Normas corporativas vinculantes de la UE de Amgen – Controlador (BCR de la UE)

Última actualización: 12 de Diciembre de 2023

Introducción

(A) Amgen es una empresa líder en biotecnología comprometida con el servicio a pacientes con enfermedades graves. Estas Normas Corporativas Vinculantes de la UE – Controlador ("**BCR de la UE**") expresan el compromiso de Amgen con la privacidad y la protección de datos, ya que se esfuerza por proporcionar una protección adecuada para las transferencias y el procesamiento de Datos Personales entre las empresas miembro.

(B) Todas las empresas miembros de Amgen y todo el personal se comprometen a respetar estas BCR de la UE y están legalmente obligados por ellas con respecto a los datos personales dentro del ámbito de aplicación de las BCR de la UE. El incumplimiento puede dar lugar a sanciones disciplinarias, según lo permitido por la legislación local. El Director de Cumplimiento, en colaboración con el Director de Privacidad, garantiza el cumplimiento de las BCR de la UE. Se puede encontrar una lista de las empresas miembro aquí: https://wwwext.amgen.com/-/media/Themes/CorporateAffairs/amgen-com/amgen-com/downloads/amgen-bcr/amgen-BCRs-participating-companies.pdf. Puede ponerse en contacto con todas las empresas miembro en privacy@amgen.com para cualquier pregunta relacionada con estas BCR de la UE.

(C) Estas BCR de la UE se han adoptado en referencia a las Leyes de Protección de Datos de la UE. Amgen Francia es responsable de garantizar el cumplimiento de estas BCR de la UE por parte de las Empresas Miembro. Las personas físicas pueden hacer valer estas BCR de la UE contra Amgen Francia como tercero beneficiario, tal y como se describe a continuación. Estas BCR de la UE están disponibles en el sitio web de Amgen: www.amgen.com/bcr. También puede ponerse en contacto con Amgen en privacy@amgen.com para solicitar una copia.

1. Ámbito de aplicación

1.1. Las BCR de Amgen EU se aplican a las transferencias y al procesamiento, automatizado o manual, de todos los datos personales de los interesados realizados por una empresa miembro que actúe como Controlador o que actúe como Procesador para otra Empresa miembro que actúe como Controlador en cualquiera de los siguientes casos:

1.1.1. la empresa miembro que Procesa los Datos Personales está establecida en la UE; o

1.1.2. la empresa miembro que Procesa los Datos Personales no está establecida en el EEE y ha recibido los Datos Personales de una empresa miembro establecida en el EEE; o

1.1.3. a las transferencias posteriores de datos personales desde Importadores de Datos a Importadores de Datos.

1.2. En el anexo 1 figura una visión general de los flujos de datos de conformidad con estas BCR de la UE.

2. Definiciones

Termino	*Definiciones*
Amgen Francia	Amgen S.A.S., compañía constituida en Francia con domicilio registrado en 25 quai du Président Paul Doumer, 92400 Courbevoie.
Legislación aplicable	La legislación de la UE y/o (según corresponda) la legislación nacional o local de los estados miembros del EEE (incluidas, entre otras, las leyes de protección de datos de la UE).
Líder de Cumplimiento	Una persona dentro de la división de Cumplimiento del Cuidado de la Salud del departamento de Cumplimiento Mundial y Ética Empresarial de una Empresa Miembro que ha oficial la responsabilidad de la protección de datos y la privacidad y, a diferencia del Oficial de Protección de Datos local, apoya al Oficial de Protección de Datos local con sus responsabilidades y tareas.
Consentimiento	Cualquier indicación libre, específica, informada e inequívoca de los deseos de un Interesado, por el que el Interesado, mediante una declaración o una clara acción afirmativa, manifiesta su acuerdo con el procesamiento de los datos personales que le conciernen.
Controlador de datos	Cualquier entidad que tome decisiones con respecto a la recopilación y el procesamiento de datos personales, incluidas las decisiones sobre los fines y la forma en que se procesan los datos personales.
Exportador de datos	Una empresa miembro que opera como Controlador de datos establecida en el EEE y que transfiere datos personales a un importador de datos.
Importador de datos	Una empresa miembro que no esté establecida en el EEE y que (a) reciba datos personales de un exportador de datos o (b) reciba una transferencia posterior de datos personales de conformidad con el Artículo 1(c) de estas BCR de la UE.
Procesador de datos	Una persona o entidad que procesa datos personales en nombre de un controlador de datos.
Autoridad de Protección de Datos (DPA)	Una autoridad pública independiente de protección de datos establecida por un Estado Miembro del EEE.
Oficial de Protección de Datos	Una persona que ha sido asignada por el Director de Privacidad de Amgen como responsable de la supervisión de la privacidad y la protección de datos a nivel local, así como de la implementación de los controles apropiados y requeridos.
Interesado	Una persona física que puede ser identificada, directa o indirectamente, por referencia a datos personales. Un interesado puede ser (sin limitación): • un paciente/sujeto de datos de ensayos clínicos (que puede incluir un niño menor de 18 años)

Termino	*Definiciones*
	• un profesional de la salud • un empleado • un vendedor o proveedor
AEMA	Los Estados miembros de la Unión Europea (Alemania, Austria, Bélgica, Bulgaria, Croacia, Dinamarca, Eslovaquia, Eslovenia, España, Estonia, Finlandia, Francia, Grecia, Hungría, Irlanda, Italia, Letonia, Lituania, Luxemburgo, Malta, Países Bajos, Polonia, Portugal, República Checa, Rumanía y Suecia) e Islandia, Liechtenstein y Noruega (todos ellos "**Estados miembros del EEE**").
Leyes de protección de datos de la UE	GDPR y (según corresponda) la legislación local o nacional relativa a la protección de datos y el procesamiento de datos personales y la aplicación del GDPR de un Estado miembro del EEE pertinente.
GDPR	El Reglamento General de Protección de Datos ((UE) 2016/679).
Empresa miembro	Una entidad jurídica del grupo Amgen que está sujeta a las BCR de la UE.
Datos personales	Cualquier información relativa a un interesado, como un nombre, un número de identificación, datos de localización, un identificador en línea o a uno o varios factores específicos o información relativa a la identidad física, fisiológica, genética, mental, económica, cultural o social de esa persona física. Entre los ejemplos de datos personales se pueden incluir los siguientes: • El nombre, la dirección, el número de seguro social, el número de licencia de conducir, la información de la cuenta financiera, la información familiar o los datos médicos de un sujeto de datos. • El nombre, la educación profesional y las prácticas de prescripción de un profesional de la salud, • La dirección de correo electrónico y otra información de identificación proporcionada por alguien que visita un sitio web de Amgen. La lista anterior es solo indicativa y no exhaustiva.
Filtración de datos personales	Cualquier violación de la seguridad que conduzca a la destrucción, pérdida, alteración, divulgación no autorizada o acceso accidental o ilegal de los datos personales transmitidos, almacenados o procesados de otro modo.
Personal	Todos los miembros del personal y los trabajadores eventuales (incluidos consultores, trabajadores de agencias temporales y trabajadores eventuales) de cualquier empresa miembro.

Termino	*Definiciones*
Procesamiento	Cualquier operación o conjunto de operaciones que se realice sobre Datos Personales (o conjuntos de Datos Personales), ya sea por medios automatizados o no, como la recopilación, el registro, la organización, la estructuración, el almacenamiento, la adaptación o alteración, la recuperación, la consulta, el uso, la divulgación por transmisión, la difusión o cualquier otra forma de puesta a disposición, la alineación o combinación, la restricción, la eliminación o la destrucción.
Datos Personales Sensibles	Datos personales que revelen el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el procesamiento de datos genéticos, datos biométricos con el fin de identificar de forma única a una persona física, datos relativos a la salud o datos relativos a la vida sexual u orientación sexual de una persona física. Independientemente de las Leyes de Protección de Datos de la UE, Amgen también considera la información financiera y la información que podría utilizarse para perpetrar el robo de identidad (por ejemplo, el número de la Seguridad Social, el número de licencia de conducir, la tarjeta de crédito u otra información de la cuenta bancaria) como Datos Personales Confidenciales.
Medidas de seguridad técnicas y organizativas	Medidas tecnológicas y organizativas destinadas a proteger los Datos Personales contra la destrucción accidental o ilícita o la pérdida accidental, alteración, divulgación o acceso no autorizados, en particular cuando el Procesamiento implique la transmisión de datos a través de una red, y contra todas las demás formas ilícitas de procesamiento.
Terceros	Una persona física o jurídica, autoridad pública, agencia o cualquier otro organismo que no sea el interesado, la Empresa Miembro que actúe como controlador o una Empresa Miembro que actúe como procesador. En Amgen, un proveedor se considera un tercero. Dependiendo de las circunstancias, un tercero puede actuar como controlador de datos o procesador de datos en relación con el procesamiento de datos personales.
Proveedor	Cualquier persona física o jurídica, empresa u organización que proporcione bienes y/o servicios a una Empresa Miembro en virtud de una relación contractual y/o sea receptora de Datos Personales de dicha Empresa Miembro con el fin de prestar dichos bienes y/o servicios.

Amgen interpretará los términos de estas BCR de la UE de acuerdo con las Leyes de Protección de Datos de la UE.

