CÓDIGO DE CONDUCTA PARA EL TRATAMIENTO DE DATOS PERSONALES EN GERMANIA AUTOMOTRIZ S.A.C.

TÍTULO I: DISPOSICIONES GENERALES

Artículo 1. Objeto

El presente Código de Conducta tiene por objeto garantizar un adecuado tratamiento de datos personales de personas naturales en un marco de respeto de las normativas de protección de datos personales, en especial lo establecido en la Ley N° 29733 Ley de Protección de Datos Personales, su Reglamento y normas complementarias.

Los asociados, colaboradores y terceros que actúen por mandato de la empresa GERMANIA S.A.C., en adelante GERMANIA, deben actuar bajo los mandatos y teniendo en cuenta las recomendaciones establecidas en el Código de Conducta a fin de establecer un ambiente colaborador con el cumplimiento de las exigencias legales y brindar un mejor trato a los datos personales que se procesa en GERMANIA o por mandato de GERMANIA.

Artículo 2. Ámbito de aplicación

a) El presente código de conducta será de aplicación al tratamiento de los datos personales que se sean recolectados, tratados, transferidos y aun a los que solo están almacenados con fines de tránsito, lo cuales se encuentran bancos de datos personales de los cuales GERMANIA es titular y/o encargados del banco de datos personales o responsable del tratamiento, asimismo a los datos personales que sean destinados a ser incorporados en estos bancos de datos personales.

Los bancos de datos personales inscritos en el Registro Nacional de Protección de Datos Personales y también sometidos a este código de conducta pueden ser consultados públicamente en: http://www.minjus.gob.pe/registro-proteccion-datos-personales/

b) La aplicación de este Código de Conducta será para la información detallada en el numeral anterior sin importar el soporte (físico, automatizado, virtual, entre otros.) en el que se encuentre.

c) El presente código es una política de privacidad de GERMANIA por lo que debe ser difundida y puesta en práctica de manera obligatoria por todos los colaboradores de la empresa y por terceros cuya relación con la empresa les permita tener acceso a información en cualquier medio de soporte o a servicios de tecnología de la información.

Artículo 3. Definiciones

a) A los efectos del presente código de conducta se entenderá por:

- Titular del dato personal: persona natural del cual concierne el dato personal, puede ser un cliente, colaborador, usuario, visitantes, un tercero que tenga o no alguna relación contractual y/o profesional, y cuyos datos personales se encuentre o vayan a ser destinados en algún banco de datos personales del cual GERMANIA sea titular o encargado.

- Dato Personal: Toda información que identifica o hace identificable a una persona natural a través de medios que puedan ser razonablemente utilizados.

Esta información puede ser: numérica, alfabética, gráfica, fotográfica, acústica, sobre hábitos personales, o de cualquier otro tipo concerniente a las personas naturales.

- Dato Sensible: Aquellos datos personales constituidos por datos biométricos que por sí mismos pueden identificar al titular, datos referidos al origen racial y étnico, ingresos económicos, opiniones o convicciones políticas, religiosas, filosóficas o morales, afiliación sindical, características físicas, morales o emocionales, hechos o circunstancias de la vida afectiva o familiar del titular del datos, hábitos personales que corresponden a la esfera más íntima, información relativa a la salud física o mental u otras análogas que afecten la intimidad. Toda medida que se adopte respecto al tratamiento de datos personales debe considerar además un acápite especial y de especial protección a los considerados como datos sensibles.

- Tratamiento de datos personales: Cualquier operación o procedimiento técnico, automatizado o no, que permite la recopilación, registro, organización, almacenamiento, conservación, elaboración, modificación, extracción, consulta, utilización, bloqueo, impresión, supresión, comunicación por transferencia o por difusión o cualquier otra forma de procesamiento que facilite el acceso, correlación o interconexión de los datos personales.

- Cesión o comunicación de datos personales: Tratamiento de los datos que supone su revelación a una persona distinta del interesado, titular del dato, que será considerado de manera interna entre los operadores del GERMANIA o terceros a los cuales la empresa comunique sea como encargados del banco de datos o encargados del tratamiento.

- Transferencia de datos personales: Cesión o comunicación de datos personales gratuita u onerosa que se realice a personas o entidades distintas a GERMANIA y que no sean encargados del banco de datos o encargados del tratamiento.

- Banco de datos personales: Todo conjunto organizado de datos de carácter personal.

- Transferencia internacional de datos: Tratamiento de datos que supone una transmisión de los mismos fuera del territorio peruano, bien constituya una cesión o comunicación de datos o una transferencia.

- Autoridad Nacional de Protección de Datos Personales: ANPDP – Entidad encargada del cumplimiento de la Ley N° 29733, su norma reglamentaria y demás normas complementarias.

- Categorización de Banco de Datos: Tipificación establecida para los bancos de datos considerando su finalidad, número de registros, tipos de datos personales, etc., a fin de implementar medidas de seguridad establecidas en la Resolución Directoral Nº 019-2013-JUS/DGPDP que aprueba la “Directiva de Seguridad de la Información Administrada por los Bancos de Datos Personales”, en adelante, Directiva de Seguridad de la Información.

Básico

No contenga información de más de 50 personas Número de datos personales no mayor a 5 No incluyen datos sensibles Tienen como titular a una persona natural

Simple

No contenga información de más de 100 personas. El periodo o tiempo de tratamiento para cumplir la finalidad es inferior a 1 año. Número de datos personales no mayor a 5. No incluyen datos sensibles. Tienen como titular a una persona natural.

Intermedio

No contenga información de más de 1000 personas. El periodo o tiempo de tratamiento para cumplir la finalidad es indeterminado o superior a 1 año. Número de datos personales no mayor a 5. Incluye datos sensibles. Tienen como titular a una persona natural o jurídica.

