UNIVERSIDAD INTERNACIONAL DE LA RIOJA

Universidad Internacional de La Rioja
Máster en Protección de Datos

Normas Corporativas Vinculantes: Evolución y Efectividad

Trabajo fin de máster presentado por:	Antonio Meroño Ortega
Titulación:	Máster en Protección de Datos
Área jurídica:	Protección de datos
Director/a:	Amaya Noain Sánchez

Ciudad: Madrid
22 de julio de 2018
Firmado por:

Índice

1. Listado de abreviaturas y siglas

Abreviatura	Texto
AEPD	Agencia Española de Protección de Datos
APD	Autorité de Protection des donnés (Autoridad Nacional de Protección de Datos de Bélgica)
BayLDA	Bayerischen Landesamt für Datenschutzaufsicht (Autoridad de Protección de Datos de Bavaria)
BCR	Binding Corporative Rules (Normas Corporativas Vinculantes)
BCR-C	Binding Corporative Rules for Controllers (Normas Corporativas Vinculantes para Responsables del tratamiento)
BCR-P	Binding Corporative Rules for Processors (Normas Corporativas Vinculantes para Encargados del tratamiento)
BfDI	Federal Commissioner for Data Protection and Freedom of Information (Autoridad Federal de Protección de Datos de Alemania)
CE	Comunidad Europea
CNIL	Commission Nationale de l'Informatique et des Libertés (Autoridad de Protección de Datos de Francia)
CNPD	Commission Nationale Pour La Protection Des Données (Autoridad Luxemburguesa de Protección de Datos)
DPA Danesa	Datatilsynet (Autoridad de Protección de Datos de Dinamarca)
DPA Holandesa	Autoriteit Persoonsgegevens (Autoridad Holandesa de Protección de Datos)
DPA Lower Saxony	Data Protection Authority of Lower Saxony (Autoridad de Protección de Datos de la Baja Sajonia)
DPA North Rhine-Westphalia	Data Protection Authority of North Rhine-Westphalia (Autoridad de Protección de Datos del Norte de Rin-Westfalia)
DPA Noruega	Datatilsynet (Autoridad de Protección de Datos de Noruega)
DPC	Irish Data Protection Commission (Autoridad Irlandesa de Protección de Datos)
EEE	Espacio Económico Europeo
EM	Estado Miembro de la Unión Europea
GT 29	Grupo de Trabajo del Artículo 29
ICO	Information Commissioner´s Office (Autoridad Británica de Protección de Datos)
IDPC	Office of the Information and Data Protection Commissioner (Autoridad Maltesa de Protección de Datos)
NCV	Normas Corporativas Vinculantes
RGPD	Reglamento General de Protección de Datos
SEPD	Supervisor Europeo de Protección de Datos
STC	Sentencia del Tribunal Constitucional
UE	Unión Europea

WP Working Paper (Documento de Trabajo)

2. Resumen y palabras clave

El presente trabajo tiene como objeto de estudio las Normas Corporativas Vinculantes, que es un instrumento jurídico pensado para aquellos grupos de empresas que realicen tratamientos de datos personales en sus diferentes sedes, ya sea dentro o fuera de la Unión Europea.

Este estudio pretende revisar dicha figura, concebida para facilitar estos flujos, imprescindibles en un mundo cada vez más globalizado, cumpliendo con los estándares de seguridad y normativos de la regulación europea, con independencia de la ubicación. Asimismo, realizaremos un análisis de dicho instrumento jurídico en el recién estrenado Reglamento General de Protección de Datos (RGPD), evaluando la adaptación de estas al escenario actual. Finalmente, intentaremos dar respuesta a la cuestión que se plantea sobre la relevancia y efectividad de esta herramienta en la vida real de las empresas.

Palabras clave: Normas Corporativas Vinculantes, UE, protección de datos, RGPD, flujo transfronterizo de datos.

Abstract

The aim of this paper is to approach the study of the Binding Corporative Rules, which is a legal instrument implemented by those Corporations performing personal data processing, located in different headquarters, either inside or outside the boundaries of the European Union.

What is intended with this figure is, on the one hand, to facilitate these data flows, which means an essential part of an increasingly globalized world. On the other, it aims to guarantee the safety standards and regulatory compliance of European regulations, regardless of its location.

This subject has been object of a new regulation in the EU, the General Data Protection Regulation (GDPR) and we will try to show the main news in it. Finally, we will try to answer the question about the effectiveness of this tool in real life.

Key words: Binding Corporative Rules, EU, data protection, GDPR, international data transfer.

3. Introducción y presupuestos de partida

En la actualidad, el flujo transfronterizo de datos es una realidad imprescindible que aumenta cada día, lo cual plantea serios problemas, ya que no existen unos estándares internacionales de seguridad aceptados por todos los países y, una vez salen los datos de las fronteras, es muy difícil controlar dónde pueden llegar y a manos de quién. Especialmente complicada resulta la conciliación de esta realidad con la protección de datos personales, entidad que la Comisión Europea define como: "cualquier información relativa a una persona física viva identificada o identificable. Las distintas informaciones, que recopiladas pueden llevar a la identificación de una determinada persona, también constituyen datos de carácter personal" [1]. Es decir, entendemos como dato personal: El nombre y apellidos; el domicilio; la dirección de correo electrónico (siempre que sea del tipo nombre.apellido@empresa.com); el número de documento nacional de identidad; o datos de localización (como la función de los datos de localización de un teléfono móvil). La base de esta definición se haya en el nuevo Reglamento General de Protección de Datos, el Reglamento 679/2016, de 27 de abril de 2016, en adelante, RGPD.

