CONDICIONES GENERALES DE CONTRATACIÓN DE VOLKSWAGEN FINANCIAL SERVICES

1. ÁMBITO DE APLICACIÓN

Las presentes Condiciones Generales serán de aplicación a cualquier colaboración comercial que comporte una contraprestación económica por la adquisición de bienes y/o la prestación de servicios entre "**VOLKSWAGEN FINANCIAL SERVICES**" (en adelante **VWFS**) y el PROVEEDOR correspondiente.

Las sociedades que conforman **VWFS** son las siguientes: (i) **VOLKSWAGEN BANK GmbH S.E.** ("**VWB**"), (ii) **VOLKSWAGEN RENTING, S.A.**, ("**VWR**"), (iii) **VOLKSWAGEN INSURANCE SERVICES, CORREDURÍA DE SEGUROS, S.L.** ("**VWIS**") y (iv) **MAN FINANCIAL SERVICES ESPAÑA S.L.** ("**MANFS**").

2. DEFINICIONES

(i) Bienes y Servicios: Se refiere tanto a Instalaciones Específicas como a Instalaciones Generales, Maquinaria, Materiales Auxiliares, Medios de Trabajo, Obra Civil, Servicios Comerciales, Servicios Generales, Energías, Consultorías y Gestorías, I+D, Formación, Vigilancia, Logística, Transporte de Personal y otros servicios, tal como se definen a continuación, así como en los Pedidos y Peticiones de Ofertas.

(ii) Condiciones Generales: Las presentes condiciones generales de contratación.

(iii) Contrato Marco: Acuerdo entre cualquiera de las sociedades (o todas en su conjunto) que componen VWFS y el PROVEEDOR en el que se definen unas tarifas y unas fechas de validez para ellas, así como un importe total del acuerdo.
En su caso, y siempre que se den unos requisitos para ello (ej. carácter puntual de los servicios, inexistencia de tratamiento de datos personales, escasa cuantía..etc) el Contrato Marco podrá ser sustituido por una **Oferta** en la que igualmente se tendrán que recoger la información necesaria del Bien o Servicio proporcionado/-s por el Proveedor.

(iv) Pedido o Petición de Oferta: Solicitud realizada por VWFS a aquellos Proveedores interesados a partir de una determinada necesidad de Bienes y/o Servicios, para que éstos formulen una oferta. Dicha solicitud incluye entre otras cosas, el pliego de condiciones, las especificaciones técnicas, los requerimientos logísticos, de calidad, medioambiental y seguridad, que deberá cumplir el objeto del Pedido.
En caso de acuerdo entre el Proveedor finalmente seleccionado y VWFS, se formalizará la correspondiente Oferta o Contrato Marco, según corresponda, atendiendo a las características del Pedido realizado por VWFS.

(v) Proveedor/es: La parte que suministra el Bien o presta el Servicio objeto de la Oferta o Contrato Marco.

(vi) Requisitos de Sostenibilidad: A los efectos de las presentes Condiciones Generales, se entenderá como tales los "Requisitos del Grupo Volkswagen para la sostenibilidad en las relaciones con socios comerciales (**Código de Conducta para Socios Comerciales**)", que son las normas sobre cómo tienen que comportarse los proveedores dentro de su actividad empresarial en relación con los principales aspectos medioambientales, sociales, económicos y de cumplimiento normativo según las políticas de Volkswagen y los principios de Global Compact (Pacto Mundial de las Naciones Unidas), la declaración para el desarrollo

sostenible a largo plazo de la Cámara de Comercio Internacional y las convenciones obligatorias de la Organización Internacional del Trabajo.

3. INDEPENDENCIA DE LAS PARTES. PERSONAL CONTRATADO POR EL PROVEEDOR

3.1. - Independencia de las partes:

Las relaciones entre las partes (VWFS y el Proveedor), son las propias de distintas personas jurídicas independientes la una de la otra y frente a terceros. Ninguna de las partes, ni sus empleados, actúa o podrá interpretarse que actúa, como representante, agente o mandatario de la otra, ni sus actos y omisiones podrán dar lugar a vínculo alguno que obligue a la otra parte frente a terceros. Asimismo, ni el perfeccionamiento ni el cumplimiento del Contrato Marco ni de sus Anexos, podrán interpretarse como una relación de asociación o de riesgo y ventura compartidos por las partes aquí intervinientes.

La naturaleza del Contrato Marco es de carácter exclusivamente mercantil. Por lo expuesto, no se deriva relación o vínculo laboral alguno entre las partes, ni entre VWFS y el personal del PROVEEDOR que, eventualmente, pudiera estar prestando alguno de los Servicios que constituye el objeto del Contrato Marco ni de sus Anexos.

3.2.- Personal

El PROVEEDOR, como entidad autónoma e independiente designará el personal capacitado y especializado que estime conveniente para que, a cargo y bajo la exclusiva responsabilidad del PROVEEDOR, y en su nombre y representación, desempeñe los Servicios objeto del Contrato Marco y de sus Anexos, siendo en consecuencia el PROVEEDOR el responsable de la determinación específica del trabajo a desarrollar de acuerdo con las instrucciones dadas por VWFS, dictando para ello las oportunas directrices para garantizar el normal desarrollo y un efectivo cumplimiento de los Servicios contratados, dentro de la más estricta legalidad.

En cualquier caso, garantizará que el personal que desarrolle las actividades contratadas, posean la cualificación, la formación, la experiencia y el nivel profesional adecuado a los trabajos a realizar, siendo responsable el PROVEEDOR de todos aquellos incumplimientos contractuales que surjan en relación con su propio personal.

Asimismo el PROVEEDOR, proporcionará los signos distintivos necesarios con la finalidad de identificación clara del personal en servicio, que de manera enunciativa y no limitativa, pueden ser: batas, uniformes de trabajo, insignias, rótulo empresarial, membretes, tarjetas colgantes de identificación, merchandising o cualesquiera otras que produzcan el fin perseguido.

El PROVEEDOR designará un representante frente a VWFS, como coordinador/a de Servicios, para mantener los contactos e informaciones oportunos entre ambas partes, atribuyéndole la función de trabajador designado en materia de prevención, encargándose igualmente el PROVEEDOR de la coordinación conjunta de los Servicios a prestar.

Dicho coordinador tendrá como norma, entre otras cosas, la de impartir las órdenes directas al personal de su plantilla, procurando una buena prestación y un normal desarrollo de los Servicios, en todos los ámbitos (vacaciones, régimen disciplinario, horarios, horas extras, descansos, bocadillo, transporte, dietas, control bajas, gestión interinidad, etc).

Para aquellos casos de ausencias justificadas (bajas, permisos, etc.), previamente autorizadas por el coordinador del PROVEEDOR y comunicados por éste a VWFS con antelación suficiente, el PROVEEDOR contrae el compromiso de sustituir, bajo sus propios criterios de selección, de forma inmediata al personal asignado a los Servicios por otros de igual valía y categoría sin coste alguno para VWFS. Para aquellos casos de ausencias injustificadas (absentismo, etc.) el PROVEEDOR igualmente contrae el compromiso de sustituir al personal asignado a los Servicios por otros de igual valía y categoría, dentro de un plazo máximo de 48 horas sin coste alguno para VWFS.

VWFS designará del mismo modo, un representante que estará en relación exclusiva con el representante del PROVEEDOR a fin de resolver cuantos problemas pudieran producirse en el desarrollo de los trabajos adjudicados y para dar las indicaciones genéricas de los Servicios a desarrollar.

En el supuesto de que VWFS no estuviera satisfecho con el Servicio prestado por el PROVEEDOR, deberá poner dicha circunstancia en conocimiento de este último detallando los motivos que sustentan la queja. El PROVEEDOR, una vez analizado el caso, se obliga a adoptar las medidas necesarias para subsanar esta situación, incluida la sustitución del personal adscrito al Servicio en un plazo máximo de siete (7) días laborables desde la comunicación de tal circunstancia por parte de VWFS, sin coste para éste.

4. OBLIGACIONES LABORALES, SALARIALES Y DE SEGURIDAD SOCIAL.

El PROVEEDOR mantendrá durante todo el período de vigencia de cada uno de los Servicios contratados, la dependencia laboral de todos los trabajadores que participen en la realización de las funciones descritas, y que son objeto del Contrato Marco y de sus Anexos, siendo responsable de su contraprestación económica, de la protección de sus derechos sociales y de ejecutar la función disciplinaria.

El PROVEEDOR con relación al personal bajo su dependencia se responsabiliza y se compromete a cumplir con los convenios colectivos y la legislación vigente en materia Laboral y de Seguridad Social así como en materia de Prevención de Riesgos Laborales, garantizando a VWFS absoluta indemnidad por cualquier responsabilidad que pudiera derivarse de las relaciones entre VWFS y el citado personal, haciéndose expresamente responsable de cualquier contingencia que pudiera afectar directa o indirectamente a VWFS como consecuencia de una infracción en dichas obligaciones por parte del PROVEEDOR o del personal que trabaja a su costa.

De acuerdo con lo anterior y en cumplimiento de la legislación laboral vigente, el PROVEEDOR declara bajo su responsabilidad y garantiza a VWFS que cumple escrupulosamente la legislación laboral vigente, encontrándose al corriente de todos sus pagos con la Seguridad Social.

El PROVEEDOR entregará a VWFS a la firma del Contrato Marco, certificación negativa expedida por la Seguridad Social mediante la que se acredite la no existencia de descubiertos o cualquier otra deuda con

dicho organismo. Igualmente, y de conformidad con el artículo 43.1 f) de la Ley 58/2003, de 17 de diciembre, General Tributaria, el PROVEEDOR aportará certificación negativa expedida por la Agencia Tributaria mediante la que se acredite la no existencia de deudas o cualquier contingencia con el mencionado organismo. Dichas certificaciones deberán ser renovadas por el PROVEEDOR y entregadas a VWFS en cada anualidad de vigencia del Contrato Marco.