Complejo

Sirven para el tratamiento de datos personales cuya finalidad se cumple en un plazo indeterminado o superior a un año. Sirven para el tratamiento de datos personales que es realizado en múltiples locaciones (Oficinas, dependencias, ciudades diferentes, servicios tercerizados o similares). Pueden incluir datos sensibles Tiene como titular a una persona jurídica o entidad pública.

Crítico

Sirven para el tratamiento de datos personales cuya finalidad está respaldada por una norma legal. Sirven para el tratamiento de datos cuya finalidad se cumple en un plazo indeterminado o superior a un año. Sirven para el tratamiento de datos personales que es realizado en múltiples locaciones. Puede incluir datos sensibles. Tiene como Titular a una persona jurídica o entidad pública.

b) En particular, se deberá observar de manera prioritaria las definiciones expuestas en el artículo 2 de la Ley N° 29733 y en el artículo 2 del Reglamento de la Ley N° 29733.

TÍTULO II: DE LA ORGANIZACIÓN PARA EL TRATAMIENTO DE DATOS PERSONALES.

Artículo 4. De la administración y responsables

a) Se debe desarrollar en cada gerencia una estructura organizativa con roles y responsabilidades con el objetivo de asegurar la protección de los datos personales, con un coordinador responsable que pueda trasladar y hacer seguimiento de las consultas de protección de datos personales que se realice al área legal.

b) El titular de los Bancos de Datos es GERMANIA como persona Jurídica.

c) El representante legal de la empresa encargado de las inscripciones de los Bancos de Datos de GERMANIA ante el Registro Nacional de Protección de Datos Personales es la Jefatura de Administración4 o quien designe considerando la representación requerida por la Ley 29733 y sus normas complementarias.

d) Los bancos de datos personales deben tener un responsable de negocio asignado denominado “responsable del tratamiento del banco”, el cual es responsable de supervisar el cumplimiento de las medidas establecidas en el código de conducta en los bancos de datos personales de la empresa y los establecidos en la Ley 29733 y sus normas complementarias.

e) Los bancos de datos personales deben tener definido un custodio que implemente las medidas de seguridad establecidas en la Ley 29733 y sus normas complementarias, el cual coordinará con el Oficial de Seguridad de la Información.

f) El Jefe de Sistemas será el responsable de la seguridad de los bancos de datos personales de la empresa y tiene como función coordinar las medidas necesarias para asegurar su disponibilidad, confidencialidad e integridad de acuerdo a la legislación vigente para este fin, en especial lo regulado en la Directiva de Seguridad.

TÍTULO III: CUMPLIMIENTO DE LOS PRINCIPIOS DE PROTECCIÓN DE LOS DATOS PERSONALES

Artículo 5. Principio de legalidad

a) Todos los datos personales tratados en GERMANIA deben ser tratados conforme a lo dispuesto en la Ley 29733 Ley de Protección de datos personales, su norma reglamentaria y demás normas complementarias, y el presente código de conducta.

b) No se deben recopilar datos personales mediante la realización de fraudes, engaños y de medios no permitidos por la legislación peruana.

Artículo 6. Principio de consentimiento

a) Sólo se deben tratar datos personales cuyos titulares hayan brindado previamente su consentimiento o que la Ley permita su tratamiento sin necesidad del consentimiento del titular del dato.

b) El consentimiento del titular del dato personal debe ser previo a la captación, libre, informado, inequívoco y expreso respecto de la finalidad del tratamiento informado por GERMANIA. Asimismo, deberá cumplir con los requerimientos establecidos en la Ley 29733 y sus normas complementarias definidas para este fin.

c) El tratamiento de datos personales sensibles debe requerir el consentimiento expreso, por escrito o firma digital u otro mecanismo que permita la autenticación de la identidad del titular del dato personal.

d) No será preciso el consentimiento cuando los datos de carácter personal cuando:

- Se recojan para el ejercicio de las funciones propias de GERMANIA en el ámbito de sus competencias sea en el ámbito contractual, precontractual, laboral, negociación y profesional, o cuando los datos figuren en fuentes de acceso público, o cuando exista excepciones establecidas por Ley 29733 y sus normas complementarias.

- Cuando se realicen actividades de disociación o anonimización.

e) En caso de obtener datos personales sin el previo consentimiento del titular del dato y no exista excepción para su solicitud, estos no deben ser tratados hasta la subsanación del requisito de consentimiento para tratarlos.

f) Para efectos de demostrar la obtención del consentimiento en los términos establecidos en la Ley 29733 y sus normas complementarias, se debe mantener la carga de la prueba para cada uno los datos personales involucrados en el tratamiento, pruebas que deberán ser resguardadas en ambientes seguros.

Artículo 7. Principio de finalidad del tratamiento

a) Los datos personales deben ser tratados de manera adecuada (apropiada), pertinente y no excesivo según los fines para los cuales el titular del dato personal o la Ley 29733 y sus normas complementarias autorizan.

b) Los datos personales deben ser tratados para fines lícitos y de manera leal.

c) Los datos serán eliminados cuando hayan dejado de ser necesarios o pertinentes a los fines para los cuales hubieren sido recolectados, no exista un mandato legal para su conservación o exigencia contractual de la cual es parte GERMANIA.

d) No se necesitará consentimiento del titular del dato personal fines históricos, estadísticos o científicos.

Artículo 8. Principio de proporcionalidad

Los datos personales que se soliciten deber los necesarios y debidamente justificados para el cumplimiento de los fines de tratamiento, es decir, deben ser adecuados, relevantes y no excesivos a a la finalidad para lo que fueron recopilados.

