Anexo XVI

DOCUMENTO 1271-00-01/08 WP 154 DEL GRUPO DE TRABAJO "ARTÍCULO 29" QUE PROPORCIONA UN MARCO PARA LA ESTRUCTURA DE LAS NORMAS CORPORATIVAS VINCULANTES (BINDING CORPORATE RULES) CONOCIDAS COMO BCR, APROBADO EL 24 DE JUNIO DE 2008 EN BRUSELAS

Este grupo de trabajo se estableció en virtud del artículo 29 de la Directiva 95/46/CE. Este es un órgano consultivo independiente europeo de protección de datos y privacidad. Sus tareas se definen en el artículo 30 de la Directiva 95/46/CE y el artículo 15 de la Directiva
2002/58/CE.

INTRODUCCIÓN

- Obligación explícita para todas las filiales y empleados a respetar el BCR.
- El compromiso por parte del Consejo de Administración de la empresa para asegurar el cumplimiento con las normas descritas.
- Objetivos del BCR (proporcionar una protección adecuada para la transferencia y tratamiento de datos personales por el grupo).
- Referencia a la legislación pertinente sobre protección de datos (Directivas de la UE95/46/CE y 2002/58/CE).
- Una subsidiaria puede actuar como controlador, procesador, exportador e importador de datos.

1 - ÁMBITO DE APLICACIÓN

- Transferencias obligatorias y tratamientos dentro del grupo,
- Su ámbito geográfico (sólo se aplican a los datos tratados en la UE y fuera de la UE o cualquier dato)
- Su ámbito de aplicación material (por ejemplo, el tipo de tratamiento: carácter automático / manual de los datos: clientes / HR / proveedores).

Descripción del flujo de datos y los propósitos de tratamiento, incluyendo:

- La naturaleza de los datos transferidos,

- El propósito de la transferencia / procesamiento,
- Los importadores / exportadores de los datos en la UE y fuera de ella.

2 - Definiciones

- Las definiciones clave (datos de carácter personal, los datos confidenciales, se refieren los datos, el controlador, el procesador, el procesamiento, la tercera parte las autoridades de protección de datos),
- Otras definiciones que podrían incluirse en un glosario, como por ejemplo los siguientes términos: exportador de datos, el importador de datos, la sede europea / filial europea responsable de la delegación filiales, delegado / instancia de encargada de la protección de los datos
- Compromiso con la interpretación de los términos de las reglas corporativas vinculantes de acuerdo con las Directivas de la UE 95/46/CE y 2002/58/CE.

3 - Limitación de la finalidad

- Los datos personales serán transferidos y procesados de manera su legítima y específica
- Los datos personales no serán objeto de un trato más incompatible con dichos fines,
- Garantías adicionales cubrirán los datos sensibles, como es requerido por la Directiva Europea 95/46/CE .

4 - Calidad y proporcionalidad

- Los datos personales deben ser exactos y en caso de ser necesario deberán actualizarse.
- Los datos personales deberán ser adecuados, pertinentes y el número de ellos no debe ser excesivo en relación con los fines para los que son transferidos y procesados,
- El tratamiento de datos personales no se llevará más tiempo de lo necesario para los fines para los que fueron recopilados.

5 - Base jurídica de tratamiento de datos personales

- El interesado ha dado su consentimiento explícito, o
- El procesamiento es necesario para la ejecución de un contrato en el que el interesado sea parte o la ejecución de medidas precontractuales adoptadas a petición de este último, o
- El tratamiento es necesario para el cumplimiento de la obligación jurídica a la que esté sujeto, o
- El Tratamiento sea necesario para salvaguardar el interés vital del interesado, o

- El procesamiento es necesario para el cumplimiento de un fin público o en el ejercicio de un acto de la autoridad o de un tercero a quien se comuniquen los datos, o

- El procesamiento es necesario por un interés legítimo del responsable, un tercero o terceros a los que se comuniquen los datos, excepto cuando tales intereses no prevalezca el interés o los derechos y libertades fundamentales del individuo.