Así pues, este escenario plantea al legislador la disyuntiva de encontrar el equilibrio entre no restringirla con la excusa de preservar la privacidad, ya que esto puede provocar un efecto contrario que de lugar a la proliferación de sistemas alternativos e ilegales difíciles de controlar y carentes de garantías, o bien garantizar que tales movimientos internacionales no puedan poner en riesgo la privacidad tan larga y costosamente conseguida en la Unión Europea. El dilema, como vemos, no es menor. La importancia de la protección de datos personales en este escenario globalizado se percibe en el hecho de que el legislador europeo haya dictado un Reglamento para regular esta materia y no una Directiva como hizo en el año 1996[2]. De hecho, los datos personales se consideran ya como el "petróleo del s. XXI" y, aunque se desconoce cuál es el límite del uso de estos, sí que se tiene la certeza de su potencial, sobre todo dados los avances tecnológicos, que son ya un presente en muchos casos (como, por ejemplo, en el uso de dispositivos como los *smartphones*), y los que nos vienen en un futuro muy cercano (el Internet de las cosas o los *weareables*, entre otros).

1 Comisión europea [Internet]: "¿Qué son los datos personales?" [consultado el 12 junio 2018]. Disponible en: https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_es#referencias.

2 En el Derecho comunitario, las Directivas precisan de un desarrollo legislativo de los Estados miembros, puesto que ejercen una función de marco jurídico que solo se puede aplicar directamente a falta de dicho desarrollo, lo cual puede dar lugar a cierta disparidad de criterios para aquellos supuestos que hayan sido recogidos en la misma, con carácter más general. El Reglamento, por su parte, es de aplicación directa a los Estados miembros y puede ser alegado por los ciudadanos desde el momento en que resulta aplicable. Por todo ello, la gran ventaja que supone esta figura es que homogeneiza la normativa comunitaria en un tema tan candente como el de la protección de datos personales.

Este es el motivo por el que en el RGPD se ha hecho mención expresa a que las transferencias se lleven a cabo siempre y cuando se asegure la protección de los datos. Dicho Reglamento diseña un modelo que sigue la misma línea que la Directiva 95/46/CE, aunque introduce algunas novedades importantes que pasaremos a detallar más adelante. El RGPD protege los datos personales independientemente de la tecnología utilizada para su tratamiento y se aplica tanto al tratamiento automatizado como manual, siempre que haya un criterio organizativo. La máxima preocupación de la nueva normativa es marcar unos estándares de seguridad en dichos tratamientos y colocar a los titulares de los derechos en el centro de la atención de la normativa, de modo que siempre sepan exactamente quién y para qué está tratando sus datos y que dicho tratamiento se basará siempre en su consentimiento. Consentimiento que, en cualquier momento, puede ser revocado y, además, se le amplían los derechos ante los responsables y encargados del tratamiento.

Este giro copernicano de la normativa, centrada ahora en la figura del ciudadano en cuanto a titular del derecho de protección de datos como derecho fundamental (derecho que, por otro lado, ha sido recogido en tratados internacionales varios y, en cuanto a España se refiere, en el art. 18.4 CE, sobre todo tras la interpretación de la sentencia del Tribunal Constitucional STC 292/2000), ha provocado que las empresas tengan que proceder a una adaptación de sus *modus operandi.*

Con el fin de dar respuesta al objetivo que nos planteamos en esta investigación se ha llevado a cabo la siguiente metodología: En primer lugar, centramos el foco en la recopilación y análisis de la legislación existente en la materia, tanto a nivel nacional, como europeo, así como en la jurisprudencia y en los informes del Grupo de Trabajo del Artículo 29 del la Directiva 95/ 46/CE. Todo ello, junto con revisión de las diferentes opiniones doctrinarias de referencia. En segundo lugar, realizaremos una breve comparativa de las Normas Corporativas Vinculantes antes y después de la entrada en vigor del Reglamento General de Protección de Datos. Finalmente, y desde un punto de vista analítico, intentaremos averiguar si en la legislación actual las Normas Corporativas Vinculantes ofrecen una respuesta útil a la protección de datos de carácter sensible en las transferencias de datos.

4. Introducción a las Normas Corporativas Vinculantes

4.1. Los conceptos de transferencia internacional de datos y garantías

Por lo que hace referencia al concepto de “transferencia internacional” en sí, es curioso que, al igual que pasaba con la Directiva 95/46/CE, el Reglamento no la define. Sí dice que, a efectos del Reglamento, las comunicaciones de datos entre Estados miembros de la UE no se

considerarán transferencias internacionales, porque parte de la premisa de que en todos los Estados Miembros de la UE existe un nivel de protección "adecuado", es decir, que equipara el nivel de protección de datos de carácter personal de todos ellos. Sin embargo, en este momento, la situación de Gran Bretaña merece especial atención ya que, tras el Brexit, pasará a ser un tercer país a todos los efectos, situación sin antecedentes en la historia de la UE y que continúa siendo objeto de debate. En cualquier caso, a 25 de mayo de 2018, Gran Bretaña sigue siendo miembro de la UE y, por tanto, debe cumplir con su normativa.

Equiparable también es el nivel de protección de datos de carácter personal que se ha reconocido, por parte de la UE a los Estados miembros del Espacio Económico Europeo (EEE), que incluyen, además de los Estados miembros de la Unión Europea, a Islandia, Liechtenstein y Noruega, ya que estos países también transpusieron a su Derecho nacional la Directiva 95/46/CE.

Así, de la normativa podríamos extraer la siguiente definición de transferencia internacional como: "aquel tratamiento de datos en el que hay implicados al menos un Estado miembro de la UE y un país tercero o una organización internacional."[3]

Mientras que la Directiva trataba siempre las transferencias internacionales entre países que garantizasen el nivel apropiado de seguridad, porque en caso contrario las prohibía, el Reglamento parte de la suposición de que siempre va a ser posible hacer una transferencia internacional si se basa en una decisión de adecuación, en garantías adecuadas o en alguna de las excepciones previstas en el RGPD[4].