Artículo 9. Principio de Calidad de los datos

Los datos de carácter personal deben ser exactos y puestos al día de forma que respondan con veracidad a la situación actual del afectado. Se debe presumir que los datos directamente facilitados por el titular de los mismos son exactos. Si los datos de carácter personal registrados resultaran ser inexactos, en todo o en parte, o incompletos, serán sustituidos por los datos rectificados, o completados los mismos, desde que se tuviese conocimiento de la inexactitud. En caso el titular del dato solicitara la actualización o rectificación de sus datos personales en atención de preservar la veracidad y exactitud de estos, las solicitudes deberán ser atendidas dentro de los plazos legales establecidos y según lo expuesto en el "Título V: Derechos de los Titulares de los Datos Personales" de este Código de Conducta.

Artículo 10. Principio de Seguridad de los datos

Se deben adoptar medidas de seguridad para evitar alteraciones, pérdidas, desvíos de información y accesos no autorizados a los bancos de datos personales. Para lo cual, se debe velar por el cumplimiento de las obligaciones establecidas en la Directiva de Seguridad de la información emitida por la Autoridad Nacional de Protección de Datos Personales.

Artículo 11. Principio de disposición del recurso

GERMANIA deberá establecer mecanismos para informar al titular de los datos personales de sobre la existencia de vías administrativas o legales para ejercer sus derechos reconocidos en la Ley 29733.

Artículo 12. Principio de nivel de protección adecuado

Las transferencias internacionales de datos personales realizados por GERMANIA deben ser formalizados mediante contrato, el cual defina las obligaciones legales para la protección de datos personales establecidos en la legislación peruana, además de otras recomendaciones adecuadas a la legislación nacional e internacional en caso aplique. Asimismo, cumplir con las inscripciones o notificaciones a realizarse ante la Autoridad Nacional de protección de datos personales.

TÍTULO IV: DEBERES DEL PERSONAL

Artículo 13. Tratamiento Inaceptable de la información referida a datos personales.

Las siguientes actividades están prohibidas y se consideran como un tratamiento inaceptable de la información referida a datos personales. La lista es un intento de proporcionar un marco para las actividades que caen en la categoría de uso inaceptable, pero no se limita a:

a) Tratar los datos personales sin el respectivo previo consentimiento del titular del dato personal.

b) Tratar la información para beneficio propio o de terceros.

c) Tratar la información de datos personales para realizar actividades contrarias a la legislación vigente.

d) Compartir, con otros colaboradores y/o terceros, de manera directa o indirecta la información de datos personales sin la autorización previa de los responsables de los bancos de datos y cumpliendo las políticas establecidas en el presente documento.

e) Comunicar, ceder o transferir directa o indirectamente información confidencial a terceros si la autorización debida de parte de GERMANIA.

Artículo 14. Deber de secreto y de confidencialidad

Todo colaborador y/o tercero que intervenga en cualquier fase del tratamiento de los datos personales está obligado a un deber de confidencialidad, de secreto y cuando corresponda del secreto profesional respectivo. Estas obligaciones subsistirán aun después de finalizar sus relaciones con GERMANIA.

Artículo 15. Gestión de Accesos a la Información de Datos Personales

Se debe cumplir la política de seguridad definida para la gestión de accesos a los sistemas informáticos y servicios de Tecnologías de la Información (ordenadores, celulares, aplicativos web o móvil, carpetas compartidas, entre otras) que soportan la gestión de los datos personales.

TÍTULO V: DERECHOS DE LOS TITULARES DE LOS DATOS PERSONALES

Artículo 16. Información al titular del dato personal

Los interesados a los que se soliciten datos personales deben ser previamente informados de manera expresa e inequívoca:

- De la identidad y dirección del responsable del tratamiento o del titular del banco de datos.

- De la finalidad de la recolección de los datos personales.

- De la identidad de los destinatarios de la información y sus fines de transferencia.

- De la facultad ejercitar los derechos de información, acceso, rectificación, actualización, inclusión supresión, oposición y tratamiento objetivo del dato.

- Del carácter obligatorio o facultativo de los dato personales demandados y las de las consecuencias de su cesión o de la negativa a suministrarlos.

- De la transferencia internacional de los datos de darse el caso o la probabilidad de ello e indicar si la transferencia es para fines distintos de las autorizaciones brindadas al recolector de los datos personales si fuera el caso.

Artículo 17. Derecho al tratamiento objetivo

No se debe someter al titular del dato personal a una decisión con efectos jurídicos sobre él o que le afecte de manera significativa, sustentada únicamente en un tratamiento de datos personales destinado a evaluar determinados aspectos de su personalidad o conducta.

Se podrá realizar la evaluación mencionada en el párrafo anterior solo en el marco de la negociación, celebración o ejecución de un contrato o en los casos de evaluación con

fines de incorporación a una entidad pública (cuando GERMANIA esté encargado de ello), de acuerdo a ley, sin perjuicio de la posibilidad de defender su punto de vista, para la salvaguardia de su interés legítimo.

Artículo 18. Derechos reconocidos al titular del dato

Se reconocen y respetan los derechos reconocidos en la Ley 29733, Ley de Protección de Datos Personales a todos los titulares del dato personal, con mayor atención a aquellos que le corresponde a GERMANIA atender de manera directa cuando el dato personal esté dentro de los bancos de datos de GERMANIA.

Los derechos que atiende directamente al titular del dato a través del Servicio de Atención al Cliente u otro canal que sea creado para la atención de estos:

a) Derecho de información del titular de datos personales

Brindar de forma detallada, sencilla, expresa, inequívoca y de manera previa a su recopilación las condiciones del tratamiento de los datos personales.

En caso de recolección en línea: Se puede realizar mediante la publicación de políticas de privacidad, las que deben ser fácilmente accesibles e identificables para los usuarios.

b) Derecho de acceso del titular de datos personales

Derecho del titular del dato a;

• Obtener la información de sí mismo que esté en posesión de GERMANIA.

• Obtener información sobre el titular del banco de datos (GERMANIA)

• Obtener información sobre el encargado del tratamiento de los datos personales.

• Obtener información sobre la forma de recolección.

• Conocer por qué y para quién se realizó la recopilación.