Asimismo, el PROVEEDOR pondrá a disposición de VWFS, cuando así lo solicite, cualesquiera otros documentos necesarios a juicio de ésta para su oportuna verificación, comprometiéndose VWFS a garantizar la confidencialidad de dichos datos.

Si como consecuencia del incumplimiento por parte del PROVEEDOR de lo anteriormente dispuesto deviniese en sanción y/o reclamación contra VWFS, el PROVEEDOR mantendrá indemne a VWFS por tales conceptos y le indemnizará por todos los daños y perjuicios que pudiera causarle por este motivo.

El PROVEEDOR única y exclusivamente podrá subcontratar personal para la realización de los Servicios objeto del Contrato Marco, en caso de que así lo autorice VWFS específicamente para la realización de cada Servicio, responsabilizándose el PROVEEDOR en dicho caso, de la actuación de dicho personal subcontratado por todos los conceptos, incluidos el laboral y de seguridad social, indemnizando a VWFS de cualesquiera reclamaciones se pudieran efectuar a ésta.

5. GARANTÍAS Y RESPONSABILIDAD

5.1 Garantías

Los Bienes en general y/o los Servicios contratados por VWFS al Proveedor estarán garantizados en su totalidad, contra todo defecto de material, fabricación o montaje, error, dolo y/o negligencia en la prestación del Servicio, durante el periodo que legalmente corresponda de acuerdo con el tipo de Bienes o Servicios prestados.

La garantía se entenderá indefinida tanto ante cualquier defecto o vicio oculto en los casos de los Bienes, como ante cualquier Servicio defectuoso por razón de error, dolo y/o negligencia, independientemente de su origen.

5.2 Responsabilidad civil por daños y perjuicios

El Proveedor, durante la ejecución de los Servicios, se compromete a cumplir con las normas internas de VWFS y será responsable de los daños y/o perjuicios que pueda ocasionar a personas o cosas, que sobrevengan por negligencia o culpa del Proveedor, sus subcontratistas y/o los trabajadores de ambos.
En los casos anteriores, el Proveedor se obliga a mantener a VWFS libre de responsabilidad y a resarcir e indemnizar a VWFS frente a toda responsabilidad emanada de los daños anteriormente citados.

VWFS se reserva el derecho de repercutir al Proveedor cualquier gasto derivado del incumplimiento de las obligaciones del citado Proveedor, en materia de prevención de riesgos laborales, seguridad social o legislación laboral respecto de los empleados de este último.

El Proveedor suscribirá una póliza de Responsabilidad Civil adecuada y por importe suficiente para cubrir cualquier eventualidad que pueda surgir durante la vigencia de la relación contractual existente entre las Partes, por deficiencias en los bienes proporcionados o los servicios ejecutados y cualquier otra responsabilidad imputable al Proveedor.

El Proveedor, siempre que sea requerido, deberá remitir una copia de la póliza y de cada una de sus renovaciones a VWFS, en la que consten las coberturas con sus respectivos límites de indemnización, cláusula de beneficiario a favor de la compañía/s del grupo VWFS que corresponda y que dicha póliza se encuentre en vigor y al corriente de pago.

6. PRECIO Y FORMA DE PAGO

6.1. Precio

El precio correspondiente a cada uno de los Bienes o Servicios objeto del Pedido realizado por VWFS, será debidamente identificado en el Contrato Marco, sin que pueda reclamar el Proveedor cantidad dineraria alguna que no conste expresamente indicada en el mismo. Dichos precios serán incrementados con los impuestos correspondientes, que serán de cuenta de VWFS.

6.2. Forma de Pago

Salvo que se establezca otra cosa en el Contrato Marco, el Proveedor emitirá con carácter mensual durante los primeros diez (10) días hábiles del mes siguiente, facturas comprensivas de los Bienes proporcionados a VWFS o Servicios prestados a VWFS durante el mes anterior, desglosando debidamente todos los conceptos.

Las facturas emitidas por el Proveedor serán pagaderas por VWFS a los 30 días siguientes a la fecha de su recepción, mediante transferencia bancaria a la cuenta corriente titularidad del Proveedor que se indique en las mismas.

VWFS manifiesta y acepta de forma expresa que la facturación que el Proveedor le emita en virtud del Contrato Marco sea mediante facturación electrónica, debiendo enviar cada factura en formato pdf, tif o jpg a la dirección: Facturación.Proveedores@VWFS.com. Para ser aceptadas, las facturas deberán ser perfectamente legibles y especificar junto con los datos de facturación, la persona de VWFS responsable de su gestión según corresponda, así como todos los requisitos legales y fiscales vigentes en cada momento. No obstante lo anterior, VWFS podrá en cualquier momento revocar el consentimiento prestado comunicando por escrito al Proveedor su deseo de recibir la facturación en papel.

Salvo pacto en contrario, los gastos extraordinarios en los que pudiera incurrir el Proveedor para prestar los Servicios, como por ejemplo viajes y gastos de estancia, serán facturados adicionalmente por el Proveedor a VWFS, siempre y cuando el Proveedor los justifique debidamente presentando el detalle o la descripción de su previsión, para su previa y escrita autorización por VWFS.

7. DURACION Y RESOLUCIÓN

7.1. Duración

El Contrato Marco tendrá una vigencia inicial de tres (3) años, produciendo sus efectos a partir de la fecha de su firma, entendiéndose prorrogado tácitamente por periodos de tiempo de un año, salvo que cualquiera de las partes manifiesten por escrito su renuncia a la prórroga, con un preaviso de dos meses de antelación, como mínimo, a la fecha de expiración del periodo de duración inicialmente pactado o de cualquiera de sus prórrogas.

No obstante lo anterior, VWFS tendrá derecho a resolver el Contrato Marco en cualquier momento de la vigencia del mismo, comunicando tal decisión con una antelación mínima de dos (2) meses a la fecha prevista de resolución.

La resolución así efectuada no dará derecho a indemnización alguna para el Proveedor siempre que se cumpla el requisito de notificación previa y sin perjuicio de las liquidaciones que corresponda hacer por los Bienes proporcionados o Servicios prestados y no abonados.

7.2. Causas de resolución

El Contrato Marco quedará resuelto de forma inmediata en caso de que alguna de las partes incumpla las obligaciones por ella asumidas. En particular, VWFS podrá resolver de pleno derecho el Contrato Marco, en adición a cualesquiera otras acciones le pudieran corresponder, por las siguientes causas:

a) En general, por el incumplimiento o cumplimiento defectuoso por parte del Proveedor de las obligaciones asumidas en virtud del Contrato Marco.

b) Por transmisión, cesión o traspaso por parte del Proveedor de todo o parte de sus obligaciones contractuales o por subcontratación de los trabajos encomendados sin previa autorización escrita de VWFS.

c) Por la declaración judicial de concurso del Proveedor siempre y cuando dicha situación impida al Proveedor el cumplimiento de sus obligaciones contractuales.

8.- CONFIDENCIALIDAD

Se entenderá por “Información Confidencial” toda información que VWFS entregue a EL PROVEEDOR ya sea por escrito, en soporte informático u oralmente o como resultado o de conformidad con las reuniones celebradas entre las partes, relativa a asuntos comerciales, documentos legales, tecnología, procesos técnicos, metodologías, manuales técnicos, información técnica, maquinaria, procesos, productos, técnicas de marketing, estrategias de ventas, listados de precios, ofertas económicas, datos personales relativos a la plantilla, candidatos y/o clientes (en adelante, “Información Confidencial”).

Se hace constar expresamente el carácter confidencial de la información que pudiera llegar a conocimiento de EL PROVEEDOR a través del acceso a los sistemas informáticos de VWFS.

EL PROVEEDOR se obliga, de conformidad con la normativa de protección de datos de carácter personal aplicable, a mantener el debido secreto profesional respecto de los datos personales que trata.

EL PROVEEDOR se compromete a utilizar dicha información únicamente para la finalidad pactada y a exigir el mismo nivel de confidencialidad a cualquier persona que actúe por su cuenta o participe en

cualquier fase de la prestación de los Servicios. El acceso a la Información Confidencial quedará restringido a aquellos empleados o asesores profesionales independientes que la precisen. El PROVEEDOR adoptará las medidas necesarias para que el personal de dicha sociedad o dependientes conozcan estas normas y las obligaciones que tienen que cumplir conforme a ellas. En caso de revelación a terceros de dicha Información Confidencial por dichos empleados o dependientes, el PROVEEDOR responderá frente a VWFS.

Todos los ejemplares de la Información Confidencial en posesión de EL PROVEEDOR serán destruidos o devueltos, la opción que VWFS elija, a la finalización de los Servicios o cuando VWFS así lo requiera, sin retener ninguna copia.

La siguiente información no será considerada como Información Confidencial: (i) información que ya esté en posesión de cualquiera de las partes por tratarse de información pública o esté depositada en instituciones u organismos públicos o privados y a disposición de terceros, (ii) información que llegue a ser pública por circunstancias o causas no imputables a cualquiera de las partes firmantes del Contrato Marco, (iii) información que tenga que ser revelada por imperativo de la ley, de un tribunal o juzgado o por una autoridad administrativa.

Las obligaciones de confidencialidad mencionadas anteriormente permanecerán en vigor durante toda la vigencia del Contrato Marco e incluso una vez finalizada la duración del mismo. Ello sin perjuicio de cualquier otro acuerdo de confidencialidad distinto que pueda ser acordado por las partes.

EL PROVEEDOR se obliga a comunicar a todos los empleados y/o terceros que estén relacionados, directa o indirectamente, con la prestación de los Servicios objeto del Contrato Marco, la obligatoriedad del cumplimiento de la presente cláusula.

9. PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

9.1. Obligaciones del PROVEEDOR como ENCARGADO

En el supuesto de que el PROVEEDOR, en el marco de la prestación de los Servicios objeto del Contrato Marco, tenga acceso a datos de carácter personal obrantes en los ficheros titularidad de VWFS, llevará a cabo el tratamiento de los datos personales indicados en el **Apéndice I** adjunto al presente documento, como ENCARGADO del tratamiento, de conformidad con las siguientes obligaciones:

- Limitarse a realizar, exclusivamente, las actuaciones que resulten necesarias para prestar al RESPONSABLE el Servicio contratado, sometiéndose a las instrucciones que le indique, inclusive con respecto a las transferencias de datos personales a un tercer país o a una organización internacional salvo el caso de cumplimiento de una obligación legal, en tal caso, informará al RESPONSABLE de esa exigencia legal previa al tratamiento.

  Si el ENCARGADO considera que alguna instrucción infringe la legislación vigente, informará inmediatamente al RESPONSABLE.
- Mantener un registro, por escrito, de todas las actividades de tratamiento efectuadas por cuenta del RESPONSABLE.
- Comprometerse a guardar bajo su control y custodia los datos personales accedidos y a no comunicarlos en modo alguno a terceros.
- Dar apoyo al RESPONSABLE en la realización de las evaluaciones de impacto relativas a la protección de datos, cuando proceda, así como en la realización de las consultas previas a la autoridad de control, cuando proceda.
- Poner a disposición del RESPONSABLE toda la información necesaria para demostrar el cumplimiento de sus obligaciones, así como para la realización de las auditorías o las inspecciones que realicen el RESPONSABLE u otro auditor autorizado por él.

- Asistir al RESPONSABLE en la respuesta al ejercicio de los derechos de los interesados debiendo dar traslado de la solicitud de forma inmediata y, a no más tardar, dentro del plazo de tres días naturales a contar desde su recepción.

9.2.- Seguridad de los datos personales.

El ENCARGADO implantará las medidas de seguridad y mecanismos establecidos en el artículo 32 del RGPD para:

- Garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento.
- Restaurar la disponibilidad y el acceso a los datos personales de forma rápida, en caso de incidente físico o técnico.
- Verificar, evaluar y valorar, de forma regular, la eficacia de las medidas técnicas y organizativas implantadas para garantizar la seguridad del tratamiento.
- Seudonimizar y cifrar los datos personales, en su caso.

Asimismo, el ENCARGADO deberá adoptar todas aquellas medidas técnicas y organizativas que, a tenor del análisis de riesgo efectuado por el RESPONSABLE, éste considere que resultan necesarias para garantizar un nivel de seguridad adecuado, teniendo en cuenta el estado de la técnica y el coste de su aplicación con respecto a los riesgos y la naturaleza de los datos personales que deban protegerse. En el **Apéndice II** adjunto al presente documento se detallan las medidas de seguridad a aplicar.

9.3.- Auditoría

El RESPONSABLE podrá solicitar al ENCARGADO la información necesaria para evaluar su nivel de cumplimiento y en particular, evidencias sobre el cumplimiento de lo establecido: (i) en el Contrato de conformidad con la legislación aplicable, así como (ii) sin carácter limitativo, en las medidas de seguridad exigidas en el mismo.

9.3.1.- Deber de Cooperación

El ENCARGADO deberá cooperar diligentemente y facilitar el acceso y la recopilación de la información adecuada para responder a las necesidades del RESPONSABLE. Las evidencias y la documentación que se recaben en el proceso de auditoría se almacenarán en un repositorio del RESPONSABLE que permita garantizar la confidencialidad y seguridad de la información de acuerdo con el estado de la técnica.

9.3.2.- Resultado de la Auditoría

Si como consecuencia de la realización de la auditoría el RESPONSABLE detectase cualquier clase de incumplimiento, de conformidad con lo establecido en la normativa aplicable y en el Contrato Marco, podrá, a su sola discreción y en función de la gravedad de los mismos:

- Requerir al ENCARGADO la resolución inmediata del incumplimiento detectado mediante la elaboración por su parte de un plan de corrección que deberá hacerse efectivo en un plazo determinado, que no podrá exceder de un mes, debiendo el ENCARGADO aportar al RESPONSABLE aquellas evidencias que acrediten su resolución.
- Terminar anticipadamente la prestación o prestaciones de Servicios, cuyos tratamientos de datos personales se vean afectados por el incumplimiento detectado. En este caso, el ENCARGADO deberá devolver al RESPONSABLE la parte proporcional de los importes percibidos correspondientes a los Servicios que no hubieran sido efectivamente ejecutados.

9.4.- Notificación de violaciones de la seguridad de los datos.

El ENCARGADO deberá notificar al RESPONSABLE, en un plazo de 24 horas, las violaciones de la seguridad de los datos personales a su cargo de las que tenga conocimiento, incluyendo toda la

información relevante para la documentación y comunicación de la incidencia de acuerdo con lo exigido por la normativa vigente.

El ENCARGADO facilitará, como mínimo, la descripción de la naturaleza de la violación de la seguridad de los datos personales, el punto de contacto en el que pueda obtenerse más información, análisis de las posibles consecuencias de la violación de la seguridad de los datos personales y descripción de las medidas adoptadas o propuestas para mitigar los posibles efectos negativos.

Si no fuera posible facilitar la información simultáneamente, y en la medida en que no lo sea, la información se facilitará de manera gradual sin dilación indebida.

9.5.- Deber de confidencialidad.

El ENCARGADO queda obligado a guardar secreto durante la vigencia del Contrato y, en función de la tipología de información de que se trate, durante los plazos máximos previstos en la legislación vigente. Asimismo, garantizará que las personas autorizadas para tratar datos personales se comprometan, de forma expresa y por escrito, a respetar la confidencialidad y a cumplir las medidas de seguridad correspondientes, de lo que informará al RESPONSABLE poniendo, además, a su disposición la documentación acreditativa del cumplimiento de esta obligación.

9.6.- Deber de información.

Corresponde al RESPONSABLE facilitar el derecho de información en el momento de la recogida de los datos.

9.7.- Obligación de devolución de los datos.

Una vez cumplida la prestación del Servicio objeto del Contrato, salvo que el RESPONSABLE exija su devolución, el ENCARGADO se compromete a destruir aquella información que contenga datos de carácter personal que haya sido transmitida por el RESPONSABLE al ENCARGADO con motivo de la prestación del Servicio. Una vez destruidos, emitirá un certificado de destrucción al RESPONSABLE donde se relacionará la información, soportes físicos y documentación destruidos.

9.8.- Subcontratación.

El ENCARGADO no recurrirá a ningún otro encargado sin la autorización previa por escrito del RESPONSABLE. Si fuera necesario subcontratar algún tratamiento, este hecho se deberá comunicar previamente y por escrito al RESPONSABLE, indicando los tratamientos que se pretende subcontratar e identificando de forma clara e inequívoca la empresa subcontratista y sus datos de contacto.

Corresponde al ENCARGADO inicial regular la nueva relación de conformidad con el artículo 28 del RGPD, de forma que el nuevo encargado quede sujeto a las mismas condiciones (instrucciones, obligaciones, medidas de seguridad…) y con los mismos requisitos formales que él, en lo referente al adecuado tratamiento de los datos personales y a la garantía de los derechos de las personas afectadas.

En el caso de incumplimiento por parte del subencargado, el ENCARGADO inicial seguirá siendo plenamente responsable ante el RESPONSABLE en lo referente al cumplimiento de las obligaciones.

9.9.- Derechos de los interesados.

El ENCARGADO asistirá al RESPONSABLE en la respuesta al ejercicio de los derechos de los interesados (derechos de acceso, rectificación, supresión, oposición, limitación del tratamiento, portabilidad de los datos, y a no ser objeto de decisiones individualizadas automatizadas).

En este sentido, el ENCARGADO deberá dar traslado de la solicitud de forma inmediata al RESPONSABLE y, a no más tardar, dentro del plazo de tres días naturales a contar desde su recepción, para que el RESPONSABLE resuelva debidamente dicha solicitud.

9.10.- Responsabilidades.

Si el ENCARGADO, incluidos sus empleados, infringe lo establecido en el RGPD al determinar los fines y medios del tratamiento será considerado RESPONSABLE con respecto a dicho tratamiento, debiendo mantener indemne al RESPONSABLE de cualquier daño y perjuicio ocasionado como consecuencia del incumplimiento del Contrato Marco, asumiendo la total responsabilidad que pudiera irrogarse al RESPONSABLE como consecuencia de cualquier tipo de sanciones administrativas impuestas por las autoridades correspondientes, así como de los daños y perjuicios por procedimientos judiciales o extrajudiciales contra el RESPONSABLE, incluidos en todos los casos gastos por minutas de Abogado, Procurador y cualesquiera otros profesionales, considerándose asimismo causa específica de vencimiento anticipado de los Servicios que se presten, el incumplimiento, por parte del ENCARGADO, de lo establecido en esta cláusula.

9.11.- Protección de datos personales de los representantes.

Los representantes de ambas partes prestan su consentimiento para que los datos personales contenidos en el encabezamiento del Contrato Marco así como aquellos necesarios para la prestación de los Servicios puedan ser tratados por ambas partes con la finalidad de gestión y mantenimiento de la relación contractual. Los representantes de ambas partes podrán en cualquier momento ejercitar los derechos de acceso, rectificación, supresión, limitación en el tratamiento y oposición respecto a sus datos personales. Dichos derechos podrán ejercitarse por cualquier de las partes mediante comunicación escrita dirigida a las direcciones indicadas en el Contrato Marco.

