Resumen de las Normas Corporativas Vinculantes (NCV)

El presente documento es un resumen y no reemplaza al documento completo de las NCV. En todos los casos, el documento completo de las NCV será el único con validez legal.

1 Un nivel adecuado y uniforme de protección de datos

Fresenius debe seguir diversas leyes de protección de datos en todo el mundo. Las Normas Corporativas Vinculantes (NCV) establecen un marco uniforme y adecuado para la protección de datos. De este modo, se permite el intercambio interno de datos personales entre las entidades abarcadas de Fresenius.

2 Aplicable en todo el mundo

Las NCV se aplican a las siguientes entidades de Fresenius:

- Fresenius Kabi AG, inclusive todas las empresas subsidiarias/asociadas
- Fresenius Digital Technology (FDT)
- Fresenius SE & Co. KGaA

Aplicable a ciertas actividades

Las NCV se aplican a las siguientes actividades de tratamiento de datos personales:

- Todas las actividades de entidades europeas
- Actividades de entidades no europeas:
  - Cuando recogen datos personales por encargo de una entidad europea de Fresenius
  - Cuando colaboran con una entidad europea de Fresenius
  - Cuando reciben datos personales de entidades europeas
  - Cuando recogen datos personales de personas situadas en Europa para ofrecer productos y servicios, o monitorear su comportamiento

Las NCV se aplican, tanto a procesos en papel, como informáticos.

Las NCV se aplican a todos los procesos que permiten una búsqueda estructurada de datos personales.

3 Las NCV establecen el nivel mínimo

Si existen leyes locales en materia de protección de datos que requieran normas adicionales o más severas para el tratamiento de datos personales, estas también deberán observarse.

Si una ley local es contraria a las NCV, se debe informar al delegado de protección de datos (DPD). El DPD evaluará las repercusiones y resolverá el conflicto.

Si una autoridad ordena a una entidad comunicar datos personales y esto infringe las disposiciones de las NCV, se debe informar al DPD. El DPD informará a la autoridad de control en Alemania.

4 Las NCV son vinculantes para la organización y nuestro personal

Las NCV son de cumplimiento obligatorio y vinculantes para:

- Todas las entidades: firman un contrato
- Todo el personal: tienen el deber de cumplir con las políticas de la empresa en función de su contrato de trabajo.

Estas obligaciones generan derechos para organizaciones y personas.

La ejecución de medidas por el incumplimiento de las NCV y las potenciales sanciones debido a incumplimientos serán idénticas a aquellas derivadas de cualquier otro incumplimiento de una política de la compañía.

5 Fresenius creó una organización de protección de datos

El grupo Fresenius creó una organización interna de protección de datos con las siguientes funciones y responsabilidades:

- El delegado de protección de datos (DPD) controla, por ejemplo, verifica y supervisa que se cumplan las NCV, así como leyes, reglamentos y procesos locales. El DPD puede llevar a cabo auditorías, inspecciones e investigaciones. Asimismo, el DPD es el punto de contacto de las autoridades de protección de datos de Europa. A continuación, se detallan los datos de contacto:

  Delegado de protección de datos
  Else-Kröner-Str. 1
  61352 Bad Homburg v.d.H.
  Alemania
  O por correo electrónico:
  Para Fresenius SE y FDT: dataprotectionofficer@fresenius.com
  Para entidades de Fresenius Kabi: dataprotectionofficer@fresenius-kabi.com

- El consultor local en materia de protección de datos (CLPD) ayuda y asesora a personal local, así como a responsables de procesos, si tienen alguna consulta o preocupación relacionada con la protección de datos. Si es necesario, el CLPD asiste al CPD y al DPD, por ejemplo, si solicitan que ejerza su función de supervisión o necesitan que contacte con autoridades de control, por ejemplo, por cuestiones de idioma.
- El consultor en materia de protección de datos (CPD) realiza tareas de asistencia y consultoría para los CLPD y es responsable del sistema de gestión de protección de datos. Si es necesario, el CPD asiste al DPD, si se solicita que ejerza su función de supervisión o se necesita que contacte con autoridades de control, por ejemplo, por cuestiones de idioma.