3. Limitación del propósito

3.1. Los datos personales se tratarán para fines explícitos, especificados y legítimos de conformidad con el artículo 5, apartado 1, letra b) del GDPR.

3.2. Los datos personales no serán procesados de manera que sean incompatibles con los fines legítimos para los que se recopilaron los datos personales o la ley aplicable. Los importadores de datos están obligados a cumplir con los propósitos originales cuando almacenen y/o procesen datos personales o procesen datos personales que serán transferidos a otra empresa miembro. La finalidad del procesamiento de los datos personales solo podrá modificarse con el consentimiento del interesado o en la medida en que lo permita la legislación aplicable.

3.3. Los datos personales confidenciales contarán con medidas de seguridad adicionales, como las previstas por las leyes de protección de datos de la UE.

4. Calidad y proporcionalidad de los datos

4.1. Los datos personales deben ser exactos y, cuando sea necesario, mantenerse actualizados; se deben tomar todas las medidas razonables para garantizar que los datos personales que sean inexactos, teniendo en cuenta los fines para los que se procesan, se eliminen o rectifiquen sin demora.

4.2. Los datos personales serán adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son procesados, de conformidad con el artículo 5, apartado 1, letra c) del GDPR.

4.3. El procesamiento de datos personales se guiará por el objetivo de limitar la recopilación, el procesamiento y/o el uso de datos personales únicamente a lo necesario, es decir, a la menor cantidad posible. Se debe considerar la posibilidad de datos anonimizados o seudónimos, siempre que el costo y el esfuerzo involucrados sean proporcionales al propósito deseado.

4.4. Los datos personales que ya no sean necesarios para el propósito comercial para el que se recopilaron y almacenaron originalmente deben eliminarse de acuerdo con el programa de retención de registros de Amgen. En el caso de que se apliquen períodos de retención legales o retenciones legales, los datos se bloquearán en lugar de eliminarse. Al final del período de retención o de la retención legal, los datos se eliminarán.

5. Fundamento Legal para el procesamiento de datos personales

5.1. El procesamiento de datos personales solo está permitido si se cumple al menos uno de los siguientes requisitos previos:

5.1.1. El interesado ha dado su consentimiento para el procesamiento de sus datos personales para uno o más fines específicos.

5.1.2. El procesamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para tomar medidas a petición del interesado antes de celebrar un contrato.

5.1.3. El procesamiento es necesario para el cumplimiento de una obligación legal a la que está sujeto el controlador en virtud de la Ley Aplicable.

5.1.4. El procesamiento es necesario para proteger los intereses vitales, como la vida, la salud o la seguridad, del interesado o de otra persona física.

5.1.5. El procesamiento es necesario para el cumplimiento de una tarea realizada en interés público o en el ejercicio de la autoridad pública conferida al controlador.

5.1.6. El procesamiento es necesario para los fines de los intereses legítimos perseguidos por el controlador o por un tercero, excepto cuando dichos intereses sean anulados por los intereses o los derechos y libertades fundamentales del interesado.

5.2. El procesamiento de datos personales relacionados con condenas y delitos penales se llevará a cabo únicamente cuando el procesamiento esté autorizado por la legislación aplicable que proporcione las garantías adecuadas para los derechos y libertades de los interesados.

6. Procesamiento de Datos Personales Sensibles

6.1. Si, de acuerdo con una finalidad específica y legítima, la empresa miembro necesita procesar datos personales sensibles, la empresa miembro solo lo hará si:

6.1.1. El interesado ha dado su consentimiento explícito para el procesamiento de esos datos personales sensibles para uno o más fines específicos, excepto cuando la ley aplicable disponga que la prohibición del artículo 9, apartado 1, del GDPR no puede ser levantada por el interesado.

6.1.2. El procesamiento es necesario para el cumplimiento de las obligaciones y derechos específicos del controlador en el ámbito del derecho laboral, de la seguridad social y de la protección social, en la medida en que esté autorizado por la ley aplicable o por un convenio colectivo de conformidad con la ley aplicable que prevea garantías adecuadas para los derechos fundamentales y los intereses del Interesado.

6.1.3. El procesamiento es necesario para proteger los intereses vitales del interesado o de otra persona física cuando el interesado sea física o jurídicamente incapaz de dar su consentimiento.

6.1.4. El procesamiento se lleva a cabo en el curso de sus actividades legítimas con las garantías adecuadas por parte de una fundación, asociación o cualquier otra entidad sin ánimo de lucro con fines políticos, filosóficos, religiosos o sindicales y a condición de que el procesamiento se refiera únicamente a los miembros del organismo o a las personas que tengan contacto regular con él en relación con sus fines y que los datos no se divulguen fuera de dicho organismo sin el consentimiento de los interesados.

6.1.5. El procesamiento se refiere a datos personales sensibles que son manifiestamente hechos públicos por el interesado.

6.1.6. El procesamiento de datos personales sensibles es necesario para la formulación, el ejercicio o la defensa de reclamaciones legales.

6.1.7. El procesamiento es necesario por razones de interés público sustancial, sobre la base de la ley aplicable que será proporcionada al objetivo perseguido, respetará la esencia del derecho a la protección de datos y preverá medidas adecuadas y

específicas para salvaguardar los derechos fundamentales y los intereses del interesado.

6.1.8. El procesamiento de los datos personales sensibles es necesario para fines de medicina preventiva u ocupacional, para la evaluación de la capacidad de trabajo del empleado, el diagnóstico médico, la prestación de atención o procesamiento sanitario o social o la gestión de sistemas y servicios de atención sanitaria o social sobre la base de la ley aplicable o de conformidad con un contrato con un profesional de la salud, y cuando esos datos personales sensibles sean procesados por o bajo la responsabilidad de un profesional de la salud, dicho profesional debe estar sujeto a la obligación de secreto profesional en virtud de la ley aplicable o de las normas establecidas por los organismos competentes de un Estado miembro del EEE o por otra persona también sujeta a una obligación de secreto en virtud de la Ley Aplicable o de las normas establecidas por los organismos competentes de un Estado miembro del EEE.

6.1.9. El procesamiento de datos personales sensibles es necesario por razones de interés público en el ámbito de la salud pública, como la protección contra amenazas transfronterizas graves para la salud o la garantía de altos niveles de calidad y seguridad de la asistencia sanitaria y de los medicamentos o productos sanitarios, sobre la base de la legislación aplicable que establece medidas adecuadas y específicas para salvaguardar los derechos y libertades del interesado, en particular, el secreto profesional.

6.1.10. El procesamiento de datos personales sensibles es necesario para fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos de conformidad con el artículo 89, apartado 1, del GDPR sobre la base de la ley aplicable, que serán proporcionales al objetivo perseguido, respetarán la esencia del derecho a la protección de datos y preverán medidas adecuadas y específicas para salvaguardar los derechos fundamentales y los intereses del interesado.

7. Derechos transparencia e información

7.1. Todas las empresas miembro tratarán los datos personales de forma transparente. Amgen se compromete a hacer que las BCR de la UE, incluida la información de contacto, estén disponibles y sean fácilmente accesibles para todos los interesados, así como a informar a los interesados de la transferencia y el procesamiento de sus datos personales. Estas BCR de la UE están disponibles en el sitio web de Amgen: www.amgen.com/bcr. También puede ponerse en contacto con Amgen en privacy@amgen.com para solicitar una copia. Amgen también utilizará diversos medios de comunicación, como sitios web corporativos, incluidos sitios web internos y boletines informativos, contratos y avisos de privacidad específicos para cumplir con este requisito de accesibilidad. Además, Amgen informará a los interesados, a través de estos medios de comunicación, de cualquier actualización o cambio en las BCR de la UE o en la lista de empresas miembro sin demora indebida.

7.2. A los interesados cuyos datos personales sean procesados por una empresa miembro se les proporcionará la información establecida en los artículos 13 y 14 del GDPR.

7.3. Cuando los datos personales no se reciban de un interesado, la obligación de informar al interesado no se aplica si el suministro de dicha información resulta imposible o supondría un esfuerzo desproporcionado o si el registro o la divulgación están expresamente establecidos por la ley.

8. Derechos de acceso, rectificación, supresión y limitación de datos

8.1. Todo interesado tiene derecho a obtener la confirmación de la empresa miembro sobre si se están tratando o no datos personales que le conciernen y, en caso afirmativo, el acceso a los datos personales y a la información que debe facilitarse en virtud del artículo 15, apartado 1, del GDPR. El seguimiento de esta solicitud, incluida la posibilidad de cobrar una tarifa o el plazo para responder a dicha solicitud, estará sujeto a la ley aplicable y se comunicará adecuadamente al interesado cuando presente su solicitud.

8.2. Todo interesado tiene derecho a obtener la rectificación, supresión o limitación de los datos personales, en particular cuando los datos sean incompletos o inexactos.

8.3. Todo interesado tiene derecho a oponerse, en cualquier momento por motivos relacionados con su situación particular, al procesamiento de sus datos personales basado en el desempeño de una tarea realizada en interés público o en los intereses legítimos de la empresa miembro o de un tercero (incluida la elaboración de perfiles basada en dichos motivos). La empresa miembro dejará de tratar los datos personales a menos que demuestre motivos legítimos imperiosos para el procesamiento que prevalezcan sobre los intereses, derechos y libertades del interesado o para la formulación, el ejercicio o la defensa de reclamaciones legales.