Este régimen de transferencias es aplicable no sólo a los responsables sino también a los encargados. Aquí conviene recordar que siempre se deberá respetar el resto de las previsiones del Reglamento y que la protección dada por el Reglamento no debe verse menoscabada por transferencias ulteriores de datos personales.

Nos vamos a centrar en esas garantías adecuadas de las que acabamos de hablar como justificación de la transferencia. En la Directiva se consideraban una excepción a la regla general, mientras que el art. 46.1 RGPD establece que:

> A falta de decisión de adecuación, el responsable o el encargado del tratamiento solo podrá transmitir datos personales a un tercer país u organización internacional si hubiera ofrecido garantías adecuadas y a condición de que los interesados cuenten con derechos exigibles y acciones legales efectivas.[5]

[3] Art. 44 RGPD
[4] Art. 49 RGPD
[5] Art. 46.1 RGPD

Se exige, por tanto, que las garantías sean efectivas para los interesados, que deben contar con derechos exigibles y acciones legales efectivas.

El Reglamento distingue dos bloques de garantías adecuadas: las que no requieren autorización y las que sí. Las que no la requieren vienen recogidas en el RGPD[6] y son las siguientes:

- un instrumento jurídicamente vinculante y exigible entre las autoridades u organismos públicos;
- Normas Corporativas Vinculantes, en adelante, NCV.
- Cláusulas tipo de protección de datos adoptadas por la Comisión
- Cláusulas tipo de protección de datos adoptadas por una autoridad de control y aprobadas por la Comisión
- Un código de conducta, junto con compromisos vinculantes y exigibles del responsable o el encargado del tratamiento en el tercer país de aplicar garantías adecuadas, incluidas la relativas a los derechos de los interesados, o
- Un mecanismo de certificación, junto con compromisos vinculantes y exigibles en los mismos términos que los códigos de conducta

Además, siempre que haya autorización de la autoridad de control competente, las garantías se pueden aportar mediante cláusulas contractuales entre el responsable o el encargado y el responsable, encargado o destinatario de los datos personales en el tercer país u organización internacional, o disposiciones que se incorporen en acuerdos administrativos entre las autoridades u organismos públicos que incluyan derechos efectivos y exigibles para los interesados[7].

4.2. Definición de Normas Vinculantes Corporativas

Una vez llegados a este punto vamos a hacer hincapié en las Normas Corporativas Vinculantes (NCV) o, como se las conoce internacionalmente, *Binding Corporative Rules* (BCR).

El Reglamento las define en su art. 4.20 como:

> Las políticas de protección de datos personales asumidas por un responsable o encargado del tratamiento establecido en el territorio de un Estado miembro para transferencias o un conjunto de transferencias de datos personales a un responsable o

[6] Art. 46.2 RGPD
[7] Art. 46.3 RGPD

encargado en uno o más países terceros, dentro de un grupo empresarial o una unión de empresas dedicadas a una actividad económica conjunta[8].

En relación con esta definición, la clave está en el hecho de que son políticas de protección de datos personales, es decir, su aplicación no sustituye a las normas en materia de protección de datos a las que estén sujetas las empresas del grupo. Por lo tanto, no solo tendrán que cumplir con sus obligaciones legales, sino que también con las NCV.

Su objetivo es el de facilitar las transferencias internacionales en el marco de las grandes corporaciones multinacionales o grupos de empresas, asegurando, de esta forma, el pleno respeto a la protección de datos. Así, una autoridad de control competente aprobará las NCV siempre que, como decimos: 1) éstas sean jurídicamente vinculantes y se apliquen y sean cumplidas por todos los miembros correspondientes del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta, incluidos sus empleados; 2) confieran expresamente a los interesados derechos exigibles en relación con el tratamiento de sus datos personales, y 3) cumplan los requisitos establecidos en el 47.2 RGPD.

Una vez realizada la necesaria aclaración de términos, procederemos a abordar la gestación, evolución y desarrollo de las NVC hasta el escenario actual, con el fin de realizar un análisis comparativo que nos permita evaluar las novedades introducidas por el RGPD y su adecuación a las demandas de la sociedad.

5. Origen: el Grupo de Trabajo del artículo 29

En 2002, utilizando como ejemplo la legislación alemana, que desde 2001 ya recogía la figura de las NCV, las autoridades de control en materia de protección de datos de Austria, Holanda y Alemania se plantearon, por primera vez, la posibilidad de llevar a cabo una acción que sirviera para coordinar los procedimientos de homologación referidos a las NCV, identificando una serie de criterios de referencia.

El encargado de llevar a cabo este proyecto fue el Grupo de Trabajo del art. 29, (en adelante GT 29), creado por la Directiva 95/46/CE. Este Grupo es un órgano consultivo independiente integrado por las Autoridades de Protección de Datos de todos los Estados miembros, el Supervisor Europeo de Protección de Datos y la Comisión Europea, que realiza funciones de secretariado. Las autoridades de los estados candidatos a ser miembros de la Unión y los países del EEE asisten a sus reuniones como observadores.

[8] Art. 4.20 RPGD

En 2003, dicho grupo publicó el documento WP 74, considerado como el primero que regula la figura de las NCV. El objetivo de este, según su propia introducción, es el de dar una respuesta a las solicitudes de autorizaciones para la transferencia de datos personales a terceros países que recibían las Autoridades de Control nacionales de las empresas multinacionales. Posteriormente, el GT 29 fue publicando otros documentos que se enfocaban en aspectos más concretos de las NCV. A continuación, vamos a nombrar los aspectos más destacables de cada uno de ellos.