6 - Base jurídica de tratamiento de datos sensibles

El tratamiento de datos sensibles está prohibido, excepto cuando:

- El interesado ha dado su consentimiento explícito al tratamiento de datos sensibles de que se trate, salvo que esté prohibido por la ley, o

- Es necesario para el cumplimiento de los derechos y obligaciones específicos del responsable del tratamiento en la legislación laboral, en la medida en que éste autorizado por la ley nacional aplicable que establezca las garantías adecuadas, o

- El procesamiento es necesario para proteger los intereses esenciales de la persona o de otra persona sin posibilidad de otorgar su consentimiento, o

- El tratamiento se lleve a cabo por una fundación, asociación u organización sin fines de lucro y con propósitos políticos, filosóficos, religiosos o sindical en el marco de sus actividades legítimas y con las debidas garantías, siempre que se refiera sólo a los miembros de ese organismo o a las personas que tienen contacto regular con estos en relación con los objetivos que persigue y los datos no sean revelados a terceros sin el consentimiento de los interesados, o

- El tratamiento se refiere a datos sensibles que fueron manifiestamente hechos públicos por el interesado, o

- Tratamiento de datos sensibles es necesario para el reconocimiento, ejercicio o defensa de un derecho, o

- Tratamiento de datos sensibles es necesario para la medicina preventiva, diagnóstico médico, la prestación de servicios o tratamientos médicos o la gestión de los servicios de salud, en la medida en que el tratamiento de estos datos se realiza mediante un profesional en materia de salud sujeto al secreto profesional en el Derecho del país en cuestión o reglamentos dictados por las autoridades nacionales competentes, o por otra persona sujeta asimismo a una obligación equivalente de secreto.

7 - Transparencia y Derecho a la Información

El compromiso de que las normas corporativas vinculantes sean de fácil acceso para todos los interesados, además de describir cómo se les

informa a los sujetos interesados todo lo relativo a la transferencia y el tratamiento de sus datos personales, a través de los siguientes compromisos:

- Identidad de los responsables del tratamiento de datos y, en su caso, su representante;
- Fines para los que se presentarán los datos;
- Cualquier otra información tal como:

i) los destinatarios o categorías de destinatarios,

ii) la existencia de un derecho de acceso de las personas afectadas respecto sus datos y el derecho de corregir los mismos, ya que, dadas las circunstancias particulares en que se recaban los datos, esta información es necesaria para garantizar el respeto de la persona en cuestión a través de un tratamiento justo.

Si los datos no fueron proporcionados por la persona, la obligación de informar a este último no se aplica si la información del interesado resulte "imposible" o exija esfuerzos desproporcionados o si la legislación prevé específicamente el registro o la comunicación de datos.

8 - Los derechos de acceso, rectificación, cancelación y bloqueo de los datos:

- Toda persona tiene derecho a obtener una copia de todos los datos procesados, sin limitaciones, con intervalos razonables y sin retrasos ni gastos excesivos,
- Cualquier persona interesada tiene derecho a obtener la rectificación, supresión o bloqueo de los datos, particularmente si están incompletos o son inexactos,
- Cualquier persona interesada tiene derecho a oponerse en cualquier momento, por razones legítimas particulares, a que sus datos sean objeto de tratamiento, salvo disposición legal en contrario. Si la oposición es justificada, el tratamiento debe ser interrumpido,
- Cualquier persona interesada tiene derecho a oponerse, previa petición y sin pago alguno, al tratamiento de sus datos con fines de mercadotecnia directa.

9 - Decisiones individuales automatizadas

Compromiso de que ninguna evaluación o decisión relacionada con la persona en cuestión y que puedan afectarle significativamente se basará únicamente en un tratamiento automatizado de los datos, a menos que la decisión en cuestión:

- Se tome para la celebración o ejecución de un contrato, siempre que la solicitud de celebración o ejecución presentada por el interesado, se ha

cumplido, o que se hayan adoptado las medidas apropiadas, tales como la oportunidad de presentar su punto de vista, garantizar la salvaguarda de sus intereses legítimos, o

- Está autorizada por una ley que especifica las medidas para salvaguardar los intereses legítimos de la persona en cuestión.