10. CESIÓN Y SUBCONTRATACIÓN

Las partes contratantes no podrán ceder los derechos y obligaciones que se derivan del Contrato Marco o de sus Anexos, salvo en virtud de acuerdo expreso formalizado, por escrito, al efecto. No se reputará cesión el cambio producido en cualquiera de las partes, como consecuencia de operaciones de fusión, escisión o modificación societaria.

En caso de que el PROVEEDOR subcontrate los servicios, previa autorización de VWFS, dicha subcontratación no relevará al PROVEEDOR de sus responsabilidades conforme al Contrato Marco o sus Anexos, siendo por tanto el PROVEEDOR responsable de las obligaciones contraídas por estos terceros.

11. PROPIEDAD INDUSTRIAL E INTELECTUAL

VWFS conservará la propiedad intelectual y/o industrial de todos los datos, documentos, procedimientos y demás elementos objeto de propiedad intelectual y/o industrial, puestos a disposición del PROVEEDOR, en su caso, exclusivamente para la ejecución de los Servicios, y de los cuales el PROVEEDOR sólo gozará de un derecho de utilización mientras continúen en vigor alguno de los Servicios encomendados en virtud del Contrato Marco. El PROVEEDOR deberá restituirlos a VWFS a primera demanda o en cualquier caso, a la terminación del Contrato Marco por cualquier causa, destruyendo asimismo cualquier copia que, para la ejecución del Contrato Marco, hubiera podido realizar.

Mediante el Contrato Marco, VWFS adquiere la plena y entera propiedad de los resultados de los trabajos, servicios y prestaciones realizadas por el PROVEEDOR en ejecución del Contrato Marco y de todos los elementos que los compongan, incluyendo, a título enunciativo que no limitativo, manuales, informes, entregables, documentación (ya sea preparatoria, de uso, o de cualquier otro tipo), etc., cualquiera que fuere su soporte, así como de todos los derechos de propiedad industrial y/o intelectual asociados, cualquiera que fuere su tipo.

El PROVEEDOR garantiza que ostenta todos los derechos de propiedad intelectual, derechos de explotación y cualquier otro derecho necesarios para ejecutar la cesión indicada en el apartado anterior, debiendo indemnizar y dejar indemne a VWFS de cualquier reclamación que éste reciba respecto a

dichos derechos. El PROVEEDOR no podrá por consiguiente gozar de los derechos de explotación mencionados en el apartado anterior. En este sentido, el PROVEEDOR no podrá utilizar en beneficio propio y/o de terceros, ni difundir a ningún tercero, los resultados de los trabajos realizados ni de ningún elemento de los mismos.

Asimismo las partes se comprometen a no hacer uso del nombre de las otras, o de sus marcas, nombres comerciales o signos distintivos sin que las otras partes lo hayan autorizado previamente por escrito.

12. CÓDIGO DE CONDUCTA PARA SOCIOS COMERCIALES

El PROVEEDOR acepta y se compromete a cumplir con lo establecido en el Código de Conducta para Socios Comerciales que se adjuntan a las presentes condiciones como Anexo I, permitiendo a VWFS la realización de auditorías e inspecciones periódicas, con el fin de comprobar su cumplimiento.

Conforme a lo previsto en el apartado V del referido Código de Conducta, en caso de incumplimiento por parte del PROVEEDOR de los requisitos en él establecidos, VWFS estará facultada para resolver de forma anticipada el Contrato Marco.

13. VARIOS

13.1 Las presentes Condiciones y el Contrato Marco no podrán ser modificadas salvo en virtud de acuerdo expreso al efecto, formalizado por escrito entre las partes contratantes.

13.2 En caso de discrepancia entre lo regulado en las presente Condiciones y lo recogido en el Contrato Marco, prevalecerá lo establecido en este último.

14. LEY APLICABLE Y FUERO

Las presentes Condiciones y el Contrato Marco se regirán por la normativa española.

Cualquier conflicto o discrepancia relativos tanto a la interpretación de las presentes Condiciones y del Contrato Marco como a la ejecución de las cláusulas contenidas en dichos documentos, y que no pudiera solventarse de mutuo acuerdo entre las partes, se someterá a la jurisdicción de los Tribunales de Alcobendas (Madrid), con renuncia expresa a cualquier otro fuero que pudiera corresponderles.

APÉNDICE I.

OBJETO DEL TRATAMIENTO

[A CUMPLIMENTAR POR LAS PARTES DEPENDIENDO DEL SERVICIO PRESTADO Y TRATAMIENTO DE DATOS EFECTUADO POR EL PROVEEDOR]

1. Sumisión al Contrato	Las Partes someten a los términos previstos en el Contrato Marco el tratamiento de Datos Personales que efectúe el ENCARGADO como consecuencia de la ejecución de los servicios detallados en este APÉNDICE, así como la determinación de las obligaciones complementarias, que aquí se recojan.			
2. Actividades principales del ENCARGADO	El tratamiento se realizará sobre datos personales de los que el RESPONSABLE es titular con motivo de la prestación de los servicios objeto del Contrato Marco.			
3. Tipo de datos personales objeto del tratamiento	**CATEGORÍAS**		**EJEMPLOS**	
	□	Datos relativos a empleo y a la organización	Nombre y apellido, género, dirección, email, número de teléfono fijo o móvil, empresa del grupo, departamento, centro de coste, responsabilidades, número personal, funciones, presencia (sí/no), etc.	
	□	Datos de uso de herramientas IT	ID de usuario, funciones, derechos, números de accesos, nombre de ordenador, dirección IP, etc.	
	□	Datos de contacto privados y datos de identificación	Nombre y apellido, género, dirección, email, número de teléfono fijo o móvil, fecha/sitio de nacimiento, números de identificación, nacionalidad, etc.	
	□	Datos contractuales	Productos adquiridos, servicios financieros, fecha del contrato, precio de compra, extras, garantías, etc.	
	□	Datos relativos a circunstancias y características personales y profesionales	Datos de pareja o hijos, estado civil, foto de retrato, posición honoraria, datos del puesto, carrera, periodo de empleo, tareas, actividades, análisis de entradas en archivos, datos de entrada y salida, calificaciones, mediciones/ evaluaciones, etc.	
	□	Datos de pago y gestión	Grupo salarial, contabilidad de nóminas, pagos especiales, embargos de salarios, tiempos de asistencia, justificaciones de ausencia, etc.	
	□	Datos de fiabilidad y financieros	Conducta de pago, balance de situación, datos de agencia comercial, scorings, circunstancias financieras, cuenta bancaria, número de tarjeta de crédito, etc.	
	□	Datos sensibles	Origen racial o étnico, opiniones políticas, convicciones religiosas o filosóficas, afiliación a sindicato, datos genéticos, datos biométricos con la única finalidad de identificar a un individuo, datos relativos a salud, o datos relativos a vida sexual u orientación sexual.	
	□	Otros	.....	
4. Interesados	**INTERESADOS**		**DESCRIPCIÓN**	**EJEMPLOS**
	□	Empleados	Empleados de la correspondiente empresa del Grupo.	Ej. empleado, becario, solicitante y exempleados
	□	Clientes	Cualquier persona que tenga una relación comercial (con la correspondiente unidad de negocio).	Ej. Adquirente de vehículos, clientes de bancos, titulares de pólizas de renting
	□	Terceros	Cualquier persona que no tenga una relación comercial con la correspondiente compañía del Grupo (unidad de negocio responsable).	Ej. Visitas, invitados, personas interesadas
	□	Menores	Menores de 13 años.	
5. Finalidad Tratamiento	□	Gestión de clientes, contable, fiscal y administrativa		
	□	Gestión de nóminas		
	□	Almacenamiento de datos		

	□	Servicios económico-financieros y de seguros	
	□	Publicidad y prospección comercial	
	□	Cumplimiento/incumplimiento de obligaciones dinerarias	
	□	Análisis de perfiles	
	□	Prestación de servicios de comunicaciones electrónicas	
	□	Comercio electrónico	
	□	Otros: finalidades recogidas en el Contrato.	
6. Clasificación del Tratamiento	□	**Interno (I)**	Nivel más bajo de Medidas de Seguridad, de conformidad con la clasificación realizada por Grupo VWFSS
	□	**Confidencial (C)**	Nivel medio de Medidas de Seguridad, de conformidad con la clasificación realizada por Grupo VWFSS
	□	**Secreto (S)**	Nivel alto de Medidas de Seguridad, de conformidad con la clasificación realizada por Grupo VWFSS