8.4. Todo interesado tiene derecho a oponerse (de forma gratuita) al procesamiento de los datos personales que le conciernen con fines de marketing directo, lo que incluye la evaluación por su perfil en que esté relacionado con dicho marketing directo. Cuando el interesado ejerza su derecho a oponerse al procesamiento de los datos personales que le conciernen con fines de marketing directo, la empresa miembro deberá cesar en el procesamiento de los datos personales con ese fin.

8.5. Todo interesado tiene derecho a obtener la notificación de los terceros a los que se les han divulgado los datos personales, sobre cualquier rectificación, supresión o restricción, de conformidad con el artículo 19 del GDPR.

8.6. Todo Interesado tiene derecho a conocer la lógica implicada en cualquier procesamiento automatizado de datos personales, de conformidad con el artículo 13, apartado 2, letra f) del GDPR.

8.7. Cuando el procesamiento se basa en el consentimiento, todo interesado tiene derecho a retirar su consentimiento en cualquier momento. El cesé del consentimiento no afectará a la legalidad del procesamiento basado en el consentimiento antes de sea retirado.

8.8. Todo Interesado tiene derecho a presentar una reclamación ante la empresa miembro en relación con el procesamiento de datos personales a través del mecanismo interno de reclamación previsto en el artículo 17.

8.9. Cualquier solicitud en virtud de este Artículo 8 (o del Artículo 9 a continuación) debe enviarse a la empresa miembro a: privacy@amgen.com. Si bien se recomienda encarecidamente realizar solicitudes por correo electrónico, esto no impide que un interesado realice una solicitud verbal. La empresa miembro informará al interesado sin demora del resultado de su solicitud y, a más tardar, en el plazo de un mes a partir de la recepción de la solicitud (incluidos, en su caso, los motivos por los que no se ha tomado ninguna medida y la posibilidad de presentar una reclamación ante la APD competente y/o de interponer un recurso judicial). Dicho plazo de un mes podrá prorrogarse por dos meses más en caso necesario, teniendo en cuenta la complejidad y el número de las solicitudes. La empresa miembro informará al

interesado de dicha prórroga en el plazo de un mes a partir de la recepción de la solicitud, junto con los motivos del retraso. Cualquier comunicación, acción y/o información proporcionada en relación con una solicitud en virtud de este Artículo 8 (o del Artículo 9 a continuación) se proporcionará al interesado de forma gratuita. Cuando las solicitudes de un interesado sean manifiestamente infundadas o excesivas, en particular debido a su carácter repetitivo, la empresa miembro podrá: (a) cobrar una tarifa razonable teniendo en cuenta los costes administrativos de proporcionar la información o la comunicación o de realizar la acción solicitada; o (b) negarse a dar curso a la solicitud. La empresa miembro asumirá la carga de demostrar el carácter manifiestamente infundado o excesivo de la solicitud.

9. Decisiones individuales automatizadas

9.1. El Interesado tendrá derecho a no ser objeto de una decisión basada únicamente en el procesamiento automatizado, incluida la evaluación de perfil, que produzca efectos jurídicos que le conciernan o le afecten significativamente de manera similar, a menos que dicha decisión:

9.1.1. sea necesaria para la celebración o ejecución de un contrato entre el interesado y la empresa miembro;

9.1.2. sea requerida o autorizada por la ley aplicable, que también establece medidas adecuadas para salvaguardar los derechos y libertades del interesado y los intereses legítimos (incluido al menos el derecho a obtener la intervención humana por parte de la empresa miembro, a expresar su punto de vista y a impugnar la decisión); o

9.1.3. se basa en el consentimiento explícito del interesado.

10. Seguridad y confidencialidad

10.1. Amgen implementa las medidas de seguridad técnicas y organizativas adecuadas para proteger y detectar las violaciones de los datos personales. Amgen utiliza marcos internacionales, como la norma ISO/IEC 27002, para determinar estas medidas de seguridad.

10.2. Amgen cuenta con procesos para garantizar que las filtraciones de datos personales estén sujetas a informes, seguimiento y acciones correctivas adecuadas, según sea necesario. Cualquier filtración de datos personales se documentará (incluidos los hechos relacionados con la filtración de datos personales, sus efectos y las medidas correctivas tomadas) y la documentación se pondrá a disposición de la APD competente que la solicite. Las empresas miembro notificarán sin demora indebida cualquier filtración de datos personales a Amgen Francia, al Director de Privacidad y a los demás responsables/funciones de privacidad relevantes, y (cuando la empresa miembro que sufra una filtración de datos personales actúe como procesador de datos) a la empresa miembro que actúa como controlador. Las violaciones de datos personales se notificarán, junto con el director de privacidad, a la APD competente sin demora indebida (y, cuando sea posible, a más tardar 72 horas después de tener conocimiento de la filtración de datos personales), a menos que sea poco probable que suponga un riesgo para los derechos y libertades de los interesados. Cuando la filtración de la seguridad de los datos personales pueda suponer un alto riesgo para los derechos y libertades de los interesados, también se notificará a los interesados sin demora indebida.

10.3. Las evaluaciones de riesgos de seguridad de la información se utilizan para identificar posibles amenazas a los datos personales confidenciales y la implementación de controles de seguridad adicionales según corresponda.

10.4. La aplicación de las medidas tendrá en cuenta el estado de la técnica, de conformidad con el artículo 32 del GDPR.

10.5. El Director de Seguridad de la Información trabaja juntamente con el Director de Privacidad para garantizar la seguridad y confidencialidad de los datos personales.

10.6. Las medidas de seguridad técnicas y organizativas estarán diseñadas para implementar los principios de protección de datos en virtud del artículo 5 del GDPR, la protección de datos desde el diseño y los principios por defecto de conformidad con el artículo 25 del GDPR y para facilitar el cumplimiento de los requisitos establecidos por estas BCR de la UE en la práctica.

11. Relaciones con los procesadores de datos (importador o proveedor de datos de Amgen)

11.1. La empresa miembro (que actúa como controlador) elegirá cuidadosamente un procesador de datos que puede ser otra empresa miembro o un proveedor. El procesador deberá ofrecer garantías suficientes respecto a sus medidas de seguridad técnicas y organizativas que rijan el procesamiento a realizar y deberá velar por el cumplimiento de dichas medidas.

11.2. Cuando la subcontratación se considere necesaria después de evaluar las necesidades y los riesgos empresariales de dicha subcontratación, el proceso de elección del procesador incluirá una evaluación de los factores de riesgo de privacidad y equilibrará las necesidades comerciales con los riesgos potenciales.

11.3. La empresa miembro que actúe como controlador, utilizando medios contractuales escritos, de conformidad con la ley aplicable (y en particular los requisitos del artículo 28, apartado 3, del GDPR), dará instrucciones al procesador que, entre otras cosas:

11.3.1. el procesador actuará únicamente siguiendo las instrucciones de la empresa miembro que actúa como controlador y que está prohibido el procesamiento de datos personales para fines propios del procesador o para los fines de un tercero;

11.3.2. sobre las normas relativas a la seguridad y confidencialidad que incumben al procesador y a la aplicación de las medidas técnicas y organizativas adecuadas para garantizar un nivel de seguridad adecuado al riesgo del procesamiento;

11.3.3. las personas autorizadas para procesar los datos personales se han comprometido a mantener la confidencialidad o están sujetas a una obligación legal de confidencialidad adecuada;

11.3.4. el procesador no contratará a otro procesador sin la autorización previa, específica o general por escrito de la empresa miembro que actúa como controlador y, cuando se otorgue dicha autorización, se impondrán a ese otro procesador las mismas obligaciones de protección de datos que se establecen en el contrato u otro acto jurídico entre la empresa miembro que actúa como controlador y el procesador;

11.3.5. teniendo en cuenta la naturaleza del procesamiento, deberá apoyar a la empresa miembro que actúa como controlador mediante medidas técnicas y organizativas adecuadas, en la medida de lo posible, para el cumplimiento de la obligación de la

empresa miembro de responder a las solicitudes de ejercicio de los derechos del interesado;

11.3.6. debe ayudar a la empresa miembro que actúa como controlador a garantizar el cumplimiento de las obligaciones relativas a la seguridad del procesamiento, la notificación de una filtración de datos personales a la APD competente, la comunicación de una filtración de datos personales al interesado, las evaluaciones de impacto de la protección de datos y la consulta previa con la APD competente, teniendo en cuenta la naturaleza del procesamiento y la información disponible para el procesador;

11.3.7. a elección de la empresa miembro que actúe como controlador, deberá eliminar o devolver todos los datos personales a la empresa miembro, que actúa como controlador, una vez finalizada la prestación de los servicios relacionados con el procesamiento, y eliminar las copias existentes, a menos que la ley de protección de datos de la UE exija el almacenamiento de los datos personales;

11.3.8. deberá poner a disposición de la empresa miembro que actúa como controlador toda la información necesaria para demostrar el cumplimiento de las obligaciones establecidas en el presente artículo 11 y permitir y contribuir a las auditorías, incluidas las inspecciones, realizadas por la empresa miembro que actúa como controlador u otro auditor designado por ella.

11.4. La empresa miembro que actúe como controlador se asegurará de que el procesador siga cumpliendo plenamente con las medidas de seguridad técnicas y organizativas acordadas.