10 - Seguridad y Privacidad

Compromiso según el cual, las medidas de índole técnico u organizacional apropiados serán adoptados para proteger los datos personales contra su destrucción accidental o ilícita, pérdida accidental, su alteración, divulgación o acceso no autorizado, sobre todo cuando el tratamiento implique la transmisión de datos en una red, y contra cualquier otra forma de tratamiento ilícito.

Teniendo en cuenta la tecnología de punta y los costos asociados con la implementación de estas medidas, éstas deben garantizar un nivel de seguridad adecuado respecto los riesgos que se presenten por el tratamiento y la naturaleza de los datos a protegerse.

En este sentido, las medidas de seguridad en cuestión deben ser aplicadas en el tratamiento de los datos sensibles.

11 - Relaciones con los subtratante que son filiales del grupo

Explicación de cómo los datos personales están protegidos cuando se utiliza un subcontratista que es una filial del grupo. Estos consisten fundamentalmente en que:

- El controlador selecciona un tratamiento que reúna garantías suficientes en relación con las medidas de seguridad técnica y de organización que rigen el tratamiento a realizar y asegura el cumplimiento de estas medidas;
- El controlador del procesador proporciona las instrucciones en forma contractual de acuerdo con la ley aplicable, el contrato establecerá entre otros rubros los siguientes:

i) que el subtratamiento solo se hará siguiendo las instrucciones del responsable del tratamiento,

ii) que las obligaciones en materia de seguridad y confidencialidad incumben solo al subtratante.

12 - Restricciones a las transferencias y las transferencias posteriores al tratamiento de los datos y los contratistas externos (que no son filiales del grupo)

Descripción de las medidas adoptadas para restringir las transferencias posteriores fuera del grupo y el compromiso de que:

- Los subtratantes externos en la UE o de un país reconocido por la Comisión Europea que garantizarán un nivel adecuado de protección estarán obligado por contrato escrito indicando que el encargado del subtratamiento sólo actuará siguiendo instrucciones del responsable del tratamiento y es responsable de la aplicación de medidas de seguridad y confidencialidad adecuadas;

- Todas las transferencias de datos a los responsables de tratamientos externos fuera de la UE deben cumplir con normas de la UE sobre los flujos transfronterizos de datos (artículos 25-26 de la Directiva 95/46/CE, utilizando, por ejemplo, las cláusulas contractuales aprobadas por decisiones de la UE 2001/497/CE y 2004/915/CE de la Comisión o de otras modalidades contractuales apropiadas, de conformidad con los artículos 25 y 26 de la Directiva de la UE);

- Todas las transferencias de datos a los subcontratistas externos situados fuera de la UE deben respetar las normas relativas a los subtratantes (artículos 16-17 de la Directiva 95/45/CE), además de las normas relativas a los flujos transfronterizos de datos (artículos 25 - 26 de la Directiva 95/46/CE).

13 - Programa de Capacitación

Compromiso de proporcionar una formación adecuada en materia de BCR al personal con un acceso permanente o seguido a los datos personales, o asociados a la obtención de datos personales o al desarrollo de herramientas para el tratamiento de los mismos.

14 - Programa de Auditoría

Compromiso de realizar auditorías sobre el cumplimiento de las BCR en el grupo, particularmente los siguientes puntos:

- El programa de auditoría cubre todos los aspectos de las BCR, incluyendo métodos para garantizar que las medidas correctivas se llevarán a cabo;

- Las auditorías se realizan de forma cotidiana (especificar la frecuencia) por los responsables de tratamiento internos o externos acordados o por petición expresa de un delegado para la protección de datos / una instancia de protección de la privacidad (o cualquier otra instancia en dentro del grupo);

- Los resultados de las auditorías se comunican a la protección de datos Jefe / a la instancia de protección de la privacidad o de una entidad de protección de la vida privada (o de otra instancia en el seno del grupo) y del Consejo de Administración;

- Las autoridades de protección de datos pueden recibir una copia de las auditorías en caso de solicitarla;

- El plan de auditorías debe permitir a las autoridades de protección de datos llevar a cabo dichas auditorías por sí mismas en caso de ser necesarias;
- Cada una de las filiales del grupo se compromete a someterse a las auditorías de las autoridades de protección de datos y se constriñe a seguir las recomendaciones de las autoridades competentes en todos los asuntos relativos a estas reglas.