APÉNDICE II MEDIDAS DE SEGURIDAD

II.1 Medidas relativas al Procesado Automatizado

Medidas Técnicas y Organizativas								
ID	MEDIDA	Tipo [1]	Clasificación [2]			TIPO DE CONTRATO		
			S	*C*	*I*	Procesado automatizado externo de datos personales (hosting externo)	Operación y administración de sistemas ubicados en CPD del RESPONSABLE	Desarrollo y mantenimiento de aplicación y sistemas
0	**Medidas relativas a la Organización de la Seguridad**							
0.1	Se deberá disponer de una estructura (departamento / rol asignado) dentro de su organización encargada de asegurar la protección de los datos personales (datos internos como externos de otros clientes).	O	**x**	**x**	**x**	**x**	**x**	**x**
0.2	Se deberá documentar y publicar una política aprobada por la alta dirección que asegure que la protección de los datos personales se lleva a cabo en conformidad con la legislación vigente.	O	**x**	**x**	**x**	**x**	**x**	**x**
0.3	Se deberá establecer un programa de formación y concienciación para proveedores, terceras partes y empleados de la organización que procesen datos personales. Todo usuario que acceda a los datos personales deberá haber recibido un curso de formación adecuado a sus funciones.	O	**x**	**x**	**x**	**x**	**x**	**x**
0.4	Los contratos de empleo deberán incorporar clausulas específicas de adherencia a las políticas de seguridad y privacidad de la organización, los cuales deberán ser firmados por los nuevos empleados previamente a la concesión de los derechos de acceso a los activos, recurso o instalaciones que procesen los datos personales.	O	**x**	**x**	**x**	**x**	**x**	**x**
0.5	Llevar a cabo un inventario de los recursos TI (servidores, ordenadores, aplicaciones, backup) que contenga datos personales.	O	**x**	**x**	**x**	**x**	**x**	**x**
1	**Medidas relativas al Control de Acceso físico y del entorno**							
1.1	Las instalaciones deberán contar con medidas de seguridad perimetrales (paredes, vallas, puertas de acceso, barreras, video vigilancia, mecanismos de autenticación de acceso a las instalaciones, recepción de visitantes, etc..) que protejan los sistemas de información y datos personales del acceso físico o manipulación no autorizado.	T	**x**	**x**	**x**	**x**	**N/A**	**N/A**
1.2	El acceso a las salas y oficinas en las cuales se procesan datos personales deberán contar con medidas técnicas y organizativas (sistema de control de acceso electrónico, video vigilancia, ventanas equipadas con sistema de detección de roturas/manipulaciones, procedimiento de solicitud de acceso a la sala/oficina, identificación de personal, sistema de alarma en caso de detección de intrusiones) que protejan frente al acceso no autorizado.	T /O	**x**	**x**	**x**	**x**	**x**	**x**

[1] Esta leyenda hace referencia al tipo de medida: Legal, Técnica u Organizativa.
[2] Deberá aplicar el Tratamiento de conformidad con la casilla marcada en el apartado 6 “Clasificación del Tratamiento”, del Anexo I.

1.3	La salida fuera de las instalaciones de dispositivos de soporte de almacenamiento (discos duros, dispositivos extraíbles, cintas de back-up) que contengan datos personales deberán ser previamente autorizados.	O	**x**	**x**	**x**	**x**	**N/A**	**N/A**
1.4	La entrada y salida a las áreas de seguridad de las instalaciones deben estar restringidas y supervisadas mediante mecanismos de control de acceso y video vigilancia que aseguren que únicamente personal autorizado accede a estas áreas.	T	**x**	**x**	**x**	**x**	**N/A**	**N/A**
1.5	El proveedor deberá planificar e implementar medidas técnicas y organizativas que protejan los datos contra amenazas del entorno como fugas de agua, fuego en el CPD, insuficiencia de suministro eléctrico, vandalismo, etc…	T/ O	**x**	**x**		**x**	**N/A**	**N/A**
2	**Medidas relativas al Control de Acceso lógico**							
2.1	**Gestión de cuentas de usuario**							
2.1.1	Definir, documentar y establecer un proceso estándar de gestión de las cuentas de acceso a los sistemas de información que procesan los datos personales (solicitud, autorización (principio de 4 ojos), creación, modificación, borrado).	O	**x**	**x**	**x**	**x**	**x**	
2.1.2	Únicamente se podrá conceder el acceso a los datos personales o los sistemas de procesado de datos personales cuando se dispongan de las autorizaciones correspondientes (de acuerdo con el proceso establecido).	O	**x**	**x**	**x**	**x**	**x**	
2.1.3	Documentar e implantar un proceso que asegure que las cuentas de acceso a los sistemas se modifican adecuadamente en caso de ocurrir cambios organizativos (p.ej. Cambio de funciones, bajas de empresa, etc…).	O	**x**	**x**	**x**	**x**	**x**	**x**
2.1.4	Asegurar que se asigna un Identificado unívoco a cada cuenta de usuario.	T	**x**	**x**	**x**	**x**	**x**	**x**
2.1.5	Los cambios en las cuentas de usuario deberán ser trazables (alta, modificación, baja) y estar documentados (P.ej. En documentos o registrados en sistemas informáticos).	O	**x**	**x**	**x**	**x**	**x**	**x**
2.1.6	Revocar las autorizaciones concedidas a usuarios de forma inmediata en caso de que la relación contractual haya finalizado (incluyendo subcontrataciones).	O	**x**	**x**	**x**	**x**	**x**	**x**

2	Medidas relativas al Control de Acceso lógico							
ID	MEDIDA	Tipo	Clasificación			TIPO DE CONTRATO		
			S	*C*	*I*	Procesado automatizado externo de datos personales (hosting externo)	Operación y administración de sistemas ubicados en CPD del RESPONSABLE	Desarrollo y mantenimiento de aplicación y sistemas
2.2	**Gestión de cuentas privilegiadas**							
2.2.1	Las cuentas privilegiadas de acceso al sistema que procesa datos personales deberán estar restringidas exclusivamente a personal autorizado y limitadas en número.	O	**x**	**x**	**x**	**x**	**x**	**x**
2.2.2	Las cuentas privilegiadas deberán ser concedidas únicamente a personal cualificado técnicamente y que han recibido previamente un curso de formación y sensibilización específico para la gestión y uso de cuentas privilegiadas.	O	**x**	**x**	**x**	**x**	**x**	**x**
2.2.3	Aquellos usuarios que requieran realizar actividades privilegiadas sobre los datos personales deberán disponer de dos cuentas en el sistema: una cuenta estándar para llevar a cabo las tareas rutinarias y operativas y una cuenta privilegiada para llevar a cabo las tareas que requieren de permisos privilegiados.	O	**x**	**x**	**x**	**x**	**x**	**x**
2.3	**Autenticación de usuarios**							
2.3.1	Se deberá prevenir la revelación no autorizada de las credenciales de autenticación de usuarios (p.ej. contraseñas, certificados, tokens de seguridad) que dan acceso a los sistemas de información y sistemas de soporte que procesan datos personales mediante la introducción de medias técnicas y organizativas (p.ej. almacenamiento cifrado de contraseñas, transferencia segura de las contraseñas al usuario, instrucciones y regulaciones que prohíban la comunicación de las contraseñas a terceros, limitación temporal de la validez de las contraseñas, complejidad de las contraseñas, proceso de asignación y reset de contraseña, etc..).	T / O	**x**	**x**	**x**	**x**	**x**	**x**
2.3.2	Las contraseñas de cuentas estándar de usuario deberán cumplir, al menos, con los siguientes requerimientos de complejidad y seguridad: -Deben ser almacenados de forma cifrada en los sistemas de información. -Las contraseñas no deben mostrarse durante el proceso de ingreso de la contraseña por parte del usuario. -La contraseña debe cambiarse de forma obligatoria tras el ingreso de la contraseña inicial de acceso al sistema. -La validez máxima de la contraseña debe ser de 90 días. El sistema deberá forzar el cambio obligatorio de la contraseña transcurrido el plazo de validez máxima. -La longitud mínima de la contraseña debe ser de 8 caracteres (incluyendo 2 números o caracteres especiales). -El histórico de contraseñas debe ser, como mínimo, de 6. -El número de intentos fallidos consecutivos a la hora de introducir la contraseña antes de que la cuenta se bloquee debe ser, como máximo, de 5. -La cuenta deberá desbloquearse de forma automática trascurridos, como mínimo, 30 minutos en el caso de haber introducido la contraseña errónea de forma reiterada. -Se deberá de impedir la introducción de contraseñas triviales o fáciles de adivinar.	T	**x**	**x**	**x**	**x**	**x**	**x**

2	Medidas relativas al control de acceso lógico								
ID	MEDIDA	Tipo	RIESGO			TIPO DE CONTRATO			
			S	*C*	*I*	Procesado automatizado externo de datos personales (hosting externo)	Operación y administración de sistemas ubicados en CPD del RESPONSABLE	Desarrollo y mantenimiento de aplicación y sistemas	
2.4	**Gestión de Autorizaciones**								
2.4.1	El gobierno de acceso a los datos y sistemas de información que procesen datos personales debe estar basado en un concepto de roles y permisos formalmente documentado y aprobado entre las partes.	O	***X***	***X***	***X***	x	x	x	
2.3.3	- La validez máxima de la contraseña debe ser de 90 días. El sistema deberá forzar el cambio obligatorio de la contraseña transcurrido el plazo de validez máxima. - La longitud mínima de la contraseña debe ser de 16 caracteres (incluyendo mayúscula, minúscula, números y caracteres especiales). - El histórico de contraseñas debe ser, como mínimo, de 6. - El número de intentos fallidos consecutivos a la hora de introducir la contraseña antes de que la cuenta se bloquee debe ser, como máximo, de 5. - La cuenta deberá desbloquearse de forma automática trascurridos, como mínimo, 30 minutos en el caso de haber introducido la contraseña errónea de forma reiterada. - Se deberá de impedir la introducción de contraseñas triviales o fáciles de adivinar Los requerimientos de complejidad y seguridad deben estar, en la medida que sea posible, forzadas en el sistema.	T	**x**	**x**	**x**	**x**	**x**	**x**	
2.3.4	Las cuentas privilegiadas de los sistemas de información (incluyendo las cuentas de administración del entorno y los compontes de soporte del sistema de información) que procesen datos personales deben utilizar mecanismos de autenticación fuerte basados en, al menos, 2 factores (PKI, One-Time Password, etc..).	T	**x**			**x**	**x**	**x**	
2.3.5	El proveedor deberá proporcionar un mecanismo de autenticación fuerte basado en, al menos, 2 factores (PKI, One-time password, etc.) para el acceso a usuarios a los sistemas de información que procesan datos personales.	T	**x**	**x**		**x**		**x**	