11.5. La empresa miembro que actúa como controlador conserva la responsabilidad de la legitimidad del procesamiento y sigue siendo responsable de los derechos del interesado. En la medida en que el procesador esté sujeto a las leyes de protección de datos de la UE, también será responsable de sus obligaciones y responsabilidades como procesador en virtud de dichas leyes.

11.6. Con el fin de cumplir con las obligaciones contractuales establecidas en este artículo sobre los procesadores de datos, se proporciona una plantilla contractual titulada Programa de Privacidad de Datos para su uso por parte de las empresas miembro que actúan como controladores de datos. La empresa miembro que actúa como controlador podrá, en función de las circunstancias específicas de cada acuerdo contractual, negociar disposiciones diferentes a las establecidas en el Anexo de Privacidad de Datos, pero las disposiciones contractuales deberán seguir cubriendo, como mínimo, las obligaciones establecidas anteriormente en este Artículo 11.

11.7. Cada empresa miembro que actúe como procesador de datos y que esté sujeta a las Leyes de Protección de Datos de la UE debe mantener un registro de todas las categorías de actividades de procesamiento llevadas a cabo en nombre de una empresa miembro que actúe como controlador de datos. Este registro debe mantenerse por escrito, incluso en formato electrónico, se pondrá a disposición del Director de Privacidad y de la APD competente que lo soliciten, y contendrá la siguiente información: (a) el nombre y los datos de contacto de la empresa miembro que actúa como procesador y de cada empresa miembro que actúa como controlador en nombre de la cual actúe, y, en su caso, su representante y DPO; (b) las categorías de Procesamiento realizadas en nombre de cada Empresa Miembro que actúe como Controlador; y (c) cuando corresponda, transferencias de Datos Personales a un tercer país u

organización internacional, incluida la identificación de ese tercer país u organización internacional y, en el caso de transferencias que se acojan a una excepción en virtud del artículo 49 del GDPR, documentación de las garantías adecuadas; y d) cuando sea posible, una descripción general de las medidas de seguridad técnicas y organizativas.

12. Restricciones a las transferencias y transferencias posteriores

12.1. Todas las transferencias de datos personales sujetas a estas BCR de la UE por terceros ubicados fuera del EEE respetarán las Leyes de Protección de Datos de la UE sobre transferencias y transferencias posteriores de datos personales, ya sea haciendo uso de las cláusulas contractuales estándar autorizadas en virtud de la Decisión de Aplicación de la Comisión (UE), el 4 de junio de 2021, sobre cláusulas contractuales para la transferencia de datos personales a países terceros de conformidad con el GDPR o por otros medios adecuados de acuerdo con el GDPR, al Capítulo V del GDPR (incluyendo, excepcionalmente, si se aplica una excepción a una situación específica de conformidad con el artículo 49 del GDPR).

12.2. Todas las transferencias de datos personales sujetas a estas BCR de la UE a procesadores de datos ubicados fuera del EEE deberán respetar las Leyes de Protección de Datos de la UE relacionadas con los procesadores (y los requisitos establecidos en el Artículo 11 anterior), además de las normas sobre transferencias y transferencias posteriores de datos personales establecidas en este Artículo 12 y en las Leyes de Protección de Datos de la UE.

12.3. Antes de transferir datos personales a un importador de datos o (con respecto a las transferencias en curso) antes de que entre en vigor cualquier legislación nacional local actualizada, el exportador de datos, junto con el Director de Privacidad y Amgen Francia, con el apoyo del importador de datos y teniendo en cuenta las circunstancias de la transferencia, evaluará si la legislación nacional local impedirá que el importador de datos cumpla con sus obligaciones en virtud de las BCR de la UE y determinará si alguna deben aplicarse las medidas complementarias necesarias. Dicha evaluación tendrá en cuenta:

12.3.1. las circunstancias específicas de la transferencia (incluidos los fines para los que se transfieren y procesan los datos personales, los tipos de entidades involucradas en el procesamiento, el sector económico en el que se produce la transferencia, las categorías y el formato de los datos personales transferidos, la ubicación del procesamiento (incluido el almacenamiento) y los canales de transmisión utilizados);

12.3.2. las leyes y prácticas del país de destino pertinentes a la vista de las circunstancias específicas de la transferencia (incluidas las que exigen la divulgación de datos a las autoridades públicas o la autorización de acceso por parte de dichas autoridades) y las limitaciones y garantías aplicables; y

12.3.3. cualquier garantía contractual, técnica u organizativa pertinente establecida con respecto a la transferencia, incluidas las medidas aplicadas durante la transmisión y el procesamiento de los datos personales en el país de destino.

Además, dicha evaluación se basará en el entendimiento de que las leyes y prácticas del país de destino respetan los derechos y libertades fundamentales del interesado y no exceden de lo necesario y proporcionado en una sociedad democrática para salvaguardar uno de los siguientes objetivos: a) seguridad nacional; b) defensa; c) seguridad pública; d) la prevención, investigación, detección o enjuiciamiento de infracciones penales o la ejecución de sanciones penales, incluida la protección y la prevención de amenazas a la seguridad pública; e) otros objetivos importantes de interés público general, en particular intereses económicos o

financieros importantes, incluidos los asuntos monetarios, presupuestarios y fiscales, la salud pública y la seguridad social; f) la protección de la independencia judicial y de los procedimientos judiciales; g) la prevención, investigación, detección y enjuiciamiento de las infracciones éticas de las profesiones reguladas; h) las funciones de control, inspección o regulación relacionadas con el ejercicio del poder público en los casos contemplados en los objetivos anteriores; (i) la protección del interesado o de los derechos y libertades de terceros; y/o (j) la ejecución de reclamaciones de derecho civil.

El Director de Privacidad revisará y aprobará la evaluación documentada y las medidas complementarias propuestas. Cuando el resultado de la evaluación demuestre la necesidad de implementar medidas complementarias, el exportador de datos implementará dichas medidas. Si no se pueden implementar medidas complementarias (o si así lo indica el Director de Privacidad o un DPA competente), el exportador de datos suspenderá la transferencia. El resultado de la evaluación y las medidas complementarias propuestas se registrarán y se facilitarán a la APD competente cuando sea necesario.

El Director de Privacidad y Amgen Francia informarán a todas las empresas miembro de la evaluación realizada y de sus resultados, con el fin de que las medidas complementarias identificadas puedan aplicarse cuando otras empresas miembro realicen el mismo tipo de transferencias o, cuando no puedan establecerse medidas complementarias efectivas, dichas transferencias se suspendan o finalicen.

12.4. El importador de datos notificará sin demora al exportador de datos, a Amgen Francia y al Director de Privacidad si tiene motivos para creer que está o ha estado sujeto a leyes o prácticas que le impedirían cumplir con sus obligaciones en virtud de estas BCR de la UE, incluso a raíz de un cambio en las leyes nacionales locales del país destino, tal como se describe en el artículo 12.3, o de una medida como una solicitud de divulgación, tal como se describe en el artículo 12.3. 16.3. Además, los exportadores de datos (junto con el Director de Privacidad) supervisarán, de forma continua, y cuando corresponda con la asistencia de los importadores de datos, los desarrollos en los países destino a los que los exportadores de datos hayan transferido datos personales que puedan afectar negativamente la evaluación inicial del nivel de protección de los datos personales y las decisiones tomadas con respecto a dichas transferencias.

12.5. Tras la suspensión de una transferencia, el exportador de datos debe poner fin a la transferencia o al conjunto de transferencias si no puede cumplir con las BCR de la UE y/o si el cumplimiento no se restablece en el plazo de un mes a partir de la suspensión. En tal caso, el importador de datos deberá, a elección del exportador de datos, devolver o destruir todos los datos personales que hayan sido transferidos antes de la suspensión, y cualquier copia de estos.

12.6. Cualquier flujo de datos personales que no esté sujeto a estas BCR de la UE y/o que no se origine en una empresa miembro establecida en un estado miembro del EEE no se considera una transferencia de datos personales en virtud de estas BCR de la UE y, en consecuencia, no está sujeto a los requisitos de estas BCR de la UE.

13. Programa de Capacitación

13.1. Tal y como se describe en el Anexo 2, Amgen proporciona a todo el personal una capacitación adecuada y actualizada sobre los principios de privacidad y, más concretamente, sobre las BCR de la UE. Esta capacitación también incluye información sobre las consecuencias en virtud de

la legislación penal y laboral y/o su contrato de servicios para el personal que incumpla las BCR de la UE.

13.2. La capacitación es obligatoria y se repite anualmente. Se documentará la participación exitosa en la capacitación.

13.3. Se impartirán capacitaciones específicas caso por caso al personal que tenga acceso permanente o regular a los datos personales, o que participe en la recopilación de datos personales o en el desarrollo de herramientas utilizadas para el procesamiento de datos personales.

13.4. Además, el equipo de Cumplimiento de Privacidad Global de Amgen proporcionará información y recursos apropiados relacionados con la privacidad, incluso en el portal de intranet de Amgen.