5.1 WP 74: Transferencias de datos personales a terceros países

En este documento se reconoce que se debe aprovechar la experiencia, aunque reciente en esa fecha, de las empresas multinacionales, porque habían sabido dar una respuesta que permitía la emisión de transferencias internacionales de datos personales dentro de sus complejas estructuras. Y, para ello, habían elaborado unos códigos de conducta que normalmente solían tratar de:

- mantenimiento y conservación de los libros y registros;
- veracidad y precisión en las comunicaciones con los usuarios y el gobierno;
- procedimientos para garantizar que el asesoramiento a los clientes y las decisiones comerciales no se vean afectados por conflictos de intereses;
- protección de la información confidencial;
- prohibición del uso indebido de los activos corporativos;
- eliminación de discriminación y acoso impropios;
- prohibición de sobornos;
- la implementación de prácticas comerciales éticas y el cumplimiento de las leyes que fomenten la competencia en el mercado;
- prohibición del comercio de valores basado en información privilegiada

El GT 29 se hacía eco de que eran las propias empresas las que reclamaban la posibilidad de simplificar los procesos de autorización atendiendo a esos códigos de conducta aplicables a todos sus miembros, con independencia de su ubicación y basándose siempre en el compromiso unilateral de esas garantías recogidas en dichos códigos de conducta.

En ese sentido, el GT 29 veía positiva la aplicación de estos instrumentos, en la medida en que pudieran tener efectos jurídicos reales y garantizados, en particular con respecto a la protección efectiva de los interesados tras la transferencia y con respecto a la posible intervención de las autoridades nacionales de supervisión u otras autoridades. Así, el GT 29

hace referencia a la Directiva 95/46 / CE[9], vigente en ese momento, como una herramienta que ofrecía a los Estados miembros un amplio margen de maniobra a este respecto.

La clave en este punto era que, por un lado, en alguno de los Estados miembros la legislación nacional no les permitía a las empresas generar obligaciones ni derechos con efectos jurídicos, y, por otro lado, las NCV no podían contravenir la legislación nacional.

El GT 29 redacta el WP 74 con la intención de aportar luz ante esta disyuntiva y para ello declara que el WP 74 no era una solución aplicable a todas las situaciones, y que habría, en determinados casos, que encontrar alternativas que pudiesen ayudar a la aplicación de las medidas.

A pesar de la imposibilidad de dar una respuesta uniforme que sirviese de modo general, el Grupo seguía considerando útil redactar un documento como el WP 74, porque de esa forma se pretendía armonizar la interpretación de la Directiva y facilitar el flujo de datos con un nivel de protección adecuada. Ello, por otro lado, no era óbice para seguir considerando ~~a~~ las cláusulas contractuales estándar como una solución totalmente a considerar. Es más, se planteaban ambos instrumentos como compatibles e, incluso, complementarios para superar los obstáculos que planteaba la falta de capacidad de las empresas para imponer sus normas en algunos Estados miembros. Por lo tanto, la circulación de datos personales dentro de los miembros del grupo corporativo podría permitirse bajo esta solución, siempre que se establecieran las garantías necesarias.

5.2 Contenido primigenio de las NCV

En cuanto al contenido de las NCV, el GT 29 reafirmaba una serie de principios que figuran en el documento de trabajo WP 12, con referencia especial a lo relativo a la autorregulación de la industria[10]. El problema es que estos principios en sí mismos pueden significar muy poco para las empresas y empleados que procesan datos personales fuera de la UE, en particular, en aquellos países donde no existe una legislación de protección de datos y, muy probablemente, ninguna cultura de protección de los mismos.

Estos principios deben ser desarrollados y detallados en las NCV para que se ajusten de manera práctica y realista a las actividades de procesamiento llevadas a cabo por cada

[9] Art. 26.2 Directiva 95/46/CE

[10] Unión Europea. WP 12 (5025/98) Applying Article 26 of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers. Documento adoptado por el Grupo de Trabajo del Artículo 29 el 24 de Julio de 1998 [consultado el 12 junio 2018]. Disponible en: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/1998/wp12_en.pdf

organización en los terceros países y puedan ser aplicados efectivamente por quienes tienen responsabilidades de protección de datos dentro de la organización.

Desde esta perspectiva, las NCV pueden tener algo en común con los códigos de conducta previstos en el artículo 27 de la Directiva, en el sentido de que deben superar el nivel de abstracción de la legislación (en este caso, los principios del documento de trabajo WP 12). Así, Las reglas corporativas deben contener un nivel razonable de detalle en la descripción de los datos, flujos, propósitos del procesamiento, etc.

Como se indica en el artículo 26, apartado 2, de la Directiva, la autorización puede referirse a una transferencia o a un conjunto de transferencias, pero, en cualquier caso, debe existir una explicación de las transferencias autorizadas. El nivel de detalle debe ser suficiente para permitir que las autoridades de protección de datos evalúen si el procesamiento llevado a cabo en terceros países es adecuado (por ejemplo, una descripción detallada de las actividades económicas realizadas por las diferentes entidades del grupo Corporativo).

El GT 29 previó, incluso, en su WP 74, que las NCV se pudiesen particularizar para diferentes países o regiones fuera de la UE, si así se favorecía el uso de estas. Todo ello, a pesar de que esta particularización obviamente agregaría complejidad al sistema que, en principio, está destinado a desarrollar políticas globales.

En cuanto a las actualizaciones de las transferencias y, por supuesto, la actualización de las NCV, el GT 29 reconoció que los grupos corporativos son entidades mutantes cuyos miembros y prácticas pueden cambiar de vez en cuando y, por lo tanto, no podrían corresponder al 100% a la realidad en el momento en que se otorgó la autorización.

De esta manera, aceptó las actualizaciones sin tener que volver a solicitar una autorización siempre que se diesen estas condiciones:

- No se realizaría una transferencia de datos personales a un nuevo miembro hasta que el exportador de los datos se hubiese asegurado de que el nuevo miembro estuviera efectivamente sujeto a las NCV.
- Una persona o departamento identificado del grupo corporativo debería tener una lista completa y actualizada de los miembros y realizar un seguimiento y registro de las actualizaciones de las reglas, proporcionando la información necesaria para los interesados o las autoridades de protección de datos previa solicitud.
- Cualquier actualización de las NCV o cambios en la lista de miembros se debería informar una vez al año a las autoridades de protección de datos que otorgan las autorizaciones, con una breve explicación de los motivos que justifican la actualización.