6 Ocho principios de protección de datos que deben seguirse en el marco de las NCV

Al tratar datos personales, seguiremos distintos principios para proteger los derechos y libertades fundamentales de las personas, de acuerdo con las NCV. Cada entidad debe cumplir con los siguientes principios al tratar datos personales:

6.1 Principio 1: Licitud

Poseer una base jurídica documentada al recoger, utilizar y tratar datos personales. Estas bases jurídicas se enumeran de forma taxativa. Algunos ejemplos son los siguientes:

- El tratamiento de datos es necesario para celebrar un contrato con la persona, como contratos de trabajo y contratos de ventas
- La persona ha otorgado su consentimiento
- Los intereses legítimos de Fresenius son mayores que las consecuencias negativas para las personas
- La necesidad de cumplir con otras obligaciones legales, como leyes fiscales, requisitos de control o requisitos de buenas prácticas.

Los datos de categorías especiales, como los datos sanitarios, necesitan fundamentos jurídicos adicionales.

Si la legislación local exige disposiciones adicionales o distintas, estas también deben respetarse (esto puede ser importante, por ejemplo, para los datos de personal).

6.2 Principio 2: Transparencia y lealtad

Tratar los datos personales de manera leal y transparente. Informar a las personas antes o en el momento de la recogida y del uso de los datos personales sobre las siguientes cuestiones:

- Quién es responsable del tratamiento y cómo se puede contactar con esa persona
- Qué datos se recogen
- Cómo se recogen los datos
- Por qué necesitamos los datos (fin)
- Con qué organizaciones se comparten los datos
- Si se comparten con otros países
- Por cuánto tiempo se almacenan los datos
- La base jurídica de la recogida y del uso de datos y una explicación de esto (principio 1)
- Si se elaboran perfiles de las personas
- Si tomamos decisiones por medios automatizados
- Si los datos deben comunicarse y qué sucede si no se comunican
- Los datos de contacto del DPD y de la autoridad
- Los derechos que tienen las personas

Toda esta información debe comunicarse de manera completa y de forma que pueda accederse a ella fácilmente, utilizando palabras claras y sencillas.

6.3 Principio 3: Limitación de la finalidad

Utilizar los datos personales para los fines determinados, explícitos y legítimos, para los que se han recogido. No se permitirán usos ulteriores, a menos que sean compatibles con el fin original y/o se adopten medidas adicionales.

Los fines de tratamientos ulteriores que, en general, se consideran compatibles con el fin original son los siguientes:

- Archivo
- Auditoría interna
- Investigaciones

Si se desea modificar el fin, se debe consultar al C(L)PD. En caso de que se permita el cambio de fin, se debe informar acerca de todos estos cambios a las personas.

6.4 Principio 4: Minimización de datos

Recoger y usar solo datos personales necesarios para el fin definido, tal como se ha comunicado a las personas. En otras palabras, se debe asegurar que los datos personales sean pertinentes y no excesivos en función del fin.

6.5 Principio 5: Exactitud

Mantener los datos personales exactos y actualizados. Se deben aplicar procedimientos para asegurar que los datos inexactos se supriman, corrijan o actualicen sin dilación.

6.6 Principio 6: Limitación del plazo de conservación

No mantener los datos personales por más tiempo del necesario para los fines que han sido recogidos, a menos que lo exija la ley. En este caso, se debe restringir el acceso a ellos. Eliminar o anonimizar los datos personales si ya no hay un motivo o un fin legal.

6.7 Principio 7: Seguridad, integridad y confidencialidad

Aplicar medidas técnicas y organizativas apropiadas para proteger los datos personales contra su destrucción, pérdida, alteración o divulgación, así como para restringir el acceso a

ellos (por ejemplo, a través de una planificación adecuada de funciones y derechos, copias de seguridad y restauraciones, o por medio de cifrado).

Al aplicar medidas de esta índole, se deben considerar los riesgos para las personas. Al instalar sistemas informáticos y realizar su mantenimiento, se debe evaluar su seguridad en función de estos riesgos.

Documentar e informar a la organización de protección de datos cualquier violación de la seguridad que pueda derivar en un riesgo para las personas afectadas.. En función de las circunstancias, estas violaciones deberán también notificarse a la autoridad de control, las personas u otras organizaciones.