14. Programa de Auditoría y Monitoreo

14.1. El Director de Privacidad se asegurará de que todas las empresas miembro (y su cumplimiento con estas BCR de la UE) estén incluidas en el programa de auditoría y monitoreo desde una perspectiva de privacidad y protección de datos. Las auditorías exhaustivas se llevan a cabo de forma periódica, con una frecuencia no inferior a 2 a 3 años (para las empresas miembro con un perfil de riesgo medio-alto basado en la metodología de evaluación de riesgos del departamento de auditoría) y cada 4 a 5 años (para las empresas miembro con un perfil de riesgo bajo basado en la metodología de evaluación de riesgos del departamento de auditoría), por el equipo de auditoría interna o auditores externos independientes certificados. Las auditorías exhaustivas incluyen asuntos de protección de datos y privacidad dentro de su ámbito de aplicación (incluido el cumplimiento de estas BCR de la UE, cuando corresponda y sea utilizado por una empresa miembro). Además de las auditorías exhaustivas, y sin perjuicio de los plazos establecidos anteriormente, se llevan a cabo otros ámbitos de auditoría, incluidas auditorías multifuncionales o de cuestiones específicas (por ejemplo, el cumplimiento de las BCR de la UE), una auditoría limitada de uno o más sistemas de procesamiento de datos personales y/o una auditoría limitada de uno o más departamentos funcionales (por ejemplo, el equipo de Cumplimiento de Privacidad Global). El programa de auditoría se desarrolla y acuerda en cooperación con el Director Ejecutivo de Auditoría y el Director de Cumplimiento, que es un Vicepresidente Sénior. El Director de Privacidad, el Director de Cumplimiento y el Director de Información pueden iniciar auditorías ad hoc relacionadas con las BCR de la UE en cualquier momento. Por ejemplo, en respuesta a cualquier problema de cumplimiento identificado o un informe de incumplimiento sustancial, una filtración de datos personales y/o un cambio sustantivo en las leyes de protección de datos de la UE. El programa de auditoría abarca todos los aspectos de las BCR de la UE, incluidos los métodos para garantizar que se adopten medidas correctivas.

14.2. Todos los informes de auditoría de las BCR de la UE se comunican al Director de Cumplimiento y al Director de Privacidad de manera oportuna. Los resúmenes y resultados de las auditorías de las BCR de la UE, así como otra información relevante, también se comunican periódicamente al Consejo de Administración de Amgen Inc. a través de los comités apropiados (por ejemplo, el Comité de Responsabilidad Corporativa y Cumplimiento y/o el Comité de Consejo de Auditoría), al Consejo de Administración de Amgen Francia y (cuando corresponda, por ejemplo, en relación con un hallazgo que requiera remediación) a la Sociedad Miembro correspondiente. El Comité de Responsabilidad Corporativa y Cumplimiento de la Junta Directiva de Amgen, Inc. se reúne cinco veces al año. La privacidad y la protección de datos se tratan anualmente, normalmente en la reunión de Octubre.

14.3. La APD competente puede recibir una copia de los informes de auditoría relacionados con las BCR de la UE si así lo solicita.

14.4. Cada empresa miembro cooperará y aceptará, sin restricciones, ser auditada por la APD competente. Cada entidad auditada debe informar inmediatamente al Director de Privacidad si recibe notificación de dicha auditoría o si se lleva a cabo dicha auditoría.

15. Cumplimiento y Supervisión del Cumplimiento

15.1. Amgen designa al personal adecuado, incluida, cuando corresponda, una red de oficiales de protección de datos, con el apoyo de la alta dirección para supervisar y garantizar el cumplimiento de las normas de protección de datos. El Director de Privacidad está a cargo del Equipo de Cumplimiento de Privacidad Global, que es un equipo global que brinda soporte experto en todo el mundo a las entidades de Amgen (incluidas las empresas miembro).

15.2. En Amgen, las responsabilidades del Director de Privacidad, entre otras, incluyen:

15.2.1. asesorar al consejo de administración;

15.2.2. garantizar el cumplimiento de la protección de datos a nivel mundial (incluida la responsabilidad general de las BCR de la UE);

15.2.3. informar periódicamente sobre el cumplimiento de la protección de datos (incluido el Director de Cumplimiento); y

15.2.4. trabajar con las investigaciones de la APD competente.

15.3. El Equipo Global de Cumplimiento de Privacidad incluye al Director de Privacidad (quien, además de las responsabilidades mencionadas anteriormente, supervisa la red global de Oficiales de Protección de Datos), el Oficial Europeo de Protección de Datos y otros Oficiales de Protección de Datos locales. El Equipo Global de Cumplimiento de Privacidad tiene la responsabilidad general de la protección de datos y el cumplimiento de la privacidad de todo el mundo en Amgen.

15.4. El Oficial Europeo de Protección de Datos ha sido nombrado por Amgen como Oficial de Protección de Datos para el EEE, el Reino Unido y Suiza. El Oficial Europeo de Protección de Datos tiene las funciones establecidas en el artículo 39 del GDPR. Amgen se asegurará de que las tareas y deberes del Oficial Europeo de Protección de Datos no den lugar a un conflicto de intereses con dichas tareas. El Oficial Europeo de Protección de Datos tiene una línea directa de reporte con el Director de Privacidad (que forma parte del nivel más alto de la dirección de Amgen) y cuenta con el apoyo del Responsable de Cumplimiento local en Francia. El responsable europeo de la protección de datos podrá ponerse en contacto con el Director de Protección de Datos si surge alguna pregunta o problema durante el ejercicio de sus funciones. Puede ponerse en contacto con el Oficial Europeo de Protección de Datos en: privacy@amgen.com

15.5. A nivel local, los Oficiales de Protección de Datos son responsables de manejar las solicitudes de privacidad local de los interesados, de garantizar el cumplimiento a nivel local con el apoyo del Equipo Global de Cumplimiento de Privacidad y de informar sobre los principales problemas de privacidad al Director de Privacidad. Amgen mantiene una red de Oficiales de Protección de Datos y se asegura de que se designe o asigne un DPO para cada país en el que

Amgen tenga una entidad corporativa (la empresa miembro) y la legislación aplicable de la jurisdicción de dicha empresa miembro exija dicho nombramiento.

15.6. Por lo general, los Oficiales de Protección de Datos son, o cuentan con el apoyo de, los Líderes de Cumplimiento locales que dependen del departamento de Cumplimiento Global y Ética Empresarial. El Equipo de Cumplimiento de Privacidad Global forma parte del departamento de Cumplimiento Global y Ética Empresarial, que está dirigido por el Director de Cumplimiento. El Director de Cumplimiento tiene la responsabilidad general del cumplimiento legal y normativo del grupo Amgen en todo el mundo. En raras ocasiones, debido a las circunstancias específicas de una empresa miembro u otras circunstancias especiales, el Oficial de Protección de Datos puede provenir de otra función, por ejemplo, Regulatoria. En cualquier caso, el Equipo Global de Cumplimiento de Privacidad se asegurará de que los Responsables de Protección de Datos y los Responsables de Cumplimiento estén debidamente formados y tengan un nivel de gestión y experiencia suficientes para desempeñar su función. Además, los Oficiales de Protección de Datos tienen una línea de reporte directa con el Director de Privacidad y cuentan con el apoyo del Personal del Equipo de Cumplimiento de Privacidad Global en caso de que necesiten orientación adicional.

15.7. Toda empresa miembro que actúe como responsable del procesamiento de datos será responsable y podrá demostrar el cumplimiento de las BCR de la UE. Como parte de este requisito, todas las empresas miembro:

15.7.1. debe mantener un registro de todas las categorías de actividades de procesamiento realizadas de acuerdo con los requisitos establecidos en el artículo 30, apartado 1, del GDPR. Este registro deberá mantenerse por escrito, incluso en formato electrónico, se pondrá a disposición del Director de Privacidad y del DPO competente cuando lo soliciten, y contendrá la siguiente información: (a) el nombre y los datos de contacto de la empresa miembro que actúe como controlador, su representante y el DPO; (b) los fines del procesamiento; (c) una descripción de las categorías de interesados y de las categorías de datos personales; (d) las categorías de destinatarios a los que se han divulgado o divulgarán los datos personales, incluidos los destinatarios de países terceros u organizaciones internacionales; e) en su caso, transferencias de datos personales a un tercer país o a una organización internacional, incluida la identificación de dicho país u organización internacional y, en el caso de transferencias que se acojan a una excepción, la documentación de las garantías adecuadas; (f) cuando sea posible, los plazos previstos para la supresión de las diferentes categorías de datos personales; y (g) cuando sea posible, una descripción general de las medidas de seguridad técnicas y organizativas.

15.7.2. llevar a cabo evaluaciones de impacto de la protección de datos para las operaciones de procesamiento que puedan suponer un alto riesgo para los derechos y libertades de las personas físicas de conformidad con el artículo 35 del GDPR. Cuando una evaluación de impacto de protección de datos en virtud del artículo 35 indique que el procesamiento daría lugar a un alto riesgo en ausencia de medidas adoptadas por la empresa miembro para mitigar el riesgo, se debe consultar al Director de Privacidad antes del procesamiento, quien a su vez consultará con la autoridad de protección de datos competente de conformidad con el artículo 36 del GDPR.

16. Acciones en caso de que la legislación nacional impida el respeto de las BCR de la UE

16.1. Cuando una empresa miembro tenga motivos para creer que las leyes que le son aplicables le impiden cumplir con sus obligaciones en virtud de las BCR de la UE o tienen un efecto sustancial

en las garantías previstas en las normas, informará de inmediato al Director de Privacidad (excepto cuando lo prohíba una autoridad policial, como la prohibición penal de preservar la confidencialidad de una investigación policial) y Amgen Francia.