• Conocer las transferencias realizadas o que se realizarían de los datos personales.

c) Derecho de actualización, rectificación, inclusión, supresión o cancelación

El titular del dato lo puede ejercer cuando los datos sean:

• Parcial o totalmente inexactos, incompletos.

• Se advierta omisión, error o falsedad.

• Si ya no sean necesarios o pertinentes a la finalidad para la cual hayan sido recopilados.

• Cuando hubiera vencido el plazo establecido para su tratamiento.

d) Derecho a impedir el suministro

Implica el derecho a impedir que los datos personales sean suministrados a terceros, especialmente cuando ello afecte sus derechos fundamentales.

e) Derecho de oposición

El titular de datos personales puede oponerse al tratamiento de sus datos personales cuando existan motivos fundados y legítimos relativos a una concreta situación personal.

En caso de oposición justificada, GERMANIA debe proceder a su supresión, conforme a ley.

El derecho de oposición también puede ser usado aun cuando el titular del dato hubiera prestado su consentimiento, siempre y cuando los motivos se relacionen a una concreta situación que demuestre el uso justificado de este derecho.

Los tiempos de atención de estos derechos debe ser en los plazos legales establecidos en el Reglamento de la Ley de Protección de datos personales, presentados en el siguiente cuadro:

Información	08 días contados desde el día siguiente de la presentación de la solicitud
Acceso	20 días contados desde el día siguiente de la presentación de la solicitud Si la solicitud fuera estimada y no acompañase la información solicitada, el acceso será efectivo dentro de los 10 días siguientes a dicha respuesta.
Rectificación Cancelación Oposición Impedir el suministro Inclusión	10 días contados desde el día siguiente de la presentación de la solicitud

Asimismo, se debe atender al derecho al tratamiento objetivo del dato personal, previniendo a tiempo al titular del dato cuando se traten sus datos personales para realizar análisis cuyos resultados tengan efectos legales en el titular del dato personal.

Artículo 19. Atención de los derechos del titular del dato personal

a) Se debe diseñar e implementar procedimientos que permitan atender los requerimientos de los titulares de los datos respecto de sus derechos en conformidad con la Ley 29733 y sus normas complementarias.

Para ello se pueden crear canales de atención exclusivos para la atención de este tipo de solicitudes o encargarlo al área del negocio que trata la atención al cliente en caso de existir.

b) La atención de los derechos, por parte de los titulares de los datos personales, debe considerar los plazos legales establecidos en el Reglamento de la Ley 29733 y sus normas complementarias.

c) En caso de atención de los derechos de rectificación, supresión o cancelación, oposición, impedir el suministro e inclusión, si los datos personales reclamados hubieran sido transferidos previamente a otros, GERMANIA como titular del banco de datos personales o en caso de ser encargado de velar por la atención de estos derechos deberá comunicar la actualización, inclusión, rectificación y/o supresión a quien se haya transferido el dato personal.

d) Durante el proceso de atención de los derechos mencionados en el ítem anterior, GERMANIA dispondrá el bloqueo del dato personal reclamado, es decir, no permitirá que terceros accedan al dato personal.

e) El derecho de impedir el suministro no aplica para la relación entre el titular del banco de datos personales y el encargado del banco de datos personales para los efectos del tratamiento de los datos personales.

TÍTULO VI: GESTIÓN Y TRATAMIENTO DE LOS BANCOS DE DATOS PERSONALES

Artículo 20. Creación, actualización o supresión de bancos de datos

a) Se debe contar con la autorización del encargado de la gerencia para la creación, actualización, eliminación y transferencia de banco de datos personales que estará bajo la responsabilidad de su área, estos deben regirse con los principios rectores expresados en la Ley 29733 y de manera complementaria lo indicado en el "Título III: Cumplimiento De Los Principios De Protección De Los Datos Personales" de este Código de Conducta.

b) La creación de bancos de datos y/o mecanismos de captación de datos personales deben ser aprobado previamente por el Jefe de Sistemas.

c) Los bancos de datos deben ser registrados, actualizados y cancelados en el Registro Nacional de Protección Datos Personales cumpliendo lo dispuesto en la Ley 29733 y sus normas complementarias.

Artículo 21. Disposiciones para la creación y actualización de bancos de datos personales

Las disposiciones de creación o de modificación de los bancos de datos personales deberán indicar:

a) La identificación del banco de datos personales, indicando su denominación, así como a descripción de su finalidad, de los tipos de datos personales y usos previstos.

b) El origen de los datos, indicando el grupo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recolección de los datos y su procedencia.

c) El sistema de tratamiento utilizado en su organización.

d) La fecha de creación del banco de datos personales.

e) Las comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios.

f) Las transferencias nacionales y/o internacionales de datos previstos. En caso de transferencias internacionales además se deberá indicar el país o países destinos.

g) La indicación del responsable del banco de datos y del área donde se pueden ejercitar los derechos reconocidos al titular del dato.

h) Las medidas de seguridad con indicación del nivel de seguridad correspondiente previamente validado con los indicadores dispuestos en la Directiva de Seguridad.

i) Respecto a la supresión o eliminación de los bancos de datos personales se deberá establecer el destino que vaya a darse a los datos o, en su caso, las previsiones que se adopten para su destrucción.

j) El área legal de GERMANIA llevará a cabo las actuaciones procedimentales para la inscripción, modificación o cancelación de un banco de datos personales para su regularización en el Registro Nacional de Protección de Datos Personales.

Artículo 22. Consideraciones contractuales para servicios en la nube o cloud computing

Para los casos de almacenamiento o tratamiento de datos personales se realice por medios tecnológicos tercerizados se deben considerarse dentro de las prestaciones mínimas en el servicio de contratación:

1) Informar con transparencia las subcontrataciones que involucren la información sobre la que presta el servicio.

