

Normas Corporativas Vinculantes (“BCR”) – Resumen de derechos de terceros

Este documento contiene en sus Secciones 3 a 9 las regulaciones de las “Normas Corporativas Vinculantes (BCR) para las empresas del Grupo Siemens y otras empresas adheridas para la protección de datos de carácter personal” que son también vinculantes para el afectado, en virtud de los derechos de tercero beneficiario.

1. Propósito de las BCR

Proteger la seguridad y privacidad de los datos de carácter personal es de máxima importancia para Siemens. Por ello, Siemens realiza sus negocios en cumplimiento con la legislación aplicable sobre protección de privacidad y seguridad de datos. Las BCR son normas internas adoptadas por Siemens, esto es Siemens AG y sus empresas del grupo participadas, que proporcionan “salvaguardas adecuadas para la protección de la privacidad y los derechos y libertades fundamentales de los individuos” en el sentido de la legislación sobre protección de datos aplicable, especialmente la de los estados miembros del Espacio Económico Europeo (“EEE”).

2. Ámbito de aplicación de las BCR

Las BCR aplican al tratamiento de todos los datos de carácter personal de un afectado por parte de las empresas adheridas, establecidas fuera de un país del EEE - en la medida en que estos datos de carácter personal hayan sido transferidos desde una empresa participante establecida en un país miembro del EEE- o establecida en un país con un nivel adecuado de protección de datos reconocido mediante una decisión de la Comisión Europea, a una de las empresas participantes establecida fuera del EEE; y en un país miembro del EEE o en un país con un nivel adecuado de protección de datos reconocido mediante una decisión de la Comisión Europea.

3. Principios sustantivos para el tratamiento de datos de carácter personal

Los siguientes principios, establecidos en la Directiva de Protección de Datos 95/46/CE de la UE y la Resolución de Madrid del 5 de noviembre de 2009, se aplican al tratamiento de datos de carácter personal por parte de las empresas participantes dentro del ámbito de aplicación de las BCR:

3.1 Legitimidad y legalidad del tratamiento de datos

El tratamiento de datos de carácter personal se efectuará conforme a la ley según las disposiciones reglamentarias relevantes y atendiendo a los principios establecidos en estas BCR.

El tratamiento de datos solo se podrá efectuar si se cumple al menos uno de los siguientes requisitos:

- El afectado ha dado su consentimiento efectivo de forma inequívoca; o
- El tratamiento de datos tiene como objeto establecer una relación contractual o una relación similar de confianza con el afectado; o
- El tratamiento es necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento (a efectos de estas BCR “**responsable de tratamiento**” es la empresa que determina las finalidades y medios para el tratamiento de datos; las sucursales dependientes, delegaciones y establecimientos permanentes se consideran parte del responsable del tratamiento), siempre que no prevalezca el interés legítimo del afectado para evitar dicho tratamiento de datos; o
- El tratamiento está determinado o permitido por la legislación y regulaciones locales a las que está sujeto el responsable del tratamiento; o
- El tratamiento es necesario para el cumplimiento de una obligación jurídica a la que está sujeto el responsable del tratamiento; o
- El tratamiento es requerido, de manera excepcional, para proteger la vida, la salud y la seguridad del afectado.

El responsable del tratamiento proporcionará procedimientos simples, rápidos y eficaces que permitan al afectado retirar su consentimiento en cualquier momento.

3.2 Finalidad

Los datos de carácter personal serán tratados exclusivamente con fines determinados, explícitos y legítimos. En ningún caso los datos de carácter personal podrán ser tratados de manera incompatible con los fines legítimos para los que dichos datos de carácter personal fueron recogidos. Las empresas participantes están obligadas a ceñirse a estos fines originales durante el almacenamiento y tratamiento ulterior o durante la utilización de datos procedentes de otra empresa participante; solo es posible modificar la finalidad del tratamiento de datos con el consentimiento del afectado o en la medida en que lo permita la legislación nacional a la que esté sujeta la empresa que transfiere los datos.