16.2. En caso de conflicto entre la legislación nacional local y los compromisos de las BCR de la UE, el Director de Privacidad, en colaboración con el asesor jurídico local y el Oficial de Protección de Datos local, determinará qué medidas jurídicamente apropiadas son necesarias. Si es necesario, el Director de Privacidad también consultará con la APD competente.

16.3. Cuando cualquier requisito legal al que esté sujeta una empresa miembro en un país tercero pueda tener un efecto adverso sustancial en las garantías proporcionadas por las BCR de la UE, el importador de datos notificará sin demora al Director de Privacidad, Amgen Francia y al exportador de datos, y el Director de Privacidad notificará a la APD competente y (cuando sea posible) a los interesados. Esto incluye (a) cualquier solicitud legalmente vinculante de divulgación de los datos personales por parte de una autoridad policial o un organismo de seguridad del estado y, en tal caso, se debe informar claramente a la APD competente sobre la solicitud, incluida la información sobre los datos solicitados, el organismo solicitante y la base legal para la divulgación y la respuesta proporcionada (a menos que se prohíba lo contrario, como la prohibición en virtud del derecho penal de preservar la confidencialidad de una investigación policial), y (b) cualquier acceso directo por parte de las autoridades públicas a los datos personales transferidos de conformidad con estas BCR de la UE de conformidad con las leyes del país de destino y, en tal caso, dicha notificación incluirá toda la información disponible para dicha empresa miembro (a menos que se prohíba lo contrario, como la prohibición en virtud del derecho penal de preservar la confidencialidad de una investigación policial).

16.4. Si en casos específicos se prohíben la suspensión y/o notificación, la empresa miembro que reciba la solicitud hará todo lo posible para obtener el derecho a renunciar a esta prohibición con el fin de comunicar la mayor cantidad de información posible y lo antes posible y poder demostrar (a solicitud del exportador de datos) que lo hizo.

16.5. El importador de datos proporcionará al exportador de datos, a intervalos regulares, la mayor cantidad de información relevante posible sobre las solicitudes recibidas (en particular, el número de solicitudes, el tipo de datos personales solicitados, la identidad de las autoridades solicitantes, si las solicitudes han sido impugnadas y el resultado de dichas impugnaciones). El importador de datos conservará dicha información durante el tiempo que los datos personales estén sujetos a las garantías previstas por las BCR de la UE y la pondrá a disposición de la APD competente cuando ésta lo solicite. Si al importador de datos se le prohíbe o se le prohíbe parcial o totalmente proporcionar al exportador de datos la información anterior, el importador de datos, sin demora indebida, informará al exportador de datos en consecuencia.

16.6. El importador de datos, junto con el Director de Privacidad, revisará la legalidad de una solicitud de divulgación por parte de una autoridad pública para determinar si se encuentra dentro de los poderes otorgados a la autoridad pública solicitante. El importador de datos impugnará la solicitud si, después de dicha evaluación, concluye (junto con el Director de Privacidad) que existen motivos razonables para considerar que la solicitud es ilegal según las leyes del país de destino, las obligaciones aplicables en virtud del derecho internacional y/o los principios de cortesía internacional. Si el importador de datos cree que existen motivos razonables para considerar que la solicitud es ilegal, buscará posibilidades de apelación. Al impugnar una solicitud, el importador de datos solicitará medidas provisionales con el fin de suspender los efectos de la solicitud hasta que la autoridad judicial competente se haya pronunciado sobre el fondo de esta. El importador de datos no divulgará los datos personales

solicitados hasta que se le exija hacerlo en virtud de la legislación aplicable y las normas de procedimiento del país de destino. El importador de datos documentará su evaluación legal y cualquier impugnación de la solicitud de divulgación y, en la medida en que lo permitan las leyes del país de destino, pondrá la documentación a disposición del exportador de datos y, previa solicitud, de la APD competente.

16.7. El importador de datos proporcionará la cantidad mínima de información permitida al responder a una solicitud de divulgación, sobre la base de una interpretación razonable de la solicitud.

16.8. En todo caso, las transferencias de datos personales por parte de una empresa miembro a cualquier autoridad pública no serán masivas, desproporcionadas e indiscriminadas de forma que vayan más allá de lo necesario en una sociedad democrática.

16.9. En el caso de las Empresas miembro ubicadas en el EEE, cualquier sentencia de un juzgado o tribunal y cualquier decisión de una autoridad administrativa de un país tercero que exija a un controlador o procesador de datos que transfiera o divulgue datos personales solo podrá ser reconocida o ejecutable de cualquier manera si se basa en un acuerdo internacional, como un tratado de asistencia judicial mutua, vigente entre el país tercero solicitante y la UE o un Estado miembro del EEE, sin perjuicio de otros motivos de transferencia de conformidad con el Capítulo V del GDPR.

17. Mecanismos internos de denuncia

17.1. Amgen utilizará su proceso de gestión de reclamaciones existente para incorporar la gestión de cualquier queja o inquietud relacionada con las BCR de la UE.

17.2. Cualquier interesado puede levantar una reclamación, en cualquier momento, de que una empresa miembro no está cumpliendo con las BCR de la UE. Dichas quejas serán gestionadas por el Equipo de Cumplimiento de Privacidad Global bajo la dirección del Director de Privacidad y en cooperación con el Oficial de Protección de Datos local correspondiente.

17.3. Amgen recomienda que dichas quejas se presenten por escrito, ya sea por correo postal o correo electrónico directamente al Equipo de Cumplimiento de Privacidad Global o a la empresa miembro. Puede ponerse en contacto con el Equipo de Cumplimiento de Privacidad Global utilizando los datos de contacto que se indican a continuación:

Dirección: 25 quai du Président Paul Doumer, 92400 Courbevoie.

Correo electrónico: privacy@amgen.com

17.4. El personal de Amgen podrá, cuando sea aceptable de acuerdo con las leyes aplicables a la empresa miembro, utilizar la línea directa de conducta empresarial para presentar una queja ante las BCR de la UE.

17.5. Si la queja es recibida localmente por la empresa miembro, el DPO traducirá, si es necesario, y la remitirá sin demora indebida al Equipo Global de Cumplimiento de Privacidad.

17.6. Se proporcionará una respuesta inicial al titular dentro de los diez (10) días hábiles informándole que su queja está siendo examinada y que recibirá una respuesta sustantiva sin demora indebida y, en cualquier caso, dentro del plazo de un mes a partir de la recepción de la solicitud. Teniendo en cuenta la complejidad y el número de solicitudes, el plazo de un mes

podrá ampliarse por un máximo de dos meses más, en cuyo caso se informará al interesado en consecuencia. La respuesta sustantiva incluirá detalles sobre nuestros hallazgos y cualquier acción que Amgen tenga o se proponga tomar. Si Amgen determina que no se debe tomar ninguna medida, se explicará al interesado junto con los motivos de esta determinación.

17.7. Si Amgen confirma la reclamación, Amgen implementará las medidas correctivas adecuadas. Dichas medidas serán decididas caso por caso por el Director de Privacidad y el Equipo Global de Cumplimiento de la Privacidad, el DPO local y, cuando corresponda, cualquier otro departamento relevante. Además, si el Equipo Global de Cumplimiento de la Privacidad descubre irregularidades individuales, se tomarán las medidas disciplinarias adecuadas, que pueden incluir la rescisión del empleo o del compromiso, en la medida en que lo permita la ley aplicable.

17.8. El interesado recibirá una respuesta informándole del resultado de su reclamación. Esto se hará sin demora indebida y, en cualquier caso, en el plazo de un mes a partir de la recepción de la reclamación (con detalles suficientes para que Amgen pueda identificar la naturaleza de la reclamación y, solo cuando sea razonablemente necesario, con cualquier información solicitada para confirmar la identidad del denunciante). Teniendo en cuenta la complejidad y el número de solicitudes, el plazo de un mes podrá ampliarse por un máximo de dos meses más, en cuyo caso se informará al Interesado en consecuencia.

17.9. Se informará al interesado de que, si no está satisfecho con la respuesta de Amgen, puede presentar una reclamación ante los tribunales de un Estado miembro del EEE o ante la APD competente. Sin embargo, no es un requisito que un interesado pase primero por el proceso de tramitación de reclamaciones de Amgen antes de poder presentar una reclamación ante la APD competente o presentar una reclamación ante los tribunales de un estado miembro del EEE.

17.10. Este proceso de tramitación de reclamaciones se hará público a través de la publicación de las BCR de la UE, tal como se menciona en el artículo 7 anterior.