La actualización de las reglas se entendía en el sentido de que los procedimientos de trabajo pueden evolucionar y las reglas deberían adaptarse a dichos entornos cambiantes. Los cambios que se consideraban significativos no eran solo los relacionados con los principios de protección, sino también con los fines del procesamiento, las categorías de los datos procesados o las categorías de los interesados.

Además de aquellas normas que trataban principios de protección de datos personales, las NCV también debían contener un sistema que garantizase su conocimiento e implementación dentro y fuera de la Unión Europea. La publicación por parte de la sede principal de la corporación multinacional o grupo corporativo de políticas de privacidad internas debía considerarse, únicamente, como un primer paso en el proceso de aducir salvaguardas suficientes en el sentido del artículo 26.2 de la Directiva. El grupo corporativo solicitante debía, asimismo, ser capaz de demostrar que dicha política era conocida, entendida y aplicada efectivamente en la totalidad de la corporación por aquellos empleados que recibieron la capacitación adecuada y que tenían acceso a la información relevante en cualquier momento, por ejemplo, a través de la Intranet. Igualmente, debía designar al personal apropiado, con el apoyo de la alta gerencia, para supervisar y garantizar conformidad.

Otras previsiones del documento WP 74 son:

- Un sistema de auditoría interna y/o externa, por auditores acreditados, que se realizase de forma regular. Debía existir una garantía inequívoca de que el grupo corporativo en su conjunto y cualquiera de sus miembros por separado aceptará las recomendaciones de la auditoría. También debía haber un compromiso inequívoco de que el grupo empresarial en su conjunto y cualquiera de sus miembros por separado se atendrá al asesoramiento de la autoridad competente de protección de datos sobre cualquier cuestión relacionada con la interpretación y aplicación de estos documentos vinculantes.
- Un departamento para gestionar las quejas, claramente identificado dentro de la organización, cuyos trabajadores gocen de un nivel de protección especial que garantice su independencia en el ejercicio de sus funciones. También se debe promover el uso de mecanismos alternativos de resolución de disputas, con la posible participación de las autoridades de protección de datos cuando corresponda, de conformidad con las leyes y regulaciones nacionales aplicables. La idea principal en este aspecto es que un sistema de protección de datos adecuado y efectivo no va a dejar nunca sola a una persona que se enfrenta a un problema con respecto a sus datos

personales, sino que se le va a proporcionar el apoyo institucional que le permita resolver su incidencia.

Como se describe en el documento WP 12, uno de los elementos más importantes para evaluar la idoneidad de un sistema de autorregulación es el nivel de apoyo y ayuda disponible para los individuos que se ocupan de los datos. De hecho, este es uno de los elementos más importantes de las NCV para las transferencias internacionales de datos: las reglas deben contener claras obligaciones de cooperación con las autoridades de control nacionales, garantizando que los individuos puedan beneficiarse de un apoyo institucional adecuado.

El asesoramiento de la autoridad competente de protección de datos consistirá en recomendaciones dirigidas al grupo empresarial, ya sea en respuesta a un cuestionario, como resultado de una denuncia presentada por un interesado o por propia iniciativa de la autoridad de protección de datos.

Además de cualquier disposición pertinente a nivel nacional, una denegación grave y / o persistente por parte del grupo empresarial de cooperar o cumplir la recomendación de la autoridad competente de protección de datos puede implicar la suspensión o el retiro de la autorización concedida por la propia autoridad de protección de datos o la autoridad competente. Esta decisión tendrá la forma de un acto administrativo que el destinatario podrá impugnar ante el tribunal competente según lo dispuesto por la legislación nacional. Será notificado a la Comisión Europea y a las demás autoridades de protección de datos implicadas y también podría hacerse público.

El objetivo de estas normas, por lo tanto, se limita a garantizar que las autorizaciones otorgadas por las autoridades de protección de datos (que posibiliten o legalmente una transferencia de datos personales al extranjero que de otro modo serían ilícitas) no terminen privando a los titulares de los datos del ejercicio de los derechos que hubieran tenido, si estos nunca hubieran salido del territorio de la UE.

Como complemento de este derecho general, las reglas también deben contener disposiciones sobre responsabilidad y jurisdicción destinadas a facilitar su ejercicio práctico.

- Responsabilidad. Si la sede del grupo está situada en la UE o hay un miembro europeo que tenga responsabilidades en materia de protección de datos, debe aceptar la responsabilidad y acordar tomar las medidas necesarias para solucionar los conflictos de otros miembros del grupo empresarial fuera de la UE y, cuando proceda, pagar una compensación por cualquier daño resultante de la violación de la obligación.

En este caso, este miembro del grupo deberá presentar las garantías suficientes de que puede asumir el pago de una indemnización o que ha tomado medidas equivalentes (como, por ejemplo, un seguro de responsabilidad). Procederá la indemnización en los casos en que se aleguen daños por incumplimiento de las NCV o, cuando, aunque no se hubiera alegado esos daños, el interesado no hubiera quedado satisfecho con los recursos o la queja ante la autoridad competente.

Se podrá liberar del pago de cualquier indemnización la entidad responsable ante la UE si consigue demostrar que la entidad por la que responde, situada fuera de la UE, realmente no produjo el daño

- Jurisdicción. En este punto, el grupo corporativo debe aceptar que los titulares de los datos puedan escoger la jurisdicción del miembro del grupo donde se originó la transferencia de datos o de la sede europea del miembro que tiene la responsabilidad frente a la UE. Lo cierto es que no se considera habitual tener que recurrir a los tribunales, dadas las herramientas previas de las que disponen los sujetos para ver satisfechas sus reclamaciones, pero en todo caso, debe reconocerse esta opción.
- Transparencia. Los grupos corporativos deben estar en condiciones de demostrar que los interesados tienen conocimiento de que los datos personales se están comunicando a otros miembros del grupo empresarial fuera de la UE sobre la base de las autorizaciones de las autoridades de protección de datos, fundamentadas en normas corporativas jurídicamente exigibles, cuya existencia y contenido debe ser de fácil acceso para individuos.