3.3 Transparencia

Todas las empresas participantes efectuarán el tratamiento de datos de carácter personal de manera transparente. La empresa participante proporcionará la siguiente información a los afectados cuyos datos de carácter personal esté tratando (en consulta con la empresa que transfiere los datos, si procede):

- Identidad del responsable del tratamiento y de la empresa que transfiere los datos
- Los tipos de destinatarios o la identidad de la entidad destinataria
- Finalidad del tratamiento
- Origen de los datos (a menos que los datos de carácter personal se hayan obtenido directamente del afectado)
- Derecho de oposición del afectado al tratamiento de los datos de carácter personal para fines publicitarios
- Otra información en la medida de lo necesario por razones de equidad, como por ejemplo
 - derechos de información, rectificación y cancelación.

En la medida en que los datos de carácter personal no procedan directamente del afectado, no es necesario proporcionar dicha información (a modo de excepción), si el no proporcionar dicha información es necesario para proteger al afectado o los derechos de otros individuos, si el afectado ya ha sido informado o si esto requiriese un esfuerzo desproporcionado.

3.4 Calidad y economía de datos

Los datos de carácter personal deben ser objetivamente correctos y, en caso necesario, mantenerse actualizados. Se deberán adoptar las medidas apropiadas para asegurar que se corrijan o supriman los datos inexactos o incompletos.

El tratamiento de datos se regirá por el principio de economía de datos. El objetivo es recabar, tratar y utilizar solamente los datos de carácter personal necesarios, es decir, utilizar tan pocos datos de carácter personal como sea posible. En particular, se hará uso de la posibilidad de datos anónimos o anonimizados siempre y cuando el coste y el esfuerzo requeridos sean acordes con el fin deseado. Los estudios o evaluaciones estadísticos basados en datos anónimos o anonimizados no son relevantes en cuanto a la protección de la privacidad de datos, siempre y cuando dichos datos no puedan ser usados para identificar al afectado.

Los datos de carácter personal que ya no se requieran para los fines empresariales para los que originalmente fueron recabados y almacenados deberán de ser suprimidos. En caso de que apliquen plazos legales de conservación, los datos serán bloqueados en lugar de suprimidos.

3.5 Transferencia ulterior de datos

La transferencia de datos de carácter personal desde una empresa participante (es decir, una empresa del Grupo Siemens u otra empresa adherida) fuera del EEE solo está permitida con las siguientes condiciones:

- La entidad destinataria dispone de un nivel de protección de datos de carácter personal adecuado, definido en el artículo 25 de la Directiva de Protección de Datos 95/46/CE de la UE, por ejemplo mediante la firma de un contrato estándar de la UE (Cláusulas Contractuales Tipo para los encargados del tratamiento 2010/87/UE o Cláusulas Contractuales Tipo entre responsables de tratamiento 2001/497/CE o 2004/915/CE) o mediante cualquier otro acuerdo contractual apropiado entre la entidad emisora y la destinataria;
- La transferencia está permitida bajo las excepciones contempladas en el artículo 26 de la Directiva de Protección de Datos 95/46/CE de la UE;
- Si la entidad receptora es un encargado del tratamiento, se deben cumplir además las condiciones estipuladas en los artículos 16 y 17 de la Directiva de Protección de Datos 95/46/CE de la UE.

3.6 Categorías especiales de datos de carácter personal

Las categorías especiales de datos de carácter personal, en otras palabras, información acerca del origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, así como el tratamiento de datos relativos a la salud o a la sexualidad, no pueden ser tratados como principio general.