6.8 Principio 8: Responsabilidad proactiva

Poseer la capacidad de demostrar el cumplimiento con las NCV. A este fin, crear y mantener documentación adecuada, como la siguiente:

- Registros de actividades de tratamiento
- Medidas técnicas y organizativas adoptadas para cumplir con los principios en materia de protección de datos y afrontar los riesgos
- Evaluaciones de riesgos y controles relativos a la protección de datos

6.8.1 Designación de encargados del tratamiento

Designar como encargadas del tratamiento solo a aquellas personas que presenten suficientes garantías para la adopción de medidas técnicas y organizativas apropiadas, de manera que el tratamiento cumpla con los requisitos de las NCV y la legislación local en materia de protección de datos. Esto debe asegurarse por medio de un contrato de protección de datos entre la entidad correspondiente y el encargado del tratamiento.

6.8.2 Transferencias (ulteriores) de datos personales

Aplicar medidas para proteger de forma adecuada transferencias de datos personales a otras organizaciones ubicadas fuera del Espacio Económico Europeo (EEE), en función de estas NCV. A este fin, se pueden acordar cláusulas contractuales tipo con la otra organización, como las adoptadas por la Comisión Europea.

7 Evaluación de riesgos relativa a la protección de datos

Para cada actividad de tratamiento de datos, se debe llevar a cabo una evaluación de riesgos de la protección de datos. Esta evaluación es un proceso formal para evaluar las repercusiones de la actividad en los derechos y la libertad de los interesados correspondientes.

Las faltas de control y los potenciales riesgos identificados deben informarse y documentarse. Antes de comenzar con la actividad del tratamiento de datos, se deben adoptar medidas técnicas y organizativas de mitigación.

8 Evaluaciones de impactos relativas a la protección de datos

Si por medio de la evaluación de riesgos relativa a la protección de datos se constata que existe un riesgo elevado, se debe llevar a cabo una evaluación de impactos relativa a la protección de datos (EIPD). En este marco, se solicitará la asistencia del DPD.

Si una EIPD identifica un riesgo elevado en una actividad específica de tratamiento de datos, se deberán aplicar medidas adecuadas para mitigar estos riesgos antes de iniciar la actividad de tratamiento. Si la EIPD informa aún de un riesgo elevado después de la aplicación de las medidas, se deberá consultar a la autoridad de control pertinente antes de tratar los datos.

9 Derechos de las personas

Las personas deben poder ejercer sus derechos (derechos de los interesados):

- **Derecho de acceso a datos personales**: Las personas pueden solicitar acceder a información sobre datos personales que les conciernan tratados por Fresenius o recibir

dicha información (por ejemplo, el fin del tratamiento, las categorías de datos personales de que se trate, los destinatarios, los plazos de conservación, la eventual existencia de decisiones automatizadas).

- **Derecho de rectificación de los datos personales:** Las personas pueden solicitar que se corrijan los datos personales inexactos o incompletos.
- **Derecho de supresión de los datos personales:** Las personas pueden solicitar que se eliminen sus datos personales, a menos que deban conservarse, por ejemplo, debido a exigencias legales de retención.
- **Derecho de limitación del tratamiento de datos personales:** Las personas pueden solicitar limitar el tratamiento de sus datos personales, si se impugna la exactitud de los datos personales o el tratamiento es ilícito (ya no es necesario para los fines perseguidos).
- **Derecho a recibir los datos personales en un formato que permita su portabilidad:** Las personas pueden solicitar recibir sus datos personales en un formato de uso común y lectura mecánica, si se cumplen las siguientes condiciones:
    - Los datos personales han sido comunicados por la persona
    - El tratamiento está basado en el consentimiento de la persona o un contrato celebrado con ella
    - El tratamiento se efectúa por medios automatizados
- **Derecho de oposición al tratamiento de datos personales:** Las personas pueden oponerse al tratamiento de sus datos personales por motivos relacionados con su situación particular y sobre la base de un interés legítimo o público. La oposición deberá evaluarse. Asimismo, las personas pueden oponerse a tratamientos que tengan por objeto la mercadotecnia directa y la elaboración de perfiles. En caso de oposición, el tratamiento deberá detenerse.
- **Derecho a no ser objeto de decisiones individuales automatizadas:** Las personas tienen derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que pudiera producir efectos jurídicos en ellas o les afecte significativamente de modo similar, a menos que:
    - Sea necesaria para la celebración o la ejecución de un contrato entre la persona y la entidad correspondiente
    - Se base en el consentimiento explícito de la persona

10 Cumplimiento de las NCV

10.1 Acceso a las NCV

Las NCV deben estar a disposición de las personas de forma adecuada. Las NCV se publicarán en internet y la intranet.