18. Derechos y responsabilidad de terceros beneficiarios

18.1. Un interesado cuyos datos personales se originen en el EEE o estén protegidos por las Leyes de Protección de Datos de la UE y se transfieran a empresas miembro fuera del EEE tendrá derecho a hacer cumplir las BCR de la UE como tercero beneficiario y tendrá derecho a solicitar reparación judicial, obtener recursos y, cuando corresponda, compensación por los daños reales sufridos como resultado del incumplimiento de estas BCR de la UE. Cualquiera de estas reclamaciones puede ser presentada por el interesado ante un DPA competente (que puede ser el DPA en el estado miembro del EEE en el que el interesado reside habitualmente, o el DPA de su lugar de trabajo o el DPA del lugar de la presunta infracción). Los interesados también pueden presentar una reclamación ante un tribunal competente de un Estado miembro del EEE (que pueden ser los tribunales del Estado miembro del EEE en el que la empresa miembro en cuestión tenga un establecimiento o los tribunales del estado miembro del EEE en el que el Interesado tenga su residencia habitual). Un interesado podrá ser representado en el ejercicio de su derecho a un recurso judicial efectivo contra una empresa miembro por un organismo, organización o asociación sin ánimo de lucro, siempre que dicho organismo, organización o asociación se haya constituido correctamente de conformidad con la ley aplicable, tenga objetivos estatutarios de interés público y esté activo en el ámbito de la protección de los derechos y libertades de los interesados en relación con la protección de sus datos personales. El interesado podrá hacer cumplir los siguientes artículos como tercero beneficiario:

18.1.1. los artículos 1 (Ámbito de aplicación), 2 (Definiciones), 3 (Limitación de la finalidad), 4 (Calidad y proporcionalidad de los datos), 5 (Base jurídica para el procesamiento de datos personales) y 6 (Procesamiento de datos personales sensibles);

18.1.2. Artículo 7 (Derechos de transparencia e información);

18.1.3. los artículos 8 (derechos de acceso, rectificación, supresión y limitación de datos) y 9 (decisiones individuales automatizadas);

18.1.4. Artículo 10 (Seguridad y Confidencialidad), 11 (Relaciones con Procesadores de Datos (Importador o Proveedor de Datos de Amgen) y 12 (Restricción de Transferencias y Transferencias Ulteriores);

18.1.5. los artículos 16 (Acciones en caso de legislación nacional que impida el respeto de las BCR de la UE) y 21 (Relación entre las legislaciones nacionales y las BCR de la UE);

18.1.6. Artículo 18 (Derechos y responsabilidad de terceros beneficiarios); y

18.1.7. Artículo 19 (Asistencia mutua y cooperación con las APD).

18.2. Para evitar dudas, los derechos de terceros beneficiarios no se extienden a los artículos y elementos de estas BCR de la UE que se refieren a los mecanismos internos implementados dentro de las empresas miembro o del grupo Amgen, como los detalles relativos a la formación (incluido el Anexo 2), los programas de auditoría, las redes y la estructura internas de cumplimiento y el mecanismo para actualizar las BCR de la UE.

18.3. Amgen Francia asume la responsabilidad y se compromete a tomar las medidas que sean razonablemente necesarias para remediar los actos de las empresas miembro establecidas fuera del EEE. Amgen Francia pagará una indemnización por cualquier daño material o inmaterial resultante de la filtración de estas BCR de la UE, a menos que pueda demostrar que la empresa miembro establecida fuera del EEE no es responsable del evento que dio lugar al daño. Amgen Francia dispone de medios financieros y seguros suficientes para cubrir los daños y perjuicios en virtud de las BCR de la UE.

18.4. Cualquier interesado que haya sufrido daños derivados de un incumplimiento de estas BCR de la UE por parte de una empresa miembro no establecida en el EEE tiene derecho, en su caso, a recibir una indemnización de Amgen Francia por los daños sufridos y los tribunales u otras autoridades competentes del EEE tendrán jurisdicción. El interesado tendrá los derechos y recursos contra Amgen Francia como si la filtración hubiera sido causada por Amgen Francia en la UE en lugar de la empresa miembro no establecida en el EEE. Si la empresa miembro no establecida en el EEE es responsable o se le considera responsable de dicho incumplimiento, indemnizará a Amgen Francia por cualquier coste, cargo, daño, gasto o pérdida en la que incurra Amgen Francia en relación con dicho incumplimiento.

18.5. En caso de que un interesado reclame que ha sufrido daños y ha demostrado que es probable que dichos daños se hayan producido debido a un incumplimiento de estas BCR de la UE, la carga de la prueba para demostrar que los daños sufridos por el interesado debido a un incumplimiento de estas BCR de la UE no son atribuibles a la empresa miembro pertinente recaerá en Amgen Francia. Si Amgen Francia puede demostrar que la empresa miembro

establecida fuera del EEE no es responsable del hecho causante del daño, no será responsable del daño.

19. Asistencia mutua y cooperación con las Autoridades de Protección de Datos (APD)

19.1. Las empresas miembro cooperarán y se asistirán mutuamente para gestionar una solicitud o queja de un interesado o una investigación o consulta por parte de la APD competente.

19.2. Las empresas miembro responderán, en colaboración con el Director de Privacidad, a las solicitudes relacionadas con las BCR de la UE de la APD competente dentro de un plazo adecuado en vista de las circunstancias de la solicitud (y, en cualquier caso, a más tardar en cualquier plazo impuesto por la APD competente) y con el detalle adecuado basado en la información razonablemente disponible para la empresa miembro. En relación con la implementación y la aplicación en curso de las BCR de la UE, las empresas miembro prestarán la debida consideración a las comunicaciones y recomendaciones de la APD competente y cumplirán con cualquier decisión formal o notificación emitida por la APD competente.

19.3. Cualquier disputa relacionada con el ejercicio de supervisión del cumplimiento de estas BCR de la UE por parte de una APD competente será resuelta por los tribunales del estado miembro de dicha APD, de conformidad con la Ley Aplicable de ese Estado miembro.

20. Actualizaciones y cambios de las BCR de la UE

20.1. Amgen se reserva el derecho de modificar y/o actualizar estas BCR de la UE en cualquier momento. Dicha actualización de las BCR de la UE puede ser necesaria específicamente como resultado de nuevos requisitos legales, cambios significativos en la estructura del grupo Amgen o requisitos oficiales impuestos por la APD competente.

20.2. Amgen informará de inmediato y sin demoras indebidas de cualquier cambio significativo en las BCR de la UE o en la lista de empresas miembro, a todas las demás empresas miembro y a la APD competente para tener en cuenta las modificaciones de la ley aplicable, el entorno normativo y/o la estructura del grupo Amgen. En particular, cuando una modificación afecte al nivel de protección ofrecido por las BCR de la UE, el Director de Protección de la Privacidad comunicará sin demora dicha modificación por adelantado a la APD competente con una breve explicación de los motivos de la modificación. Algunas modificaciones pueden requerir una nueva aprobación de la ADP competente.

20.3. El Director de Privacidad mantendrá una lista completamente actualizada de las empresas miembro de las BCR de la UE y realizará un seguimiento de cualquier actualización de las normas, así como proporcionará la información necesaria a los interesados o a la APD competente que lo solicite. Cualquier cambio administrativo en las BCR de la UE se informará a las empresas miembro de forma periódica.

20.4. No se realizará ninguna transferencia de datos personales a una nueva empresa miembro bajo las garantías de las BCR de la UE hasta que la nueva empresa miembro esté efectivamente obligada por las BCR de la UE y de conformidad con las BCR de la UE.

20.5. Cualquier cambio administrativo en las BCR de la UE o en la lista de empresas miembro se informará a las empresas miembro de forma periódica y se notificará al menos una vez al año a la APD competente con una breve explicación de los motivos de la actualización.

20.6. Las modificaciones sustanciales de las BCR de la UE también se comunicarán a los interesados por cualquier medio de conformidad con el artículo 7 de las BCR de la UE.

21. Relación entre las legislaciones nacionales y las BCR de la UE

21.1. Cuando las leyes nacionales locales aplicables a una empresa miembro exijan un mayor nivel de protección de los datos personales, ésta tendrá prioridad sobre las BCR de la UE. Si las leyes nacionales locales aplicables a una empresa miembro proporcionan un nivel de protección de los datos personales inferior al de las BCR de la UE, se aplicarán las BCR de la UE.

21.2. En caso de que las obligaciones derivadas de las leyes nacionales locales aplicables a una empresa miembro entren en conflicto con las BCR de la UE, la empresa miembro informará al Director de Privacidad sin demora indebida y cumplirá con los requisitos adicionales establecidos en el Artículo 16 anterior.

21.3. En cualquier caso, los datos personales se tratarán de conformidad con el artículo 5 del GDPR y la legislación local pertinente.

22. Disposiciones finales

22.1. Las BCR de la UE entrarán en vigor a partir de la aprobación por parte de la APD competente y serán aplicables a las empresas miembro en el momento de la firma del Acuerdo de Adopción de las BCR de la UE.

22.2. No se realizará ninguna transferencia a una empresa miembro a menos que esté obligada por estas BCR de la UE. Cuando un importador de datos deje de estar obligado por las BCR de la UE, deberá devolver o eliminar de inmediato todos los datos personales (incluidas las copias de los mismos) que se hayan transferido en virtud de estas BCR de la UE, excepto que, siempre que el importador de datos proporcione obligaciones legalmente vinculantes para mantener la protección de los datos personales de acuerdo con el capítulo V del GDPR, podrá retener los datos personales que se hayan transferido en virtud de estas BCR de la UE.

22.3. El importador de datos debe informar sin demora al exportador de datos, a Amgen Francia y al Director de Privacidad si no puede, por cualquier motivo, cumplir con estas BCR de la UE (incluidas las situaciones descritas en el Artículo 12.3 anterior). Cuando el importador de datos incumpla estas BCR de la UE o no pueda cumplirlas, deberá notificar al Director de Privacidad y suspender la transferencia de datos personales.