2.4.2	La asignación de las autorizaciones/roles debe efectuarse teniendo en cuenta el principio de segregación de funciones (SoD) y principio del mínimo privilegio y deben tener una validez temporal.	O	***X***	***X***	***X***	x	x	x
2.4.3	Los roles y autorizaciones concedidos en el sistema de información que procesa los sistemas de información deben estar registrados.	O	***X***	***X***	***X***	x	x	x
2.4.4	Las autorizaciones concedidas deben ser revisadas de forma regular (máximo 1 año) para asegurar su adherencia y validez.	O	***X***	***X***	***X***	x	x	x
2.5	**Acceso seguro a ordenadores y estaciones de trabajo**							
2.5.1	Disponer de una política de pantallas limpias, la cual deberá ser distribuida de forma regular a los empleados y formar parte de las actividades de concienciación y sensibilización que lleva a cabo la organización.	O	***X***	***X***	***X***	x	x	x
2.5.2	Los ordenadores y estaciones de trabajo del proveedor con acceso a los sistemas de información que procesan los datos personales deben disponer de un protector de pantalla protegido por contraseña que se active de forma automática transcurridos un periodo de inactividad de, como máximo, 10 minutos.	T	***X***	***X***	***X***	x	x	x
2.5.3	Los empleados y terceros que hagan uso de ordenadores y estaciones de trabajo propiedad del proveedor deben estar obligados a bloquear la pantalla una vez éstos abandonen su puesto de trabajo.	O	***X***	***X***	***X***	x	x	x
3	**Medidas relativas al Control de transferencia, almacenamiento y portabilidad**							
3.1	La transferencia electrónica de datos personales debe efectuarse de forma cifrada.	T	**x**	**x**		**x**	**x**	**x**
3.2	Los datos personales procesados de forma automatizada deberán ser almacenados de forma cifrada.	T	**x**			**x**	**x**	**x**
3.3	En el caso que existan interfaces con otros sistemas (tanto internos como sistemas de información de terceros), los datos deberán ser transmitidos de forma cifrada.	T	**x**	**x**		**x**		**x**
3.4	El proveedor hace uso de estándar, algoritmos y sistemas de cifrado robustos de acuerdo con el estado del arte vigente.	T	**x**	**x**	**x**	**x**	**x**	**x**
3.5	La transmisión mediante soporte físico de datos personales debe estar formalmente documentada (p.ej. Proceso de autorización para la transmisión, registro de destinatarios, datos de la transmisión (emisor, fecha de emisión, destinatarios, etc..) y medidas técnicas y organizativas adoptadas para asegurar su confidencialidad).	O/ T	**x**	**x**	**x**	**x**	**x**	**x**
3.6	La administración remota de los sistemas de información que procesan datos personales deben efectuarse a través de un canal de comunicación seguro (SSH, IPSec, TLS /SSL, VPN, etc..).	T	**x**	**x**	**x**	**x**	**x**	**x**
3.7	En caso requerido por parte EL RESPONSABLE, el proveedor permitirá el uso de las claves privadas propiedad del RESPONSABLE para el cifrado de la información durante su transmisión y almacenamiento, asegurando en todo momento la confidencialidad de las claves empleadas.	T	**x**	**x**	**x**	**x**		
3.8	El proveedor introducirá medidas técnicas en los sistemas de información que restrinjan la posibilidad que datos personales puedan ser exportados de forma no autorizada (p.ej. Restricción de las funcionalidades de descarga, impresión y almacenamiento de datos en los sistemas de información que procesan los datos personales).	T	**x**	**x**		**x**		**x**

3.9	Se deberán implementar medidas técnicas que permitan detectar transmisiones no autorizadas de datos personales dentro de la organización y hacia fuera de la misma (p.ej. Sistemas de prevención de fugas de información, herramientas de monitorización de actividades de usuarios en los sistemas de información).	T	**x**	**x**		**x**		
3.10	El soporte físico empleado para la transmisión de datos personales deberá estar encriptado.	T	**x**	**x**		**x**	**x**	**x**
3.11	Los soportes informáticos móviles (p.ej. USBs, ordenadores portátiles, tabletas) del proveedor que almacenen y procesen datos personales deberán estar cifrados.	T	**x**	**x**		**x**	**x**	**x**
3.12	EL proveedor solicitará la autorización del RESPONSABLE previamente a que los datos incluidos las copias de respaldo se vayan a reubicar en otro Centro de Procesamiento de Datos (CPD), país o región que no esté recogido en el contrato de servicio.	O/ L	**x**	**x**	**x**	**x**		
3.13	En caso de retirada de soportes informáticos (USB, discos duros, etc..) que procesen datos personales sensibles, éstos deberán ser borrados de forma segura (irrecuperable) previamente a su retirada.	T	**x**	**x**		**x**	**x**	**x**

4	**Control de Gestión de incidentes de seguridad**							
ID	**MEDIDA**	**Tipo**	**Clasificación**			**TIPO DE CONTRATO**		
			S	***C***	***I***	Procesado automatizado externo de datos personales (hosting externo)	Operación y administración de sistemas ubicados en CPD del RESPONSABLE	Desarrollo y mantenimiento de aplicación y sistemas
4.1	El proveedor monitoriza de forma continua y en tiempo real los incidentes de seguridad (p.ej. Mediante una herramienta SIEM). Los datos son transferidos desde los sistemas al SIEM de forma segura.	T	**x**	**x**		**x**	**N/A**	**N/A**
4.2	Los equipos informáticos y los componentes perimetrales (p.ej. plataforma de correo electrónico, sistema de acceso a Internet) disponen de un software de detección y protección frente a software malicioso (p.ej. Virus, troyanos, etc..) que se actualice de forma periódica.	T	**x**	**x**	**x**	**x**	**x**	**x**
4.3	EL RESPONSABLE será informado de forma inmediata y a través de canales de información prestablecidos en caso de ocurrir una brecha de seguridad.	O	**x**	**x**	**x**	**x**	**x**	**x**
4.4	El proveedor dispone de un procedimiento de gestión de incidencias de seguridad en el cual se establecen los criterios para clasificar, priorizar y escalar los incidentes de seguridad.	O	**x**	**x**	**x**	**x**	**x**	**x**
4.5	El proveedor evalúa periódicamente la disponibilidad de actualizaciones de seguridad para los sistemas TI y sus componentes (incluyendo clientes, componentes de red, servidores,..) que procesan los datos personales. La instalación de las actualizaciones de seguridad se realiza de forma regular a través de un procedimiento formal.	T	**x**	**x**	**x**	**x**	**x**	**x**

4.6	Los sistemas de información que procesan datos personales son escaneados de forma regular para detectar vulnerabilidades conocidas. Las vulnerabilidades detectadas son clasificadas en base a su criticidad e impacto de seguridad y corregidas de forma acorde.	O	**x**	**x**		**x**		
4.7	El proveedor responde a los incidentes de seguridad a través de un equipo de respuesta a incidentes de seguridad (p.ej. CERT), que contribuye la coordinación de la resolución de incidencias de seguridad.	O	**x**	**x**		**x**		
4.8	El proveedor aplica medidas para el bastionado *(hardening)* de las configuraciones de diferentes componentes (sistema operativo, base de datos, balanceadores, entorno de virtualización, etc..) del sistema (p.ej., deshabilitar cuentas por defecto, hacer uso de los protocolos de transferencia más seguros, etc..) que procesa los datos personales. Las guías de bastionado se basan en estándares ampliamente reconocidos y aceptados en el sector, están documentados y la implementación se revisa de forma periódica.	T	**x**	**x**		**x**	**x**	
5	**Control de Resilencia operacional**							
5.1	Definir, documentar e implantar planes de continuidad de servicios TI que abarcan todos los sistemas y componentes TI (incluyendo redes de telecomunicaciones) que procesan los datos personales, incluyendo otras ubicaciones y centros de procesamiento de datos (CPD).	O	**x**	**x**	**x**	**x**		
5.1	El proveedor dispone de herramientas para detectar y prevenir intrusiones o ciberataques (P.ej. Cortafuegos, IPS, IDS, herramientas de detección y prevenciones de ataques dirigidos,..).	T	**x**	**x**		**x**		
5.2	El proveedor dispone de herramientas o servicios para detectar y limitar el impacto de ataques de denegación de servicio (p.ej DoS, DDoS).	T	**x**	**x**		**x**		
5.3	El proveedor lleva a cabo de forma regular simulaciones de ataques informáticos (p.ej. Tests de intrusión/penetración). Las desviaciones detectadas son evaluadas y corregidas de forma regular atendiendo a un procedimiento definido.	O	**x**	**x**		**x**		
5.4	Los componentes y dispositivos que procesan datos personales están protegidos, mediante la implantación de las correspondientes medidas técnicas y organizativas, frente a desastres causados por elementos naturales (p.ej. Fuego, inundaciones, tornados).	T/O	**x**	**x**		**x**		
5.5	Las redes de telecomunicaciones del proveedor están segmentadas mediante la implantación de cortafuegos para poder limitar el impacto en caso de un incidente de seguridad.	T	**x**	**x**	**x**	**x**	**x**	**x**
5.6	Se debe disponer de una política de respaldo de los datos procesados por los sistemas informáticos. La política debe establecer el alcance de los sistemas TI, las frecuencias de las copias de respaldo, el periodo de retención, la ubicación física de las copias y las medidas de seguridad para asegurar la confidencialidad e integridad (p.ej. cifrado)). La política debe tener en consideración requerimientos regulatorios y legales.	O	**x**	**x**	**x**	**x**		
5.7	Se deben llevar a cabo de forma regular copias de respaldo de los sistemas informáticos (incluyendo los datos de configuración del sistema) que procesan los datos personales de acuerdo con la política establecida.	T	**x**	**x**	**x**	**x**	**x**	**x**