  Este deber particularizado de proporcionar información significa que, sin perjuicio del acceso a las NCV en su conjunto, los grupos corporativos deben estar en condiciones de demostrar que las personas tienen información fácilmente accesible sobre las principales obligaciones de protección de datos asumidas por el grupo corporativo, información actualizada con respecto a los miembros vinculados por las normas y los medios disponibles para los interesados a fin de verificar el cumplimiento de las reglas.
- Procedimiento de coordinación entre autoridades nacionales, recogido en el art. 26.3 de la Directiva. La idea principal de estos procedimientos es permitir a las empresas pasar por un proceso de solicitud de un permiso a través de una autoridad de protección de datos de un Estado miembro que, a través del proceso de coordinación entre las autoridades de protección de datos implicadas, conduzca a la concesión de permisos del resto de autoridades de los Estados miembros donde operen estas

empresas. Los detalles del procedimiento se determinarán puntualmente caso por caso por las autoridades de protección de datos involucradas.

5.3 Documentos de trabajo posteriores

Tras el WP 74, el GT 29 ha ido publicando otros trabajos que no han hecho sino completar y actualizar los contenidos de este en relación con las NCV con carácter general entre las que destacaremos, los siguientes:

- WP 133, de 10 de enero de 2007: Recomendación 1/2007 sobre la Solicitud Estándar para la Aprobación de Normas Corporativas Vinculantes para la Transferencia de Datos Personales.
- WP 154, de 24 de junio de 2008: Documento de trabajo que establece un marco para la estructura de las NCV.
- WP 244, de 13 de diciembre de 2016 (actualizado el 5 de abril de 2017): Directrices para determinar la autoridad de control principal de un responsable o encargado del tratamiento.
- WP 107, de 14 de abril de 2005: Documento de trabajo por el que se establece un procedimiento de cooperación para la emisión de dictámenes comunes sobre las garantías adecuadas que resultan de las NCV.
- WP 195a, de 17 de septiembre de 2012: Recomendación 1/2012 sobre el formulario de aplicación estándar para la aprobación de las NCV para la transferencia de datos personales para actividades de tratamiento.
- WP 108, de 14 de abril de 2005: Documento de trabajo por el que establece una lista de comprobación (*checklist*) modelo para la solicitud de aprobación de las NCV.
- WP 212, de 27 de febrero de 2014: Dictamen 02/2014 sobre un documento de referencia para los requisitos en materia de NCV presentadas a las autoridades nacionales de protección de datos en la UE y normas de privacidad transfronterizas remitidas a los agentes de rendición de cuentas de dichas normas de la APEC.

Los WP 107 y 108 ayudaron a establecer los criterios para: a) la elección de la autoridad de protección de datos que iba a liderar el proceso de autorización; b) el tratamiento de las cuestiones a desarrollar por el solicitante para la evaluación de su adecuación por las autoridades de protección de datos implicadas en el proceso de autorización; y c) el establecimiento de unas directrices para la cooperación entre las autoridades implicadas.

Por tanto, dichos documentos de trabajo establecieron que los criterios para decidir cuál es la autoridad de control competente son los siguientes (considerando siempre que el primero es el más importante):

- La ubicación de su sede principal europea del grupo.
- Si la sede no se encontrara en la UE o el Espacio Económico Europeo, el grupo empresarial debe designar un miembro europeo con responsabilidades delegadas en materia de protección de datos, de tal forma que sea el encargado de asegurarse de que cualquier miembro del grupo fuera y dentro de la UE ajuste sus actividades de tratamiento a los compromisos del grupo, colaborando con la autoridad de control líder cuando proceda y abonando una indemnización en caso de daños resultantes del incumplimiento de las NCV por cualquier miembro del grupo.
- La ubicación de la compañía dentro del grupo con responsabilidades delegadas en materia de protección de datos.
- La ubicación de la compañía que esté mejor situada (en términos de funciones de gestión o de cargas administrativas) para gestionar la solicitud y exigir el cumplimiento de las NCV en el grupo.
- El lugar donde se adoptan más decisiones en términos de finalidades y medios del tratamiento de datos personales.
- Los Estados miembros en la UE desde donde se realizan más transferencias fuera del EEE.

Aunque el grupo de empresas que solicite la autorización tiene que justificar siempre el motivo de elección de la autoridad de control, la autoridad elegida siempre puede decidir si efectivamente es la más apropiada o no para liderar el proceso de autorización. O, incluso, las autoridades pueden decidir entre ellas cuál es la más competente, con independencia de cuál haya sido elegida por el grupo empresarial.

En cualquier caso, hay que tener en cuenta que, cuando se decidieron estos criterios, fue siempre con la intención de tener seguridad jurídica, para evitar el conocido como "*forum shopping*"[11], es decir, que las empresas se dirijan a la autoridad de control que les parezca más favorable para sus intereses.