Asimismo, las personas pueden acceder a las NCV al contactar con el DPD correspondiente o cualquier miembro de la organización de protección de datos.

10.2 Tramitación de reclamaciones relacionadas con las NCV

Todas las personas están facultadas para:

- Reclamar incumplimientos de las NCV, leyes locales en materia de protección de datos, resoluciones de autoridades de control, políticas internas y directrices, o compromisos voluntarios relacionados con la protección de datos
- Hacer referencia a sus derechos personales
- Hacer cumplir cualquier otro derecho relacionado con las NCV

Cualquiera de estas reclamaciones puede presentarse, por ejemplo, telefónicamente, por correo electrónico o postal, o de forma oral ante el DPD correspondiente, el CLPD respectivo o la línea de atención de cumplimiento normativo.

En caso de que la reclamación se considere justificada, la entidad adoptará las acciones pertinentes para abordar la reclamación e informará a la persona de manera respectiva en el transcurso de un mes.

10.3 Responsabilidad y ejecución de medidas por el incumplimiento de las NCV

Las personas que se hayan visto afectadas o hayan sufrido daños como resultado del tratamiento de sus datos personales están facultadas para hacer cumplir las partes correspondientes de las NCV y, si corresponde, recibir una compensación ante un tribunal competente.

En caso de incumplimientos demostrados de partes establecidas fuera de la Unión Europea o del Espacio Económico Europeo, Fresenius acepta la responsabilidad por cualquier daño que hayan podido sufrir las personas. La entidad que causó el daño deberá asistir a Fresenius de forma razonable para responder a tiempo a estas reclamaciones o solicitudes.

10.4 Cooperación con autoridades de control

Todas las entidades deben cooperar con las autoridades de control, respetar la interpretación de estas NCV y aceptar la ejecución de auditorías por parte de las autoridades de control pertinentes.

10.5 Formación

Cada entidad inscribirá a su personal para que participe de forma obligatoria en una formación sobre las NCV y la protección de datos, y repita esta formación con regularidad. Como mínimo, cada dos años se deberá llevar a cabo una formación general para todo el personal pertinente. Asimismo, se deberán realizar formaciones según las funciones específicas (por ejemplo, para departamentos de RRHH. o compras), en función de las necesidades determinadas de ciertos puestos/personas.

10.6 Auditorías

Todas las partes se comprometerán a someterse a auditorías periódicas (planificadas o *ad hoc*) para evaluar y comprobar que se cumplan las NCV, y aplicar mecanismos adecuados y suficientes para subsanar el incumplimiento de las NCV por parte de una entidad. La organización de protección de datos realizará un seguimiento de las auditorías llevadas a cabo para evaluar si las acciones correctivas sugeridas se han aplicado de forma apropiada y documentar los resultados en el informe de auditoría. Cada entidad se compromete a poner a disposición de las autoridades de control los informes de auditoría, si los solicitan.

10.7 Actualización de las NCV

Las partes examinarán las leyes locales en materia de protección de datos e informarán si se deben realizar cambios en las NCV. Fresenius puede modificar las NCV en caso necesario. Cualquier cambio significativo en las NCV se informará sin dilación a cada entidad y a la autoridad de control. Cualquier otra modificación no sustancial en las NCV se informará a las partes, tan pronto sea viable.

11 Gestión de salidas

En caso de que una entidad deje de estar sujeta a las NCV (por ejemplo, por la conclusión o rescisión del acuerdo correspondiente con el grupo), dicha entidad deberá:

- Devolver todos los datos personales a cada una de las partes de las cuales ha recibido estos datos
- Destruir todos estos datos personales, en cumplimiento de las normas locales de retención de datos
- Proporcionar garantías suficientes en relación con estos datos personales (por ejemplo, pactandor cláusulas contractuales tipo).