2) No incluir condiciones que autoricen o permitan al prestador asumir la titularidad sobre los bancos de datos personales tratados en la tercerización.

3) Garantizar la confidencialidad respecto de los datos personales sobre los que preste el servicio.

4) Mantener el control, las decisiones y la responsabilidad sobre el proceso mediante el cual se realiza el tratamiento de los datos personales.

5) Garantizar la destrucción o la imposibilidad de acceder a los datos personales después de concluida la prestación.

Además, el prestador del servicio, debe contar con los siguientes mecanismos:

1) Dar a conocer los cambios en sus políticas de privacidad o en las condiciones del servicio que presta al responsable del tratamiento, para obtener el consentimiento si ello significara incrementar sus facultades de tratamiento.

2) Permitir al responsable del tratamiento limitar el tipo de tratamiento de los datos personales sobre los que presta el servicio.

3) Establecer y mantener medidas de seguridad adecuadas para la protección de los datos personales sobre los que presta el servicio.

4) Garantizar la supresión de los datos personales una vez que haya concluido el servicio prestado al responsable y que este último los haya podido recuperar.

5) Impedir el acceso a los datos personales a quienes no cuenten con privilegios de acceso, o bien en caso sea solicitada por la autoridad competente informar de ese hecho al responsable.

El tratamiento que se les dará a los datos personales, no debe facultar al prestador del servicio de almacenamiento la transferencia de datos personales; por lo que no podrá transferir los mismos a terceros sin autorización del titular del banco de datos personales y con el consentimiento del titular del dato personal, cuando se requiera está de acuerdo a ley.

Se puede realizar un tratamiento de datos personales, mediante una subcontratación, que requerirá una previa autorización por parte del titular del banco de datos personales o responsable del tratamiento. En ese caso, el tercero debe asumir las mismas obligaciones que se establezcan para el encargado del tratamiento en la Ley 29733 y en su reglamento; asumiendo las obligaciones del titular del banco de datos personales o encargado del tratamiento cuando destine o utilice los datos personales con una finalidad distinta a la autorizada por el titular del banco de datos o responsable del

tratamiento; o efectúe una transferencia, incumpliendo las instrucciones del titular del banco de datos personales, aun cuando sea para la conservación de dichos datos

Artículo 23. Comunicación y Transferencia de datos

a) Los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados y/o transferidos a un tercero para cumplimiento de una relación contractual, profesional, y además exista un consentimiento previo del titular del dato salvo disposición contraria de la Ley 29733 y sus normas complementarias.

b) La comunicación internacional de datos solamente será posible si el destinatario ofrece una garantía igual o mayor de protección de datos personales a lo establecido en la legislación peruana. Cuando se considere necesario se deberá solicitar opinión del procedimiento a la Autoridad Nacional de Protección de Datos Personales.

c) Las transferencias internacionales deben ser comunicadas e inscritas en el Registro Nacional de Protección de Datos Personales. El área legal de GERMANIA llevará a cabo las actuaciones procedimentales para este proceso.

d) El receptor de la comunicación y/o transferencia está sujeto a lo dispuesto en la Ley 29733 y sus normas complementarias y lo dispuesto en el presente Código de Conducta.

e) No se considerará transferencia, el acceso de un tercero a los mismos, cuando dicho acceso sea necesario para la prestación de un servicio a GERMANIA, se trata de un servicio por encargo.

f) La comunicación de datos o su uso interno con fines de investigación y estadístico sólo se producirá sin la autorización del titular del dato cuando se utilice un procedimiento de disociación o anonimización.

g) La transferencia de datos personales hacia terceros, incluidas otras empresas del grupo empresarial de la corporación del GERMANIA debe ser aprobada previamente por el Jefe de Sistemas y el responsable del banco de datos asignado.

Artículo 24. Tratamiento de datos por cuenta de un tercero

a) La realización de tratamientos por cuenta de terceros debe estar regulada en un contrato que deberá constar por escrito, estableciéndose expresamente que el encargado del tratamiento únicamente o del encargado banco de datos tratará los datos conforme a las instrucciones de la GERMANIA. En el caso de incumplimiento de las estipulaciones establecidas, el encargado del tratamiento responderá de las infracciones en que hubiera incurrido personalmente.

b) Si el encargado de tratamiento de datos personales necesita, para la prestación de un servicio a GERMANIA, subcontratar con un tercero como parte del tratamiento; deberá contar con autorización previa escrita de la GERMANIA. En cualquier caso, el subcontratista tendrá las obligaciones de encargado de tratamiento y seguirá las instrucciones de GERMANIA.

c) Una vez cumplida la prestación contractual, los datos de carácter personal deben ser destruidos o devueltos a GERMANIA, o conservarse según estipulación contractual. Se recomienda no establecer un plazo mayor a dos años de conservación desde la última orden de tratamiento.

d) La obligación de confidencialidad que se establezca con este tercero respecto a los datos personales debe perdurar aun luego del término de las relaciones contractuales.

Artículo 25. GERMANIA como encargada del tratamiento de datos de otras entidades.

Cuando GERMANIA sea encargada del banco de datos, encargado y/o responsable del tratamiento de datos personales de otras entidades distinta a GERMANIA, se aplicará este código de conducta en su tratamiento interno así como las medidas de seguridad adoptadas por GERMANIA, y de manera complementaria la de la otra entidad involucrada si se acepta por acuerdo contractual.

GERMANIA debe garantizar la protección de los datos personales que reciba por encargo según lo previsto en las leyes, así comprometiéndose a no divulgarlos salvo consentimiento de los interesados o salvo los casos de obligación legal o cumplimiento de resoluciones judiciales o administrativas. En estos casos, GERMANIA debe cumplir lo dispuesto en este Código de Conducta para la protección de datos confiados por sus clientes y proveedores u otras personas, para ello siempre deberá GERMANIA solicitar a estos además la confirmación del nivel de seguridad del banco de datos personales a fin de tenerlo en cuenta durante el proceso de tratamiento de los datos personales.