La autorización de las NCV requiere asimismo presentar los flujos de información en el tratamiento de datos y las garantías individuales y mecanismos para atender las quejas de los

[11]El *forum shopping* es un concepto propio del Derecho internacional privado, que explica la situación en que una persona que inicia una acción puede verse tentada a elegir un foro no porque sea el más adecuado para conocer del litigio, sino porque las normas sobre conflictos de leyes que este tribunal utilizará llevarán a la aplicación de la ley que más le convenga - http://ec.europa.eu/civiljustice/glossary/glossary_es.htm .

afectados. A la hora de analizarlas, debe destacarse que la revisión debe de hacerse a la luz de lo dispuesto en la Directiva 95/46/CE:

> Cualquier requisito adicional que se derive del respectivo Derecho nacional de un Estado miembro no puede ni debe ser objeto de debate entre las autoridades en el contexto del procedimiento de cooperación europeo. Estos requisitos específicos conforme al respectivo Derecho nacional, en cambio, deberían ser recogidos por las distintas autoridades en una 'lista de comprobación conforme a la normativa nacional'. Este documento complementario podría ser entregado a las entidades junto con la 'Lista de comprobación modelo' que se acaba de aprobar. Así, las empresas podrán adaptarse a tiempo a los requisitos nacionales una vez que el reglamento corporativo haya sido homologado conforme al mecanismo de coordinación europeo[12].

El GT 29 ha publicado también una serie de documentos especialmente destinados tanto al responsable como al encargado del tratamiento:

- Para el responsable:
    - WP 256, de 29 de noviembre de 2017: Documento de trabajo que establece una tabla con los elementos y principios a incluir en las NCV.
    - WP 153, de 24 de junio de 2008: Documento de trabajo que establece una tabla con los elementos y principios a incluir en las NCV.
- Para el encargado:
    - WP 257, de 29 de noviembre de 2017: Documento de trabajo que establece una tabla con los elementos y principios a incluir en las NCV para encargados del tratamiento.
    - WP 204, de 19 de abril de 2013 (actualizado el 22 de mayo de 2015): Documento explicativo sobre las NCV para encargados del tratamiento.
    - WP 195, de 6 de junio de 2012: Documento de trabajo 02/2012 que establece una tabla con los elementos y principios a incluir en las NCV para encargados del tratamiento[13].

[12] Gardain, A.M. (2005). Transferencia de datos personales a países terceros. Reglamentos Corporativos de Carácter Obligatorio ¿Nuevos instrumentos jurídicos? ¿Derecho aplicable? Datospersonales.org: La revista de la Agencia de Protección de Datos de la Comunidad de Madrid, n.17, pp. 38-42.

[13] Pero son muchas más las publicaciones del GT 29 relacionadas con las NCV: Programa de trabajo de 2004 (WP 92), de 17 de marzo de 2004; Document Strategy (WP 98) de 29 de septiembre de 2004; Programa de trabajo para 2005 (WP 109) de 14 de abril de 2005; Programa de trabajo 2006-2007 (WP 120), de 5 de abril de 2006; Programa de trabajo 2008-2009 (WP 146), de 18 de febrero de 2008.

Por su parte, el 25 de noviembre de 2004, se publicó el WP 102, que establece el *Model Checklist Application for approval of Binding Corporate Rules*, un documento para grupos de empresas que recoge los contenidos que se deben dar y probar en una solicitud de autorización de NCV. En dicho texto se establece el contenido del compromiso, tanto interno como externo, que establecen las NCV, es decir, tanto a efectos internos del grupo como frente a las personas afectadas.

Como podemos observar, el GT 29 ha dedicado tiempo y esfuerzos para ir diseñando un modelo base de NCV que va adaptándose a las novedades legislativas que han ido acompañando la regulación de la protección de datos hasta la publicación del nuevo RGPD.

Con la entrada en vigor de este, va a ser clave el Comité Europeo de Protección de Datos, del que forma parte el GT 29, para que los documentos de trabajo ya publicados se adapten e interpreten conforme a la nueva legislación y esta se pueda aplicar a las NCV. Así el art. 70 RGPD recoge las funciones del Comité Europeo de Protección de Datos, y en su apartado 1.i) dice que:

> Emitirá directrices, recomendaciones y buenas prácticas (…) con el fin de especificar en mayor medida los criterios y requisitos para las transferencias de datos personales basadas en normas corporativas vinculantes a las que se hayan adherido los responsables del tratamiento y en normas corporativas vinculantes a las que se hayan adherido los encargados del tratamiento y en requisitos adicionales necesarios para garantizar la protección de los datos personales de los interesados a que se refiere el artículo 47. [14]

Además, cabe destacar en este momento lo establecido en el art. 64.1.f) RGPD:

> El Comité emitirá un dictamen siempre que una autoridad de control competente proyecte adoptar alguna de las medidas enumeradas a continuación. A tal fin, la autoridad de control competente comunicará el proyecto de decisión al Comité, cuando la decisión: (…) tenga por objeto la aprobación de normas corporativas vinculantes (…)[15].

Es decir, que cuando una autoridad de control quiera autorizar unas NCV tendrá que pedir al Comité que emita un dictamen, aunque la experiencia de estos años demuestra que los países integrantes del Espacio Económico Europeo vienen reconociendo las NCV que se van

[14] Art. 70.1. i) RGPD
[15] Art. 64.1.f) RGPD

autorizando entre sus componentes, asumiendo que todos tienen un nivel de control equiparable.

Para finalizar este punto destacaremos que el pasado 29 de noviembre de 2017, el GT 29 actualizó documentos relativos a las NCV para responsables y encargados, atendiendo a la entrada en vigor del RGPD: WP 256 y WP 257. Ambos documentos están concebidos con la misma finalidad:

- Actualizar los documentos anteriores.
- Adaptar el contenido de las NCV al art. 47 del RGPD.
- Distinguir el contenido que debe incluirse en las NCV y en la solicitud que se presente a la autoridad de supervisión competente.
- Proporcionar explicaciones y comentarios para cada principio.

6 RGPD y novedades respecto a las NCV

La entrada en vigor del RGPD ha supuesto la introducción en la regulación europea de una serie de principios y valores que implican la necesidad de una adaptación de los textos que el GT 29 había publicado en relación con las NCV.