En caso de que se precisara el tratamiento de categorías especiales de datos de carácter personal, se deberá obtener el consentimiento explícito del afectado, a menos que

- el afectado no esté en posición de dar su consentimiento (por ejemplo, en el caso de una urgencia médica) y sea necesario el tratamiento de los datos para proteger los intereses vitales del afectado o de otro individuo; o
- el tratamiento resulte necesario en relación al diagnóstico médico, la medicina preventiva, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios, siempre que dicho tratamiento sea realizado por un profesional sanitario sujeto a la obligación de secreto profesional o por otro miembro del personal sujeto asimismo a una obligación equivalente de secreto; o
- el afectado ya haya hecho públicos los datos en cuestión; o
- el tratamiento sea necesario para el reconocimiento, ejercicio o defensa de un derecho en un procedimiento judicial, siempre y cuando no haya razones para suponer que el afectado posee intereses legítimos preponderantes para asegurarse de que no se efectúa el tratamiento de dichos datos; o
- el tratamiento esté permitido expresamente por la ley según la legislación nacional aplicable (por ejemplo, para fines de registro/protección de minorías) y se den garantías adicionales según lo dispuesto en la Directiva de Protección de Datos 95/46/CE de la UE para el tratamiento de los datos, incluyendo medidas de seguridad específicas adecuadas para estos datos.

Se deberá consultar al DPO competente de la empresa participante antes de proceder al tratamiento de categorías especiales de datos de carácter personal.

3.7 Decisiones individuales automatizadas

Si los datos de carácter personal se tratan para la toma de decisiones individuales automatizadas, se deben asegurar los intereses legítimos del afectado a través de medidas apropiadas. No se podrán tomar decisiones que tengan consecuencias legales negativas para el afectado o perjudiquen sustancialmente al afectado exclusivamente en base a un procedimiento individual automatizado diseñado para evaluar las características personales de un individuo, es decir, no se podrán tomar decisiones basadas exclusivamente en el uso de tecnologías de la información. Se aplicará una excepción solamente si la decisión

- se ha adoptado en el marco de la celebración o ejecución de un contrato, siempre que se haya satisfecho la petición de celebración o ejecución del contrato presentada por el afectado o existan medidas apropiadas para la salvaguardia de su interés legítimo, como la posibilidad de defender su punto de vista; o
- es autorizada por una ley que establece medidas que garantizan los intereses legítimos del afectado.

3.8 Seguridad de los datos

Los responsables del tratamiento deberán tomar las medidas técnicas organizativas adecuadas para garantizar la seguridad de los datos requerida, que protegen los datos de carácter personal contra la supresión, accidental o ilícita, el uso no autorizado, la alteración, contra la pérdida, la destrucción, además de contra la difusión o el acceso no autorizados. Dichas medidas deberán garantizar, habida cuenta de los conocimientos técnicos existentes y del coste de su aplicación, un nivel de seguridad apropiado en relación con los riesgos que presente el tratamiento y con la naturaleza de los datos que deban protegerse. Se proporcionará protección especial a las categorías especiales de datos de carácter personal.

Las medidas de seguridad que se habrán de proporcionar se refieren en particular a ordenadores (servidores y ordenadores en el lugar de trabajo), redes, enlaces de comunicación y aplicaciones.

Para asegurar un nivel adecuado de medidas técnicas y organizativas para la protección de datos, Siemens publicó la Guía para la Seguridad de Información Corporativa con efecto vinculante para todo el Grupo Siemens.

Las medidas específicas empleadas para asegurar una protección adecuada de los datos de carácter personal incluyen controles de: admisión, acceso al sistema, acceso a los datos, transmisión, entrada, trabajo, disponibilidad y controles de segregación.

Todos los ordenadores del lugar de trabajo, incluidos tanto dispositivos móviles como ordenadores portátiles, están protegidos por contraseña. La intranet de Siemens tiene un servicio de cortafuego (firewall) para proteger el contenido interno de la compañía del acceso externo no autorizado. La transmisión de datos de carácter personal dentro de la propia red de la empresa normalmente está encriptada, en la medida en que lo requieran la naturaleza y el fin de los datos personales.