6	Control de desarrollo y operación de Aplicaciones TI			
ID	MEDIDA	Tip	Clasificación	TIPO DE CONTRATO

		o	*S*	*C*	*I*	Procesado automatizado externo de datos personales (hosting externo)	Operación y administración de sistemas ubicados en CPD del RESPONSABLE	Desarrollo y mantenimiento de aplicación y sistemas
6.1	El proveedor incluye la seguridad como un elemento integral dentro de su ciclo de vida de desarrollo de software a través de la adopción de estándares reconocidos internacionales para el desarrollo de aplicaciones seguras (p.ej. OWASP, estándares y buenas prácticas de codificación.). El proveedor deberá identificar e implementar los requerimientos de seguridad y legales en las fases tempranas del desarrollo.	O	**x**	**x**	**x**	**x**		**x**
6.2	Las actividades relativas al acceso a la aplicación (inicio, cierre de sesión, intentos exitosos/fallidos, etc..) deben ser registradas en la aplicación tanto para usuarios como para administradores. El registro de información debe permitir identificar, como mínimo, quien ha realización la acción, cuando se ha llevado a cabo la acción y el tipo de actividad realizada (p.ej. inicio de sesión, intento fallido de acceso,...).	T	**x**	**x**		**x**	**x**	**x**
6.3	Los datos de registro (logs) deben almacenarse de forma segura y el acceso debe restringirse exclusivamente a personal autorizado. Los registros se deben archivar teniendo en consideración su contenido y/o requerimientos legales y deben ser eliminados una vez hayan cumplido con su finalidad.	T	**x**	**x**		**x**	**x**	**x**
6.4	Las actividades llevadas a cabo sobre los datos personales procesados en la aplicación (creación, modificación, borrado) deben ser registrados. El registro de información debe permitir identificar, como mínimo, quien ha realización la acción, cuando se ha llevado a cabo la acción y el tipo de actividad realizada.	T	**x**	**x**		**x**	**x**	**x**
6.5	El proveedor deberá disponer de herramientas de explotación de los datos de registros (logs) que permitan detectar violaciones a las políticas de seguridad TI.	T	**x**	**x**		**x**		
6.6	El proveedor lleva a cabo tests (estáticos / dinámicos) del código fuente que desarrolla (o desarrollados por terceros), previamente a su despliegue en productivo.	O	**x**	**x**	**x**	**x**		**x**
6.7	Los entornos que no son de Producción (p.ej. Desarrollo, tests, consolidación) deben estar completamente segregados del entorno de Producción. Los datos empleados en los entornos no productivos deben estar pseudoanonimizados, en la medida que sea técnicamente factible.	T	**x**	**x**		**x**		**x**
6.8	El proveedor destruirá de forma segura los datos personales sensibles (incluyendo meta datos) en todos los sistemas de almacenamiento y respaldo en caso de que: - Se lleve a cabo la sustitución del soporte de almacenamiento (p.ej. Retirada en caso de fallo del soporte). Sea requerido por parte del RESPONSABLE. - Finalice la relación contractual con EL RESPONSABLE. Los métodos y técnicas empleadas para el borrado de los datos (p.ej. sobrescritura del soporte de almacenamiento múltiples veces mediante un algoritmo robusto) deben asegurar que la información es irrecuperable, incluso mediante el uso de técnicas forenses.	T	**x**	**x**		**x**	**x**	**x**
7	**Control de aseguramiento y cumplimiento**							

7.1	El proveedor lleva a cabo de forma regular (al menos una vez al año) e independiente, revisiones de seguridad de los sistemas informáticos que procesan datos personales con el fin de asegurar el cumplimiento y efectividad de los controles técnicos, organizativas y legales. Los tests (y sus resultados) deberán estar documentados. Las desviaciones detectadas son evaluadas, priorizadas y corregidas.	O	**x**	**x**		**x**	**x**	**x**
7.2	Llevar a cabo de forma regular simulaciones y pruebas de los planes de continuidad de los servicios TI establecidos (al menos una vez al año). Los tests (y sus resultados) deberán estar documentados. Las desviaciones detectadas son evaluadas, priorizadas y corregidas.	O	**x**			**x**	**x**	
7.3	El proveedor lleva a cabo de forma regular (al menos una vez al año) revisiones de seguridad de sus controles de seguridad física y del entorno implementados para asegurar su efectividad. Los tests (y sus resultados) deberán estar documentados. Las desviaciones detectadas son evaluadas, priorizadas y corregidas.	O	**x**	**x**		**x**		
7.4	El proveedor llevará a cabo de forma regular tests de las copias de respaldo realizadas y de los procedimientos de restauración definidos para asegurar la integridad y disponibilidad de las copias. Los tests (y sus resultados) deberán estar documentados. Las desviaciones detectadas son evaluadas, priorizadas y corregidas.	O	**x**			**x**	**x**	
7.5	El proveedor deberá llevar a cabo de forma regular e independiente revisiones de sus procesos de gestión de la seguridad de la información. El alcance de las revisiones deberá incluir, como mínimo, aquellos controles que puedan afectar a la seguridad de los datos personales del RESPONSABLE.	O	**x**			**x**	**x**	**x**
7.6	El proveedor está en posesión de certificados reconocidos internacionalmente para la gestión de la seguridad de la información como CSA Star, ISO/IEC 270001, SOC1, SOC2, SOC3, etc... Emitidos por un tercero autorizado.	O	**x**			**x**		
7.7	El proveedor dispone de procesos, procedimientos operativos e instrucciones para asegurar cumplimiento con los requerimientos legales y regulatorios, así como las regulaciones aplicables a la naturaleza del servicio.	O	**x**	**x**	**x**	**x**	**x**	**x**

II.2 Medidas relativas al Procesado No Automatizado

Medidas relativas al Procesado No Automatizado				
ID	**MEDIDA**	**Clasificación**		
		S	**C**	**I**
1.1	**Criterio de archivo**			
	Deberá garantizar la correcta conservación de los documentos, la localización y consulta de la información y posibilitar el ejercicio de los derechos de los interesados. Para ello, deberá archivar la documentación en soporte papel, en compartimentos cerrados con llave a los que sólo tenga acceso personal autorizado, y que permitan a su vez, su fácil y pronta recuperación para el caso en que se requiera.	**x**	**x**	**x**
1.2	**Dispositivos de almacenamiento**			
1.2.1	Los dispositivos de almacenamiento de los documentos que contengan datos de carácter personal deberán disponer de mecanismos que obstaculicen su apertura, (por ejemplo, archivadores, armarios, …).	**x**	**x**	**x**

1.2.2	Para todas aquellas operaciones de Tratamiento que conlleven el Tratamiento de categorías especiales de datos (por ejemplo; datos de salud, de afiliación sindical opiniones políticas, convicciones religiosas, datos biométricos,…), deberá disponer de armarios, archivadores u otros elementos en los que se almacenan los documentos con esta tipología de datos, localizados en áreas en las que el acceso está protegido con puertas de acceso dotadas de sistemas de apertura mediante llave u otro dispositivo equivalente. Dichas áreas permanecerán cerradas cuando no sea preciso el acceso a este tipo de documentos.	**x**	**x**	
1.3	**Custodia de soportes**			
1.3.1	Mientras la documentación con datos de carácter personal no se encuentre archivada en los dispositivos de almacenamiento establecidos en el punto 1.2, por estar en proceso de revisión o tramitación, ya sea previo o posterior a su archivo, la persona que se encuentre al cargo de la misma deberá custodiarla e impedir en todo momento que pueda ser accedida por persona no autorizada.	**x**	**x**	**x**
1.3.2	Siempre que vaya a desecharse cualquier documento o soporte que contenga datos de carácter personal deberá procederse a su destrucción o borrado, por medios que eviten el acceso a la información contenida en el mismo o su recuperación posterior.	**x**	**x**	**x**
1.4	**Copia y reproducción**			
1.4.1	La generación de copias o la reproducción de los documentos que contengan **categorías especiales de datos** (por ejemplo; datos de salud, de afiliación sindical opiniones políticas, convicciones religiosas, datos biométricos, …), únicamente podrán ser realizadas bajo el control del personal autorizado.	**x**		
1.4.2	Deberá procederse a la destrucción de las copias o reproducciones desechadas de forma que se evite el acceso a la información contenida en las mismas o su recuperación posterior.	**x**	**x**	**x**
1.5	**Traslado de la documentación**			
	En el supuesto de tener que proceder, por necesidades del servicio, al traslado físico de la documentación, siempre deberá impedir el acceso o manipulación de la información por parte de personal no autorizado o terceros no vinculados con EL RESPONSABLE.	**x**	**x**	**x**
1.6	**Acceso a la documentación**			
1.6.1	Deberá limitar exclusivamente al personal autorizado el acceso a la documentación que contenga datos personales.	**x**	**x**	**x**
1.6.2	Deberá controlar los accesos a la documentación y tener implementado un registro de accesos general.	**x**		
1.6.3	Deberá indicar los documentos o tipos de documentos que puedan ser utilizados por múltiples usuarios.	**x**		
1.7	**Personal autorizado a acceder a categorías especiales de datos**			
	El personal autorizado a acceder a la documentación que contenga **categorías especiales de datos** (por ejemplo; datos de salud, de afiliación sindical opiniones políticas, convicciones religiosas, datos biométricos, …), deberá ser previamente autorizado, en un Libro Registro, identificando el puesto ocupado, así como los datos a los cuales se les permite el acceso.	**x**		

ANEXO I. CÓDIGO DE CONDUCTA PARA SOCIOS COMERCIALES

Requisitos del Grupo Volkswagen para la sostenibilidad en las relaciones con sus socios comerciales (Código de conducta para socios comerciales)

I. Prefacio

Los requisitos siguientes concretan las expectativas del Grupo Volkswagen en cuanto a la actitud y el comportamiento de los socios comerciales dentro de su actividad empresarial. Los requisitos se consideran la base para un diseño exitoso de las relaciones comerciales entre el Grupo Volkswagen y sus socios.