15 – Respecto las reglas y control de su aplicación

Compromiso para designar el personal necesario (por ejemplo, una red de responsables de protección de datos), asistidos por la dirección, a fin de supervisar y garantizar el respeto de las reglas.

Una breve descripción de la estructura interna, del papel y las competencias de la red, de los responsables de la protección de datos o de la función similar creada con miras a garantizar el respecto de las reglas. Puede estar previsto, por ejemplo, que la persona responsable de la protección de datos realice funciones de consejero a la luz de un

DOCUMENTO 1271-00-01/08 WP 154 DEL GRUPO DE TRABAJO "ARTÍCULO 29" QUE PROPORCIONA UN MARCO PARA LA ESTRUCTURA DE LAS NORMAS CORPORATIVAS VINCULANTES (BINDING CORPORATE RULES) CONOCIDAS COMO BCR, APROBADO EL 24 DE JUNIO DE 2008 EN BRUSELAS

Este grupo de trabajo se estableció en virtud del artículo 29 de la Directiva 95/46/CE. Este es un órgano consultivo independiente europeo de protección de datos y privacidad. Sus tareas se definen en el artículo 30 de la Directiva 95/46/CE y el artículo 15 de la Directiva 2002/58/CE.

INTRODUCCIÓN

- Obligación explícita para todas las filiales y empleados a respetar el BCR.
- El compromiso por parte del Consejo de Administración de la empresa para asegurar el cumplimiento con las normas descritas.
- Objetivos del BCR (proporcionar una protección adecuada para la transferencia y tratamiento de datos personales por el grupo).
- Referencia a la legislación pertinente sobre protección de datos (Directivas de la UE 95/46/CE y 2002/58/CE).
- Una subsidiaria puede actuar como controlador, procesador, exportador e importador de datos.

1 - ÁMBITO DE APLICACIÓN

- Transferencias obligatorias y tratamientos dentro del grupo,
- Su ámbito geográfico (sólo se aplican a los datos tratados en la UE y fuera de la UE o cualquier dato)
- Su ámbito de aplicación material (por ejemplo, el tipo de tratamiento: carácter automático/ manual de los datos: clientes / HR / proveedores).

Descripción del flujo de datos y los propósitos de tratamiento, incluyendo:

- La naturaleza de los datos transferidos,
- El propósito de la transferencia / procesamiento,
- Los importadores / exportadores de los datos en la UE y fuera de ella.

2 - Definiciones

- Las autoridades competentes en materia de protección de datos.

Compromiso que establezca que todas las personas que gocen derechos como terceros beneficiarios también podrán acceder a esta cláusula.

19 - RESPONSABILIDAD

Compromiso según el cual:

- La sede europea o la filial responsable europea de protección de datos se compromete a asumir la responsabilidad y tomar las medidas necesarias para reparar las acciones de las subsidiarias de otras filiales del grupo fuera de la UE y pagar una indemnización por cualquier daño que resulte de la violación de la BCR por dichas filiales. En caso de imposibilidad, existen otros mecanismos como aquellos conocidos de responsabilidad solidaria establecidos por la propia Comisión europea;
- Es al sitio europeo o a la filial europea responsable de protección de datos a quiénes les corresponde la carga de la prueba de que la filial establecida fuera de la U.E. no es responsable de la violación que dio lugar a la demanda de reparación.

Si la sede europea o la filial europea de protección de datos delegado está en posibilidad de probar de que la filial establecida fuera de la U.E. no es responsable de la transgresión, este o ésta podrá deslindarse de toda responsabilidad.