3.9 Confidencialidad del tratamiento de los datos

Solo el personal autorizado e instruido específicamente de acuerdo con los requisitos para la protección y privacidad de datos puede recabar, tratar o utilizar datos de carácter personal. La autorización de acceso de cada empleado individual estará restringida en función de la naturaleza y el ámbito de aplicación de su campo de actividad particular. El empleado tiene prohibido el uso de datos de carácter personal para fines privados, así como transferir o facilitar el acceso a los datos de carácter personal a personas no autorizadas. En este contexto se incluyen como personas no autorizadas, por ejemplo, otros empleados, siempre y cuando no requieran los datos personales para el cumplimiento de sus funciones específicas. La obligación de confidencialidad continúa después de que finalice la relación laboral del empleado en cuestión.

3.10 Tratamiento de los datos cuya gestión se encarga a terceros

Si las empresas participantes encargan el tratamiento de datos de carácter personal a otra empresa al amparo de estas BCR, deben observarse los siguientes requisitos:

- El encargado del tratamiento deberá ser seleccionado cuidadosamente por el responsable del tratamiento; se seleccionará un encargado que pueda asegurar las medidas de seguridad técnicas y organizativas necesarias que se requieren para efectuar el tratamiento de los datos de acuerdo con las regulaciones para la protección de la privacidad de datos.
- El responsable del tratamiento asegurará y verificará de manera regular que el encargado del tratamiento sigue cumpliendo estrictamente con las medidas técnicas y organizativas acordadas.
- El tratamiento de los datos por el encargado deberá regularse mediante un contrato por escrito o documentado de otra manera, en el que se definan de manera inequívoca los derechos y obligaciones del encargado del tratamiento.
- El encargado del tratamiento debe estar obligado por contrato al tratamiento de los datos recibidos del responsable del tratamiento solamente dentro del marco contractual y de acuerdo con las instrucciones dictadas por el responsable. El tratamiento de los datos para fines propios del encargado del tratamiento o para fines de terceros deberá estar prohibido por contrato.
- El responsable del tratamiento mantiene la responsabilidad respecto a la legitimidad del tratamiento y sigue siendo la persona de contacto para el afectado.

4. Derechos sustantivos del afectado

Los afectados tienen los derechos inalienables que se enumeran a continuación respecto al tratamiento de sus datos de carácter personal por parte de una empresa participante dentro del ámbito de aplicación de estas BCR:

- El afectado puede exigir el **acceso** de forma inteligible a sus datos de carácter personal que se traten, a cualquier información disponible en relación a su fuente y a las finalidades del tratamiento. El afectado también tiene derecho de información acerca de la identidad del responsable del tratamiento y, en caso de que exista una transferencia de datos de carácter personal, el afectado también tiene derecho a ser informado sobre los destinatarios o los tipos de destinatarios. El derecho de información también aplica a la estructura lógica de las operaciones de tratamiento automatizadas, en la medida en que se refiera a decisiones automatizadas. Si la legislación local aplicable así lo estipula, el afectado no tiene derecho de información si esto supusiera un problema considerable para los fines empresariales, incluyendo específicamente si afecta a la divulgación de secretos comerciales y el interés en la salvaguardia de dichos secretos comerciales pesan más que el interés del afectado respecto a dicha divulgación. Las regulaciones legislativas locales pueden restringir el derecho de información del afectado si este derecho se ejerce de manera repetida en un periodo corto de tiempo, a menos que el afectado pueda probar una razón legítima para las peticiones repetidas de información. La empresa participante puede cobrar una tarifa razonable al afectado por proporcionar la información, en la medida en que la legislación nacional aplicable lo permita.
- El afectado puede pedir que se **rectifiquen** sus datos de carácter personal si éstos fueran incorrectos o incompletos.
- El afectado tiene derecho a requerir que sus datos de carácter personal sean **bloqueados** si no fuera posible determinar si dichos datos son correctos o incorrectos.
- El afectado tiene derecho a requerir que sus datos de carácter personal sean **cancelados** si el tratamiento de los datos fue ilícito, se ha vuelto ilícito o tan pronto como los datos no sean necesarios para los fines del tratamiento. Las peticiones justificadas por parte del afectado para la cancelación deben cumplirse dentro de un periodo de tiempo razonable, en la medida en que los plazos legales de conservación u otras obligaciones contractuales no impidan su cancelación. En el caso de la existencia de plazos legales de conservación, el afectado puede pedir que sus datos sean bloqueados en lugar de cancelados. En caso de imposibilidad para cancelar los datos, aplicará el mismo principio.
- El afectado tiene derecho a **oponerse** al tratamiento de sus datos de carácter personal para fines publicitarios o de estudios de mercado y/o encuestas de opinión. El afectado será informado de su derecho a oponerse sin coste alguno.
- El afectado también tiene un **derecho general de oposición** al tratamiento de sus datos de carácter personal si, debido a la situación personal especial del afectado, el interés legítimo del mismo tiene mayor peso que el interés legítimo del responsable del tratamiento para tratar los datos de carácter personal.