TÍTULO VII: SEGURIDAD DE BANCO DE DATOS

Artículo 26. Gestión de la Seguridad de la Información de Banco de Datos

a) Los datos personales recopilados por GERMANIA se considera un activo valioso y es clasificada como INFORMACIÓN CONFIDENCIAL.

b) La protección de los datos personales se debe incorporar dentro del Sistema de Gestión de Seguridad de la Información a fin de asegurar el cumplimiento de las medidas necesarias para salvaguardar su integridad, confidencialidad y disponibilidad.

Artículo 27. Medidas de Seguridad Organizativas

El área de Sistemas como responsable de la organización de las medidas de seguridad:

a) Lleva un control y registro de los operadores con acceso al banco de datos personales con el objetivo de poder identificar al personal con acceso en determinado momento (Trazabilidad).

b) Revisa periódicamente la efectividad de las medidas de seguridad adoptadas y registrar dicha verificación en un documento adjunto al banco de datos personales.

c) Adecua los sistemas de gestión o aplicaciones existentes que intervengan en el tratamiento de datos personales, conforme a la Ley N° 29733, Ley de Protección de Datos Personales, y su reglamento, contará con el apoyo de la gerencia responsable del banco de datos personales.

d) Adecua en conjunto con los responsables de los bancos de datos personales los procesos del negocio involucrados en el tratamiento de datos personales a los requisitos establecidos en la Ley N° 29733, Ley de Protección de Datos Personales, y su reglamento.

e) Desarrolla en conjunto con los responsables de los bancos de datos personales los procedimientos documentados adecuados para el tratamiento de datos personales contenidos en estos bancos.

f) Desarrolla un programa de creación de conciencia y entrenamiento en materia de protección de datos personales, para ello cuenta con el apoyo de los gerentes.

g) Realiza una auditoría anual como mínimo respecto de las medidas de seguridad implementadas.

Cada responsable de un banco de datos personales asignará los privilegios de acceso al banco de datos personales baja su responsable, su correspondiente registro de acceso e informará al área de sistemas para la ejecución de la asignación de privilegios en los sistemas.

Artículo 28. Medidas de Seguridad Técnica en el Uso de Tecnologías de información y comunicación (TIC)

a) El uso de TIC como (bancos de datos, aplicaciones de negocio, equipos de comunicación, servidores, sistemas operativos, etc.) que soportan la gestión del tratamiento de datos personales, deben implementar los controles de seguridad requeridos en la Ley 29733 y en sus normas complementarias en especial lo referido en la Directiva de Seguridad considerando la categorización del banco de datos involucrado.

b) Gestión de contraseñas. Se debe controlar la asignación y el uso de las contraseñas de los usuarios de los sistemas de información que realizan tratamiento de datos personales mediante la adopción de las siguientes medidas:

i. Solicitar a los usuarios que mantengan en secreto las contraseñas asignadas.

ii. Cuando se utilice un servidor de autenticación, éste debe almacenar las contraseñas de manera cifrada.

iii. Permitir que el usuario cambie la contraseña asignada cuando lo considere necesario.

iv. Requerir el uso de contraseñas que contengan al menos 8 dígitos y que sean alfanuméricas (mayúsculas, minúsculas y números) y al menos incluyan un carácter especial.

v. Cuando el acceso al sistema esté expuesto en entornos públicos (intranet, internet o similares), se debe bloquear al usuario luego de cinco (05) intentos fallidos de autenticación consecutivos.

c) Revisión y registro de los privilegios de acceso. Se debe revisar periódicamente, al menos una vez por mes, que los privilegios de acceso a los datos personales correspondan al personal autorizado.

Esta revisión debe generar un registro de revisión que evidencie la realización de dicha revisión. El responsable de cada banco de datos personales realizará la revisión.

d) Protección del banco de datos personales contra acceso físico no autorizado. Cuando se contengan datos sensibles, ubicar el banco de datos personales en un ambiente aislado protegido por cerradura o similar mecanismo, donde la responsabilidad del mecanismo de acceso recae en el responsable del banco de datos personales.

e) Protección del banco de datos personales contra acceso lógico no autorizado. Los usuarios deben tener un identificador único de acceso asociado a perfiles de usuarios y los accesos autorizados para cada uno de ellos. Asimismo, se debe contar con mecanismos de restricción para evitar el acceso a recursos no autorizados. La autenticación de usuarios puede estar basada en contraseñas o mecanismos de fuerte

autenticación como el uso de toquen, dispositivos biométricos, firmas digitales, tarjetas inteligentes, tarjetas de coordenadas, entre otros.

f) Autorización o retiro del acceso de usuarios que realicen tratamiento de datos personales. El responsable de cada banco de datos personales debe autorizar o retirar el acceso de usuarios a los datos personales contenidos en el banco de datos personales, dicha operación debe ser registrada.

Los datos a registrar deben incluir como mínimo:

• Usuario (en sistemas informáticos el identificador de usuario).

• Fecha y hora de asignación y/o retiro de autorización del usuario.

• Usuario que autoriza.

g) Identificación de los accesos realizados a los datos personales para su tratamiento. El área de sistemas implementa un registro de accesos al banco de datos personales, el cual debe contener al menos los siguientes campos:

• Fecha y hora del acceso.

• Persona o personas que realiza el acceso.

• Identificador del titular de los datos personales a tratar (mediante mecanismo de disociación aplicado).

• Motivo del acceso.