22.4. A elección del exportador de datos, el importador de datos deberá devolver o eliminar inmediatamente todos los datos personales (incluidas las copias de los mismos) que hayan sido transferidos en virtud de estas BCR de la UE, y deberá certificar lo mismo al exportador de datos, cuando:

22.4.1. el exportador de datos ha suspendido la transferencia de datos personales, y el cumplimiento de estas BCR de la UE no se restablece dentro de un plazo razonable y, en cualquier caso, dentro de un mes a partir de la suspensión; o

22.4.2. el importador de datos está incumpliendo sustancialmente estas BCR de la UE; o

22.4.3. el importador de datos no cumple con una decisión vinculante de un tribunal competente o de un DPA competente con respecto a sus obligaciones en virtud de estas BCR de la UE.

Hasta que los datos personales hayan sido eliminados o devueltos, el importador de datos debe seguir garantizando el cumplimiento de estas BCR de la UE. Si las leyes nacionales locales aplicables al importador de datos prohíben la devolución o eliminación de los datos personales transferidos en virtud de estas BCR de la UE, el Importador de datos debe seguir garantizando el cumplimiento de estas BCR de la UE y solo procesar los datos personales en la medida y durante el tiempo que lo exijan dichas leyes nacionales locales.

23. Anexos

Los anexos adjuntos forman parte integrante de las BCR de la UE.

Anexo 1: Descripción general de los flujos de datos de Amgen

Anexo 2: Descripción general del programa de formación de Amgen

Anexo 1: Descripción general de los flujos de datos de Amgen

Interesados	Categorías de datos	Propósitos	Transferencia
Empleado	Datos de identificación como nombre, dirección, fecha y lugar de nacimiento, fecha de contratación, números de seguro social, números de tarjetas de crédito, información financiera y de cuentas bancarias, y números de licencia de conducir y tarjeta de identificación emitida por el gobierno Vacaciones y beneficios, quejas, bonificaciones, promociones, revisiones y evaluaciones, registros de trabajo, información relacionada con la cobertura de salud y bienestar, planes de jubilación y detalles de opciones sobre acciones Información personal fiscal y financiera Datos sensibles, como el origen nacional, cuando lo permita la legislación local	Fines de gestión de personal, soporte y administración de tecnología de la información en relación con la relación laboral y los beneficios, o la administración de los beneficios posteriores al empleo, así como para cumplir con las obligaciones legales, administrativas y corporativas de Amgen.	Las bases de datos globales de Amgen se encuentran en los EE. UU., donde se encuentra la sede central de Amgen Inc. Los datos fluyen de Amgen Francia (o el exportador de datos correspondiente) a Amgen Inc. en los Estados Unidos o a las empresas miembro en Suiza. Posteriormente, los datos pueden: - simplemente se almacenan y mantienen allí - ser analizados para proporcionar estadísticas e informes globales - ser compartidos dentro del grupo Amgen con otras empresas miembro cuando exista una necesidad comercial de dicho acceso por parte de personal específico o funciones comerciales en esas empresas miembro (por ejemplo, un empleado que solicita un trabajo fuera de su país o que tiene que informar a un gerente con sede fuera de su país). En la mayoría de los casos,
Profesionales de la salud	Nombre, información de contacto comercial, incluido el número de teléfono y la dirección de correo electrónico, campo de especialización Trayectoria profesional (hoja de vida) Participación en otras investigaciones Información financiera (información de facturación y pago)	Administración y gestión de las actividades profesionales y científicas de Amgen – Investigación y Desarrollo (por ejemplo, participación en investigaciones médicas, estudios clínicos, reuniones profesionales o congresos) Promoción de los productos y servicios de Amgen Divulgación de información financiera cuando lo exija la ley aplicable o el cumplimiento del código de la industria Cumplimiento normativo, como la supervisión de la seguridad y la notificación de eventos adversos	

Vendedores / Proveedores	Nombre de la persona, nombre de la organización, información de contacto de la empresa Información de facturación y pago	Procesamiento de pagos a vendedores y proveedores Cumplimiento normativo, como la legislación fiscal	dichas empresas miembro actuarán como controladores del procesamiento, pero en función de las necesidades del negocio, las empresas miembro también pueden actuar como controladores del procesamiento de datos (por ejemplo, en la prestación de asistencia técnica de TI o en la prestación de asistencia relacionada con el Centro de Servicios HR Connect).
Sujetos de datos de ensayos clínicos (que pueden incluir niños menores de 18 años cuando haya un paciente pediátrico involucrado en un estudio clínico patrocinado por Amgen).	Datos codificados: el nombre del paciente y la información de contacto se sustituyen por un número de identificación generado internamente. Solo el centro del ensayo clínico (hospital/centro de investigación) mantiene la lista para vincular el número de identificación con el nombre del paciente. Identificadores indirectos como el año o la fecha de nacimiento (la fecha completa de nacimiento solo se recopila para estudios pediátricos), el sexo, el peso y la altura. Datos de salud necesarios como se describe en el protocolo del estudio de investigación. Otros datos relacionados con el paciente necesarios para la realización de la investigación, como el origen étnico, la situación familiar (como el número de hijos), el consumo de drogas, alcohol, drogas, hábitos o comportamientos generales, la situación profesional como el trabajo, el desempleo, la participación en otras investigaciones.	Administración y gestión de la investigación biomédica (ensayos clínicos, estudios observatorios)	
Pacientes (que pueden incluir niños menores de 18 años cuando se produzca un evento adverso que implique el uso de un producto de	Identificadores indirectos del paciente, como la edad, el año o la fecha de nacimiento, las iniciales del paciente (según lo permita la legislación local), el sexo, el peso/altura o el número de identificación del paciente (excluidos los identificadores nacionales de salud).	Cumplimiento normativo y de farmacovigilancia, como monitoreo de seguridad e informes de eventos adversos (cuando lo permita la ley local)	

Amgen con indicación pediátrica).	Datos relativos a la identificación del producto Amgen, como el producto o dispositivo utilizado, los números de serie de los dispositivos, el método de entrega o la dosificación del producto, los números de lote del producto. Datos de salud, incluidos los procesamientos administrados, los resultados de los exámenes, la naturaleza de cualquier efecto indeseable, los antecedentes médicos personales o familiares, las enfermedades o eventos asociados, los factores de riesgo, la información relacionada con la prescripción y el uso de medicamentos y la conducta terapéutica de los profesionales de la salud involucrados en el manejo de la enfermedad del paciente. Otros datos relativos al paciente necesarios para la evaluación del evento adverso para la salud de acuerdo con las obligaciones de cumplimiento normativo como etnia, vida profesional, consumo de drogas, alcohol, drogas y/o hábitos o comportamientos generales.		

Anexo 2: Descripción general del programa de capacitación de Amgen

Programa de Capacitación y Concientización sobre Privacidad y Protección de Datos

El Programa de capacitación en Privacidad y Protección de Datos se esfuerza por garantizar que todo el personal de Amgen reciba la formación adecuada en relación con las BCR de Amgen en la UE, así como con cualquier obligación legal que afecte al procesamiento de datos personales. Este programa contiene varios elementos.

Capacitación general para todo el personal de Amgen

Todo el personal de Amgen debe realizar una capacitación anual en línea sobre protección de datos como parte de la formación sobre el Código de Conducta. Esta capacitación es obligatoria y supervisada y suele durar unos 75 minutos. Esta capacitación incluye las BCR de la UE e información sobre las consecuencias en virtud de la legislación penal y laboral y/o su contrato de servicios para el personal que incumpla las BCR de la UE.

Capacitación específica para DPO

Todos los DPO de Amgen reciben formación periódica sobre nuevos procesos a través de llamadas periódicas de DPO realizadas por el Equipo Global de Cumplimiento de la Privacidad y talleres de privacidad in situ y/o en línea según sea necesario. Todos los DPO tienen acceso a una página wiki que responde a las preguntas más frecuentes y proporciona orientación, así como enlaces a recursos externos.

Capacitación específica al personal

La capacitación específica puede impartirse en función de las necesidades necesarias, ya sea en línea o in situ, o mediante la publicación de información en la intranet de Amgen. Esta capacitación puede estar enfocada a grupos específicos que pueden procesar datos personales a diario o apoyar a otros grupos que procesan datos personales. Por ejemplo, el grupo de auditoría, las funciones de investigación y desarrollo y el departamento legal se capacitan regularmente. Esto incluye información sobre los procedimientos para gestionar las solicitudes de acceso a los Datos Personales por parte de las autoridades públicas, cuando corresponda a personal específico. Esta capacitación puede tener lugar a nivel regional o a nivel nacional. Es posible que se desarrolle más formación específica sobre las BCR de la UE en función de la necesidad de conocerlas.

Conocimiento

Amgen tiene una página dedicada en su intranet a la privacidad y la protección de datos que proporciona enlaces a otros recursos, ya sea interna o externamente.

El Equipo de Cumplimiento de Privacidad Global de Amgen colabora con el departamento de Seguridad de la Información en el programa Sentinela, que es un programa global para concienciar al personal de Amgen sobre la seguridad de la información.

Apoyo a la capacitación

Todas las capacitaciones relacionadas con la privacidad son desarrolladas por el Equipo Global de Cumplimiento de Privacidad y aprobadas por el Director de Privacidad. La capacitación puede ser realizada directamente por un miembro del Equipo Global de Cumplimiento de Privacidad o por un DPO local en un modelo de "capacitación del capacitador".