II. Cooperación

Los requisitos se basan en las directrices y convenciones nacionales e internacionales, las normas y los valores internos. Se basan, entre otras cosas, en los Principios del Pacto Mundial de las Naciones Unidas, la Carta de las Empresas para un Desarrollo Sostenido de la Cámara de Comercio Internacional así como en las convenciones correspondientes de la Organización Internacional del Trabajo, y se complementan con la política medioambiental de Volkswagen, con los objetivos y condiciones medioambientales derivados de ella, la política de calidad, así como la declaración de derechos sociales de Volkswagen.

Con el objetivo de mantener una actividad comercial satisfactoria y sostenible, la calidad y el valor de nuestros productos y servicios representan una ventaja competitiva. Los socios comerciales de Volkswagen participan decisivamente en el diseño del éxito empresarial del Grupo. La relación de cooperación proporciona vínculos comerciales consistentes, que se caracterizan por los beneficios para ambas partes. Por ello, Volkswagen apuesta por una estrecha cooperación con sus socios comerciales. Los valores básicos de nuestra colaboración son la integridad, equidad, transparencia y cooperación.

Volkswagen desea una actuación respetable, honesta y que cumpla con las reglas en la actividad comercial cotidiana. Esto es lo que espera también de los socios comerciales, especialmente respecto a los derechos humanos, la protección laboral y de la salud, la protección medioambiental y la lucha contra la corrupción. Por lo tanto, Volkswagen espera que también los socios comerciales y sus empleados actúen con responsabilidad y se comprometan a cumplir con los requisitos establecidos en este documento. Además, el Grupo Volkswagen espera que sus socios comerciales cuiden también del cumplimiento de los

requisitos por parte de sus proveedores. Estos requisitos no pueden ser la base para ninguna reclamación de terceros.

III. Ámbito de aplicación

Los requisitos de sostenibilidad son válidos para todas las relaciones comerciales entre el Grupo Volkswagen y sus socios comerciales.

El Grupo Volkswagen se reserva el derecho de comprobar in situ, por medio de expertos, el cumplimiento por parte de los socios comerciales de los requisitos mencionados a continuación, sólo después de aviso previo y en presencia de representantes del socio comercial, dentro de horarios comerciales normales y cumpliendo con la legislación respectivamente aplicable, especialmente la de protección de datos.

IV. Requisitos

1. Protección medioambiental

Volkswagen desarrolla, produce y distribuye en todo el mundo automóviles para asegurar la movilidad individual. Asume la responsabilidad de la mejora continua de la compatibilidad medioambiental de sus productos y la reducción de la explotación de los recursos naturales teniendo en cuenta los puntos de vista económicos. Por ese motivo, los socios comerciales deben cumplir estrictamente todas las leyes y disposiciones medioambientales aplicables en todos los países en que actúan. Es obligatorio cumplir con

- la Política Medioambiental de Volkswagen;
- los Objetivos Medioambientales de Desarrollo Técnico;
- la Norma VW 01155 (piezas de vehículos suministradas);
- los párrafos 2.1 (Objetivos de la Norma), 8. (Impacto ambiental), 9.1 (Obligaciones y prohibiciones sobre materiales) y 9.2 (Requisitos para los materiales) de la Norma VW 99000 (Requisitos Generales para la Prestación de Servicios en el Desarrollo de Piezas) y las especificaciones de los pliegos de condiciones de piezas estándar.

Además, Volkswagen espera de sus socios comerciales la consideración y el cumplimiento de los aspectos siguientes:

Elaboración y aplicación de sistemas de gestión medioambiental

La gestión orientada al medio ambiente es uno de los objetivos preferentes de la política empresarial. Por lo tanto, Volkswagen espera que todos los socios comerciales con centros de producción tengan un sistema de gestión medioambiental adecuado. Además, Volkswagen espera de sus proveedores principales un sistema de gestión medioambiental homologado según la norma internacional ISO 14001 o el reglamento EMAS de la Unión Europea.

Tratamiento activo de los desafíos ecológicos

Los desafíos ecológicos deben tratarse con cuidado y previsoramente. Se toman medidas para un tratamiento responsable del medioambiente. Debe intentarse conseguir un desarrollo y difusión de tecnologías ecológicas.

Prevención de daños medioambientales y para la salud; productos y procesos con bajo consumo de recursos y emisión de gases invernadero

En todas las actividades, el impacto sobre el medio ambiente y la salud de los trabajadores se evita o se mantiene lo más bajo posible. Para el desarrollo, la fabricación y en la fase de uso de los productos, así como en otras actividades, se tienen en cuenta el uso ahorrativo de la energía y las materias primas, la minimización de las emisiones de gases invernadero, el uso de recursos renovables y la minimización de los daños medioambientales y para la salud.

Residuos y reciclaje

En el desarrollo, la fabricación y para la fase de uso de productos, así como para el desarrollo y ejecución de procesos de producción y otras actividades, se tienen en cuenta evitar la generación de residuos, la reutilización, el reciclaje, así como la disposición ecológica y sin peligro de los residuos generados.

Formación de los trabajadores

Los trabajadores son informados, calificados y motivados en la protección medioambiental de acuerdo con sus tareas.

2. Derechos de los trabajadores

Para Volkswagen, el cumplimiento de los derechos humanos reconocidos internacionalmente es la base de todas las relaciones comerciales. Deben tenerse especialmente en cuenta las disposiciones siguientes, así como el derecho laboral del país en el que actúan los socios comerciales:

Libertad de asociación

Se reconoce el derecho básico de todos los trabajadores a formar sindicatos y representaciones de los trabajadores y adherirse a ellos. Donde este derecho esté limitado por las leyes locales, deben fomentarse posibilidades alternativas de representación de los trabajadores, cumpliendo con las leyes.

No discriminación

Se garantiza la igualdad de oportunidades e igualdad de trato con independencia del origen étnico, color de piel, sexo, religión, nacionalidad, orientación sexual, origen social o tendencia política, siempre que se base en los principios democráticos y en la tolerancia frente a quienes piensan de modo diferente. Los trabajadores se seleccionan, contratan y promocionan básicamente en base a su calificación y sus capacidades.

No trabajos forzados

Volkswagen rechaza cualquier uso consciente de trabajos forzados u obligados, incluidos la esclavitud por deudas o el trabajo de prisioneros no voluntario.

No trabajo infantil

Está prohibido el trabajo infantil. Se tendrá en cuenta la edad mínima para autorizar el trabajo según las regulaciones estatales.

Remuneración y prestaciones

La remuneración y las prestaciones pagadas o realizadas a cambio de una semana laboral normal no serán inferiores a los mínimos garantizados y legalmente vigentes. Si no existen regulaciones legales o de convenio colectivo, la remuneración y las prestaciones se regirán por las tarifas sectoriales, locales habituales, que aseguren a los empleados y a sus familias un nivel de vida apropiado.

Tiempos de trabajo

El tiempo de trabajo cumplirá, como mínimo, las condiciones legales nacionales respectivas o con las normas mínimas de los sectores económicos nacionales respectivos.

Protección laboral y sanitaria

El socio comercial cumplirá, como mínimo, con las normas nacionales referidas a un entorno de trabajo seguro e higiénico y adoptará en este contexto las medidas apropiadas para garantizar la salud y la seguridad en el puesto de trabajo, con el fin de garantizar las condiciones de trabajo adecuadas para la salud.

3. Relaciones comerciales transparentes

Prevención de conflictos de intereses

Los socios comerciales de Volkswagen toman sus decisiones, exclusivamente, en base a criterios objetivos y no se dejan influir por intereses y relaciones personales.

Lucha contra la corrupción

Volkswagen apoya los esfuerzos nacionales e internacionales para no influir en la competencia o adulterarla mediante sobornos y rechaza toda clase de comportamientos corruptos y perjudiciales para las empresas. Volkswagen requiere de sus socios comerciales que rechacen y eviten cualquier forma de corrupción, incluyendo también los llamados ”Facilitation Payments“ (“pagos de facilitación” para agilizar los trámites funcionariales rutinarios). Los socios comerciales deben asegurar que sus trabajadores, subcontratistas o representantes no paguen, ofrezcan o reciban sobornos, mordidas, donaciones no permitidas u otros pagos o ventajas no permitidos a/de clientes, funcionarios u otras terceras partes.

4. Comportamiento correcto en el mercado

Libre competencia

Volkswagen requiere de sus socios comerciales que cumplan con las leyes de la competencia y antimonopolio vigentes y aplicables. En especial, no deben establecer acuerdos contrarios a la competencia con competidores, proveedores, clientes u otras terceras partes ni abusar de una eventual posición dominante en el mercado.

Controles de importación y exportación

Para la importación y exportación de bienes/ servicios, los socios comerciales deben cumplir todas las leyes vigentes y aplicables.

Blanqueo de dinero

Los socios comerciales sólo deben mantener relaciones comerciales con socios comerciales de cuya integridad estén convencidos. Deben cuidar de que no se violen las disposiciones legales vigentes sobre blanqueo de dinero respectivas.

V. Consecuencias jurídicas del incumplimiento de los requisitos

Volkswagen considera que el cumplimiento de los requisitos formulados en este documento es fundamental para la relación contractual correspondiente. Si un socio comercial de Volkswagen no cumple estos requisitos, Volkswagen se reserva el derecho a finalizar la relación comercial con él mediante rescisión extraordinaria. Volkswagen puede decidir libremente no ejercer este tipo de consecuencias y, en su lugar, adoptar medidas alternativas si el socio comercial se compromete de forma creíble y puede justificar que ha adoptado inmediatamente medidas para evitar futuros incumplimientos similares.