Artículo 29. Medidas de Seguridad Técnica relacionadas a la alteración no autorizada del banco de datos personales.

a) Todo traslado de datos personales hacia lugares fuera de los ambientes en donde se ubica el banco de datos personales debe contar con la autorización del responsable del banco de datos personales o quien éste designe para ello.

b) Todo traslado de datos personales debe considerar:

i. Los datos en soporte físico deben estar contenidos en un contenedor que evite su acceso y legibilidad, así como un mecanismo de verificación de la no vulneración del contenedor.

ii. Los datos contenidos en soporte informático deben transportarse previa encriptación y un mecanismo de verificación de la integridad (checksum MD5, firma digital o similar).

c) Cuando se requiera eliminar la información contenida en un medio informático removible se deben utilizar mecanismos seguros de eliminación que incluyan el borrado total de la información y/o la destrucción del medio; de forma tal que, no permitan la recuperación de los datos. El área de Sistemas proporcionará a las áreas estos mecanismos.

El responsable de cada banco de datos personales debe designar a las personas autorizadas a eliminar la información de datos personales contenida en los medios informáticos removibles.

d) Cuando sea necesario, el responsable de cada banco de datos personales debe designar a las personas autorizadas a generar y/o eliminar las copias o reproducciones de los datos personales.

e) Para preservar la confidencialidad de los datos personales se va:

i. Utilizar impresoras, fotocopiadoras, scanner u otros equipos de reproducción autorizados.

ii. Supervisar el proceso de copia o reproducción de los documentos. No dejar desatendido el equipo.

iii. Retirar los documentos originales y las copias del equipo inmediatamente después de finalizada la copia o reproducción.

f) Se deben registrar las copias o reproducciones de los documentos con datos personales realizadas indicando como mínimo:

i. Nombre de la persona que solicita la copia.

ii. Nombre de la persona autorizada a realizar copias.

iii. Descripción de los datos personales copiados.

iv. Número de copias.

v. Motivo.

vi. Nombre de la persona que recibe la copia.

vii. Lugar de destino.

viii. Periodo de validez de la copia. Las copias o reproducciones de los documentos deben tener una marca que identifique el periodo de validez de las mismas. La cual será designada por cada gerencia usuaria.

Artículo 30. Medidas de Seguridad Técnica relacionadas a la pérdida del banco de datos personales.

a) Toda copia de respaldo de los datos personales debe estar protegida mediante técnicas de cifrado y almacenada en un local seguro y distante al ambiente principal de tratamiento de datos, para garantizar su disponibilidad frente a un desastre en el ambiente principal (considerar el almacenamiento en una localización diferente o remota).

b) La frecuencia y el periodo de conservación de los respaldos deben ser acorde con la finalidad del tratamiento a realizar y el impacto de la pérdida en los derechos del titular de los datos personales.

c) Cuando sea pertinente, se debe incorporar mecanismos que garanticen la continuidad del tratamiento de datos personales, principalmente cuando la finalidad tenga un alto impacto en relación con los titulares de datos personales o el bien común, tales como los bancos de datos personales del personal, clientes y proveedores.

d) Se deben realizar pruebas de recuperación de los datos personales respaldados para comprobar que las copias de respaldo pueden ser utilizadas en caso de ser requerido.

Estas pruebas deben realizarse por lo menos en forma semestral y se deben documentar los resultados de las pruebas incluyendo:

i. Fecha y hora de la prueba.

ii. Nombre de la persona que realizó la prueba.

iii. Banco de datos personales recuperado.

iv. Archivo recuperado y fecha de los datos recuperados.

v. Tiempo de recuperación.

vi. Resultados de las pruebas.

vii. Acciones tomadas en caso de pruebas insatisfactorias.

e) La información de datos personales que se transmite electrónicamente debe ser protegida para preservar su confidencialidad e integridad.

i. Transporte electrónico de datos personales en forma cifrada, lo cual puede realizarse mediante el cifrado de la información antes de su transmisión o mediante el uso de protocolos de comunicación cifrados (Ejemplo: VPN, correo electrónico cifrado, FTP seguro, entre otros).

ii. Uso de firmas digitales para validar la identidad del emisor de la información.

TÍTULO VIII: CAPACITACIÓN Y MONITOREO EN LA PROTECCIÓN DE DATOS PERSONALES

Artículo 31. Gestión de Incidencias

a) Se debe desarrollar un procedimiento de gestión de incidentes de seguridad para la protección de datos personales que considere el registro y la solución oportuna de los incidentes. Se debe registrar los incidentes de seguridad relacionados con los bancos de datos, incluyendo como mínimo : Fecha y hora del incidente, Persona que reporta el incidente, Naturaleza del incidente, Datos personales comprometidos, Personas involucradas en la resolución del caso, Consecuencias del incidente, Medias Correctivas, Recomendaciones, Recuperación del banco de datos. (Persona que realizó la recuperación, descripción de los datos restaurados).

b) Se debe informar al titular de datos personales los incidentes que afecten significativamente sus derechos patrimoniales o morales, tan pronto como se confirme el hecho. La información mínima que debe proporcionarse incluye: Naturaleza del incidente, Datos personales comprometidos, Recomendaciones al titular Y las Medidas correctivas implementadas.

Artículo 32. Auditoría

Se debe desarrollar un programa de auditoría respecto de las medidas de seguridad implementadas para asegurar la mitigación de los riesgos relacionados a la protección de datos personales. Esta actividad se debe desarrollar como mínimo una auditoría al año.

Artículo 33. Capacitación y Compromiso

a) Se debe desarrollar un programa de creación de conciencia y entrenamiento en materia de protección de datos personales.

b) Se debe mantener un compromiso documentado de aceptación a la presente política a fin de evidenciar el conocimiento y respeto a los principios de la Ley de protección de datos vigente.

TÍTULO IX: GENERALES

Artículo 34. Actualización del código de conducta

c) El Jefe de Sistemas es el custodio del código de conducta y es responsable de garantizar que la misma se mantenga actualizada y sea apropiada. La periodicidad para su revisión, actualización o ratificación es de cada 2 años, o cuando ocurran cambios significativos en los procesos internos o en la normativa externa. Se entenderá que un cambio es significativo cuando pueda repercutir en el cumplimiento de las medidas implantadas en este Código de Conducta.

d) Cada actualización del documento deberá ser acompañado de la respectiva notificación y capacitación a los obligados de cumplirla y de conocerla.

