de cumplir con todos aquellos requerimientos legislativos, normativos y contractuales, que le sean de aplicación a la Compañía. En este sentido, la Dirección de la Compañía se compromete a dotar de los recursos necesarios para dar cumplimiento a toda la legislación y regulación aplicable a la actividad de la Compañía y a establecer la responsabilidad de dicho cumplimiento sobre todos sus miembros.

6.14. Concienciación y Formación

Todos los empleados de la Compañía con responsabilidades en materia de privacidad y protección de datos personales deberán disponer de la formación adecuada para el desempeño de sus funciones. Asimismo, deberá asegurarse la adecuada concienciación de todos los miembros de la Compañía en términos de privacidad y buenas prácticas.

Los empleados de la Compañía deberán disponer de acceso y conocimiento de las actualizaciones regulares de la presente política y del resto del cuerpo normativo.

6.15. Gobierno y Facultades

La elaboración de esta política ha sido llevada a cabo por la Dirección de Riesgos y presentada ante la Dirección General para su aprobación y propuesta al Consejo de Administración de Unión de Créditos Inmobiliarios, S.A., Establecimiento Financiero de Crédito.

Las modificaciones de esta política serán sometidas a la aprobación del Consejo de Administración cuando sufran cambios significativos y en cualquier caso cada tres años como máximo. Los cambios menos significativos serán igualmente informados al Consejo en el momento en el que se produzcan y tras haber sido informado previamente el órgano delegado correspondiente, normalmente el Comité de Auditoría y Riesgos del Consejo.

Está política será revisada siempre que concurra cualquier circunstancia que así lo exija, como, por ejemplo, cambios normativos, directrices del regulador, cambios en la estructura de Gobernanza o cambios en el negocio.

La interpretación de las políticas corresponderá a la función relevante, encargada de su aplicación operativa.

Las políticas entrarán en vigor desde la fecha de publicación. Los contenidos de las políticas quedan sujetos a revisiones periódicas, introduciendo los cambios y modificaciones que se consideren convenientes, siguiendo el proceso de revisión contenido en este documento.

7. Registros

Se deberán tener en cuenta los siguientes **documentos corporativos**:

- **Gobierno de Privacidad y DPO:** El objeto es establecer el modelo de gobierno sobre el que se realiza la gestión de protección de datos y privacidad y definir las relaciones y canales de comunicación entre todos los involucrados en las actividades de protección de datos y su relación con el DPO.

- **Política de Plazos de conservación de datos:** Identifica el plazo de conservación de los datos de los distintos stakeholders de la Entidad, teniendo en cuenta las obligaciones derivadas de la relación mantenida con cada uno de ellos, así como las obligaciones legales y la necesidad de conservación ante posibles acciones judiciales.

- **Política de supresión de datos cedidos por terceros**: Define las obligaciones que estipula el RGPD, establece el marco regulatorio y proporciona información sobre protección de datos y la supresión o mantenimiento de éstos.

- **Procedimiento de Evaluación de Impacto en Privacidad (EIPD o PIA):** Desarrolla los pasos a llevar a cabo para determinar la necesidad de realización y la elaboración de una Evaluación del Impacto en Privacidad o PIA.

- **Procedimiento de Modelo de Reporting**: Define el modelo y las necesidades de reporting, así como los elementos de coordinación entre las principales figuras que gobiernan el cumplimiento de la normativa de protección de datos en el Grupo UCI.

- **Procedimiento de Transferencias Internacionales de dato**s: Desarrolla los pasos a llevar a cabo para la detección y realización de transferencias internacionales, partiendo de la identificación del tratamiento.