El afectado puede ejercer los derechos anteriormente mencionados por escrito ante la empresa participante, el Data Privacy Officer (DPO) de la empresa participante o el Departamento Legal & Compliance - Data Privacy - de Siemens AG. La petición justificada del afectado recibirá una respuesta de la entidad con la que se ha puesto en contacto dentro de un plazo de tiempo razonable. La respuesta se dará en forma escrita (un correo electrónico es suficiente).

5. Naturaleza vinculante para el afectado

Las regulaciones de las BCR incluidas en las secciones 3 a 9 de este documento son también vinculantes para el afectado, en virtud de los derechos de tercero beneficiario.

Los afectados pueden elegir presentar una queja por incumplimiento de las regulaciones relevantes de las BCR por parte de una empresa participante contra la misma, o bien contra Siemens AG (L CO-O DP).

Asimismo, los afectados tienen derecho a exigir el cumplimiento de cualquiera de los derechos de tercero beneficiario mencionados anteriormente por parte de una empresa participante, bien mediante la pre-

sentación de una queja ante la autoridad de protección de datos competente o mediante un recurso en el tribunal competente. Los afectados pueden pedir una indemnización por daños.

Los afectados pueden elegir presentar dicha queja

- ante la jurisdicción de la empresa participante que ha transferido los datos; o
- ante la jurisdicción de la sede de Siemens AG; o
- ante la autoridad de protección de datos competente.

Esto significa que en caso de un incumplimiento de las regulaciones de las BCR por parte de una empresa participante establecida fuera del EEE, los tribunales y autoridades del EEE también tienen competencia. El afectado tiene los mismos derechos frente a una empresa participante que ha aceptado esta responsabilidad, que si dicho incumplimiento hubiera sido cometido por una empresa participante establecida en un país miembro del EEE.

Sin embargo, la competencia de los tribunales y autoridades del EEE descrita anteriormente no aplica si el destinatario está establecido en un país fuera del EEE pero dicho país no tiene un nivel de protección de datos adecuado reconocido mediante una decisión de la Comisión de la Unión Europea.

Para asegurar que los afectados disfruten de los derechos de tercero beneficiario exigibles legalmente también en esos países donde la concesión de derechos de tercero beneficiario en el documento de las BCR pudiera ser insuficiente, Siemens AG redactará, en la medida de lo necesario, acuerdos contractuales adicionales con las empresas participantes relevantes para permitirlos. En la Declaración de Compromiso se incluye una cláusula de derechos de tercero beneficiario que confiere al afectado los derechos necesarios, que las empresas del grupo firman para expresar su aceptación y aplicación de las BCR. Lo mismo aplica para el Acuerdo de Adhesión que las otras empresas adheridas firman con Siemens AG.

6. Proceso de gestión de quejas

Los afectados pueden contactar en cualquier momento con el departamento competente de gestión de quejas de Siemens AG (L CO-O DP; para los detalles de contacto, consultar la Sección 9) o la persona de contacto local competente para la protección de datos de la empresa participante (por regla general el DPO) para tratar quejas sobre el incumplimiento de las BCR por parte de una empresa participante o relativas a cualquier otra cuestión. Se dará al afectado una pronta confirmación de la recepción de la queja en la entidad contactada y la queja deberá ser procesada dentro de un periodo de tres (3) meses desde la recepción de la misma. Este marco de tiempo se podrá exceder de manera razonable en caso de retrasos no atribuibles a empresas del Grupo Siemens u otras empresas adheridas, como por ejemplo en caso de que el afectado no proporcione en tiempo la información razonablemente necesaria.