Artículo 35. Excepciones y Sanciones

a) Cualquier excepción al cumplimiento de la presente política debe ser registrado y aprobado por el Jefe de Sistemas.

b) El incumplimiento del presente documento se considerará como falta grave y será sancionado como tal.

c) El incumplimiento del presente documento será sancionado de conformidad con lo previsto en la legislación vigente y será considerado como falta grave según lo dispuesto por la normativa interna de GERMANIA.

Artículo 36. Plazos

Todos los plazos señalados en este documento deben entenderse como días hábiles.

ANEXO I: DOCUMENTOS MODELOS

De acuerdo con lo dispuesto en el numeral 3 del artículo 90º del Reglamento de la Ley 29733 se consignan las siguientes clausulas y documentos modelos para el tratamiento de datos personales.

Germania Automotriz

ORDEN DE TRABAJO

FECHA

OT

R | T | G | P

CLIENTE

Identificado con DNI / CE / RUC

Celular | Teléfono | Correo

Dirección | Distrito

Solicito realizar en el vehículo de:

Placa | Marca | Modelo | Color | Kms | Año

Los siguientes trabajos:

Por cuenta de la Cía. de Seguros (Rimac, Pacífico, Mapfre, La Positiva, Interseguros)	Por cuenta personal
Daños adicionales por evaluar	
Modificaciones adicionales	

Comprobante de venta: ☐ Boleta de Venta DNI / CE _____ / ☐ Factura RUC _____

El cliente o representante acepta las condiciones generales y el tratamiento de los datos personales colocados al reverso de este documento, declarando tener conocimiento de su contenido.

p. Germania Automotriz SAC | *Firma p. Cliente* | *Nombre y Apellidos*

CONDICIONES GENERALES

El CLIENTE declara que la información detallada en la presente orden de trabajo es real y autoriza a Germania Automotriz SAC (en adelante "Germania") a: (1) Realizar los trabajos solicitados por cuenta de EL CLIENTE y/o su Cía. de Seguros. (2) Efectuar las pruebas de carretera y/o ciudad ó trasladar el vehículo de EL CLIENTE a otros talleres o sedes de Germania en caso el servicio así lo requiera. (3) Enviarle la información relacionada al vehículo a través de coreo electrónico, mensajes al celular u otro medio de comunicación. (4) Utilizar pruebas fotográficas para evidenciar daños o características del vehículo. Así mismo, toma conocimiento que: (i) Germania podrá cobrarle US $10 diarios por concepto de almacenaje y guardianía a partir del segundo día de habérsele informado vía correo electrónico ó carta notarial, del término de los trabajos de reparación ó de la no aceptación del siniestro por parte de la Cía. de Seguros. (ii) Es obligación de EL CLIENTE retirar todas sus pertenencias del vehículo, Germania no se responsabiliza por artículos no declarados en el inventario al momento de ingresar el vehículo a sus instalaciones.

Germania no asumirá faltantes, deterioros y/o daños ocultos en el vehículo de EL CLIENTE.

TRATAMIENTO DE DATOS PERSONALES

Por el presente documento, EL CLIENTE autoriza de manera previa, libre, informada, expresa e inequívoca a Germania, con domicilio en Av. San Luis 1873, Distrito de San Borja, provincia y departamento de Lima, para que los datos personales consignados en la presente orden de trabajo sean tratados por este último, para el cumplimiento de las obligaciones contractuales y profesionales establecidos entre ambos, para que, de existir la posibilidad, pueda remitirle información acerca de sus beneficios, productos o servicios y para las labores de coordinaciones que sean necesarios con los terceros con quienes interactúa Germania.

Los datos personales recopilados se conservarán mientras se mantenga la relación contractual o comercial y hasta 10 años posteriores a la culminación de estos vínculos. Germania es el responsable del banco de datos personales mencionado en este documento y de los datos personales contenidos en estos; con el objeto de asegurar las medidas de seguridad y de protección de los datos personales.

En caso de ejercer derechos reconocidos en la Ley 29733, Ley de Protección de Datos Personales, se deberá presentar comunicación escrita a: Av. San Luis 1873, Distrito de San Borja, provincia y departamento de Lima; o al correo electrónico atencionalcliente@germania.com.pe

SOLICITUD DE DERECHOS DE PROTECCIÓN DE DATOS PERSONALES

*Formato para solicitar el ejercicio de sus derechos de información, acceso, rectificación, cancelación y oposición.

1. _____ Responsable receptor de la solicitud	2. _____ Fecha (DD/MM/AA)

DATOS DEL TITULAR DEL DATO PERSONAL

3. _____

Apellidos y Nombres

4. _____

Tipo y número de documento de identidad

5. _____

Domicilio

6._____	7. _____
Teléfono de contacto	Correo electrónico

Deseo ser contactado por: ☐ Correo electrónico ☐ Domicilio señalado

8. DERECHO A EJERCER

☐ Información ☐ Acceso ☐ Rectificación ☐ Cancelación ☐ Oposición

9. RESERVADO PARA ADMINISTRACIÓN (NO LLENAR)

_____	_____	_____
Fecha de presentación ante el responsable	Fecha de respuesta del responsable al titular del dato	Fecha de solicitud de ampliación de plazo

10. DESCRIPCIÓN Y FUNDAMENTOS DE LA SOLICITUD

_____

_____

_____

_____

11. DOCUMENTOS ADJUNTOS QUE LA FUNDAMENTAN: Copia de documento de identidad

_____

_____

_____

_____

_____

NOMBRES DEL TITULAR DEL DATO O SU REPRESENTANTE:

DOCUMENTO DE IDENTIDAD: _____ FIRMA: _____