20 – Asistencia mutua y cooperación hacia las autoridades de protección de datos

Compromiso según el cual:

- Las filiales cooperarán y se prestarán ayuda mutua para la gestión de las solicitudes o reclamaciones de particulares, o con las consultas o solicitudes de información de las autoridades de protección de datos;

- Las entidades adopten las recomendaciones de las autoridades de protección de datos relativas a la interpretación de las normas corporativas vinculantes.

21 - Actualización de las reglas

Compromiso de comunicar a todas las filiales y las autoridades de protección de datos cualquier cambio significativo en las BCR o a la lista de filiales, para tomar en cuenta los cambios en el entorno normativo y la estructura de empresa, estipulando puntualmente que:

- Algunos cambios pueden requerir la emisión de una nueva autorización por las autoridades de protección de datos ;

- Actualizaciones de las normas corporativas vinculantes o de la lista de filiales sujetas a las BCR son posibles sin necesidad de introducir una nueva solicitud de autorización, con sujeción a las siguientes condiciones:

i) una persona designada actualice la lista de las subsidiarias sujetas a las normas corporativas vinculantes, registre y difunda toda actualización de las reglas y provea las informaciones requeridas por las personas interesadas o por las autoridades de protección de datos;

ii) ningún transferencia será realizada hacia una nueva filial, en tanto que ésta no ésta no éste obligada por la normativa vinculante y no éste en posibilidades de garantizar su cumplimiento;

iii) cualquier cambio en las normas o la lista de filiales, acompañada de una breve exposición de motivos que justifiquen dicha actualización, debe notificarse una vez al año a las autoridades de protección de datos que expiden las autorizaciones.

Compromiso que cualquier cambio sustancial a las reglas también se comunicará a los interesados.

22 - Vínculos entre la legislación nacional y las normas corporativas vinculantes

Explicación según la cual:

- Si las leyes locales - por ejemplo, la legislación de la UE - exige un mayor grado de protección de datos personales, prevalecerá sobre las reglas corporativas vinculantes;

- En todos los casos, los datos serán procesados de acuerdo con la ley aplicable en los términos del artículo 4 de la Directiva 95/46/CE y de la legislación local que corresponda.

23 – Disposiciones Finales

- Fecha de entrada en vigor

- Período de transición

Documentación para proporcionar a las autoridades de protección de datos

1 - El formulario de solicitud que figura en el documento WP133.

2 - La documentación para demostrar que los compromisos contenidos en las normas corporativas vinculantes son respetados, por ejemplo:

- Políticas en materia de protección a la vida privada por el tipo de tratamiento (por ejemplo, la política de protección de la privacidad del cliente, recursos humanos, etc.) destinadas a informar a las personas interesadas (por ejemplo, clientes o empleados) sobre las medidas adoptadas por la empresa para proteger sus datos personales;
- Directrices para los empleados con acceso a datos personales y facilitarles la comprensión y aplicación de normas corporativas vinculantes (por ejemplo lineamientos sobre la forma de responder a las reclamaciones de los afectados, comunicación de la información a los interesados, o sobre las medidas a seguir en materia de seguridad y confidencialidad);
- Un plan y un programa de auditoría para la protección de los datos personales que indique a las personas competentes (controladores internos o externos autorizados por la empresa);
- Ejemplos y/o explicación del programa de capacitación;
- Documentación que acredite que la filial en donde se origina la transferencia de datos fuera de la UE, la sede europea o la filial europea responsable en materia de protección de datos disponen de recursos financieros suficientes para cubrir el pago de una indemnización por incumplimiento de las BCR;
- Descripción del sistema interno de reclamación;

- Lista de entidades vinculadas a las BCR;
- La política de seguridad aplicable en los sistemas informáticos de tratamiento de datos personales en el seno de la UE;
- El proceso de certificación para asegurar que todas las nuevas aplicaciones de software tratamiento de datos comunitarios están acordes con las BCR;
- Cualquier contrato tipo a utilizarse en las relaciones con los subtratantes (filiales o no filiales del grupo) que aseguren el tratamiento de datos comunitarios;
- Descripción del puesto de delegado para la protección de datos u otras personas responsables de la protección de datos dentro de la empresa.