Los empleados involucrados en la gestión de las quejas en el departamento competente se benefician de un nivel de independencia apropiado en el ejercicio de esta función.

En caso de que se realice una investigación, la empresa participante y L CO-O DP están obligados a cooperar con las autoridades de protección de datos del país y a respetar sus opiniones.

7. Asistencia mutua y cooperación con las autoridades de protección de datos

Siemens AG y las empresas participantes cooperarán en un marco de confianza y se apoyarán mutuamente en caso de investigaciones o quejas por parte de los afectados en relación a incumplimientos de las BCR.

Siemens AG y las empresas participantes se comprometen además a cooperar en el referido marco de confianza con las autoridades de protección de datos competentes en el ámbito de aplicación de las BCR. Responderán a las peticiones relacionadas con las BCR de la autoridad de protección de datos dentro de un marco de tiempo y de forma apropiados, y seguirán los consejos y decisiones de la autoridad de protección de datos competente en lo relativo a la aplicación de las BCR.

8. Relación entre las BCR y las normativas legales locales

La legitimidad del tratamiento de datos de carácter personal se juzga en base a la legislación local aplicable. Siempre que dicha legislación estipule un nivel de protección de datos de carácter personal mayor que el establecido en estas BCR, el tratamiento de datos se efectuará de acuerdo con la legislación aplicable. Cada empresa participante deberá comprobar individualmente (como por ejemplo por parte del responsable de protección de datos o el departamento legal) si existen dichas normativas legales (como por ejemplo leyes sobre la privacidad de datos) y asegurará la conformidad con las mismas. Si la legislación local proporciona un nivel de protección de datos menor que el de las BCR, entonces se aplicarán las presentes BCR.

En el caso de que las obligaciones derivadas de la legislación local aplicable estén en conflicto con estas BCR, la empresa participante habrá de informar al Departamento Legal & Compliance - Data Privacy - (L CO-O DP) de Siemens AG sin demora injustificada. L CO-O DP dejará constancia del conflicto del que se ha informado.

L CO-O DP informará sobre el conflicto entre las BCR y la legislación local a todas las empresas participantes que hayan transferido datos previamente a la empresa en cuestión. L CO-O DP también informará a la autoridad de protección de datos competente del conflicto regulador y, junto con la autoridad de protección de datos competente y la empresa participante, buscará una solución práctica que se acerque lo máximo posible a los principios de la Directiva de Protección de Datos 95/46/CE de la UE.

9. Responsabilidad

Siemens AG asume la responsabilidad por el incumplimiento de las BCR por parte de las empresas participantes establecidas fuera del EEE. Siemens AG se compromete a controlar el cumplimiento de las BCR por parte de las empresas participantes establecidas fuera del EEE y a asegurar que dichas empresas llevan a cabo las acciones correctivas necesarias para reparar los incumplimientos de las BCR.

Siemens AG además se compromete a pagar una indemnización por daños en caso de que se pruebe que ha habido un incumplimiento de las BCR que haya resultado en la violación de los derechos del afectado.

La carga de la prueba incumbe a Siemens AG. Siemens AG demostrará que no ha habido un incumplimiento de las BCR o que la empresa participante establecida fuera del EEE no es responsable del incumplimiento de las BCR sobre el que se basa la reclamación del afectado.

10. Contacto

Los afectados pueden dirigir sus dudas al DPO de la empresa participante correspondiente o a la Dirección de Protección de Datos de Siemens AG.

Siemens AG

L CO-O DP

St.-Martin-Str. 76

D-81541 Munich

Tel.: +49 (0) 89 636- 34141

Fax: +49 (0) 89 636-...

E-mail: datenschutz@siemens.com

Internet: <http://www.siemens.com>