EL RGPD establece que la autoridad de control competente aprobará normas corporativas vinculantes siempre que estas sean jurídicamente vinculantes y se apliquen y sean cumplidas por todos los miembros correspondientes del grupo empresarial dedicadas a una actividad económica conjunta, incluidos sus empleados; confieran expresamente a los interesados derechos exigibles en relación con el tratamiento de sus datos personales, y cumplan los requisitos siguientes[16]:

- Especifiquen la estructura y los datos de contacto del grupo empresarial y de cada uno de sus miembros;
- Detallen las transferencias o conjuntos de transferencias de datos, incluyendo las categorías de datos personales, el tipo de tratamientos y sus fines, el tipo de interesados afectados y el nombre del tercer o los terceros países en caso de que salgan de la UE.
- Aseguren que tienen carácter jurídicamente vinculante, tanto a nivel interno como externo, es decir, que son exigibles entre los miembros del grupo, así como ante las solicitudes de terceros (por ejemplo, titulares de derechos que quieran ejercerlos.

[16] Art. 47 RGPD

- Se les aplicarán los principios generales en materia de protección de datos, en particular la limitación de la finalidad, la minimización de los datos, los periodos de conservación limitados, la calidad de los datos, la protección de los datos desde el diseño y por defecto, la base del tratamiento, el tratamiento de categorías especiales de datos personales, las medidas encaminadas a garantizar la seguridad de los datos y los requisitos con respecto a las transferencias ulteriores a organismos no vinculados por las normas corporativas vinculantes;
- Se reconocerán los derechos de los interesados en relación con el tratamiento y los medios para ejercerlos, como el derecho a no ser objeto de decisiones basadas exclusivamente en un tratamiento automatizado, incluida la elaboración de perfiles, el derecho a presentar una reclamación ante la autoridad de control competente y ante los tribunales competentes de los Estados miembros, y el derecho a obtener una reparación, y, cuando proceda, una indemnización por violación de las normas corporativas vinculantes;
- Se establecerá que haya un responsable o encargado del tratamiento, que, como residente en el territorio de un Estado miembro, asuma la responsabilidad por cualquier violación de las normas corporativas vinculantes por parte de cualquier miembro no establecido en la Unión; el responsable o el encargado solo será exonerado, total o parcialmente, de dicha responsabilidad si demuestra que el acto que originó los daños y perjuicios no es imputable a dicho miembro;
- Se facilitará a los interesados la información sobre las normas corporativas vinculante.
- Se recogerán las funciones del delegado de protección de datos (DPO) o de cualquier otra persona o entidad encargada de la supervisión del cumplimiento de las normas corporativas vinculantes dentro del grupo empresarial, así como de la supervisión de la formación y de la tramitación de las reclamaciones;
- Se incluirán también los procedimientos de reclamación;
- Asimismo, incluirán los mecanismos para garantizar la verificación del cumplimiento de las normas corporativas vinculantes. Dichos mecanismos incluirán auditorías de protección de datos y métodos para garantizar acciones correctivas para proteger los derechos del interesado. Los resultados de dicha verificación deberían comunicarse a la persona o entidad encargada de la supervisión del cumplimiento de las normas, sea el DPO u otra, y al consejo de administración de la empresa que controla un grupo empresarial, y ponerse a disposición de la autoridad de control competente que lo solicite.

- Se deben contemplar también los mecanismos establecidos para comunicar y registrar las modificaciones introducidas en las normas y para notificar esas modificaciones a la autoridad de control;
- Deben prever un mecanismo de cooperación con la autoridad de control para garantizar el cumplimiento por parte de cualquier miembro del grupo, en particular poniendo a disposición de la autoridad de control los resultados de las verificaciones de las medidas de supervisión.
- Adicionalmente, se debe hacer referencia a los mecanismos para informar a la autoridad de control competente de cualquier requisito jurídico de aplicación en un país tercero a un miembro del grupo, que probablemente tengan un efecto adverso sobre las garantías establecidas en las normas corporativas vinculantes,
- Por último, deben incluir la formación en protección de datos pertinente para el personal que tenga acceso permanente o habitual a datos personales.

7 Adaptación de las NCV a la nueva normativa: los WP 256 y 257

Así, el 29 de noviembre de 2017, como ya dijimos, se publicaron los WP 256 y 257, que lo que pretenden es adaptar el uso de las NCV para Responsables y Encargados, respectivamente[17]. Por tanto, vamos a proceder a analizar como el GT 29 ha recogido los principios de la nueva normativa y los ha trasladado al ámbito de las NCV.

7.2 Las NCV para responsables (BCR-C)

Lo primero que hace el WP 256 es indicar que las obligaciones que recoge se aplican a las entidades que, dentro del grupo, actúan como responsables y sus relaciones con las que actúan como encargados. En cuanto a este último caso, vale la pena recordar que un contrato u otro acto jurídico conforme a la legislación de la Unión o de algún Estado miembro, vinculante para el encargado con respecto al responsable y que comprende todos los requisitos establecidos en el RGPD[18], debe firmarse con todos los encargados o sub-encargados, ya sean internos o externos.

[17] Siguiendo sus siglas en inglés, se conocen como "NCV-C – *Binding Corporative Rules – Controllers*" las referidas a los responsables del tratamiento de los datos, mientras que las "NCV-P – *Binding Corporative Rules – Processors*" las relativas a los encargados del tratamiento.
[18] Art. 28.3 RGPD

Teniendo en cuenta que el RGPD establece un conjunto mínimo de requisitos que deben cumplir las NCV[19], el WP 256 lo que pretende es:

- Ajustar la redacción de la terminología usada en los trabajos anteriores, para que sea acorde con el RGPD.
- Aclarar el contenido necesario de las NCV, teniendo en cuenta los documentos WP 74 y WP 108 adoptados por el GT 29 en el marco de la Directiva 95/46 / CE.
- Hacer la distinción entre lo que debe incluirse en las NCV y lo que debe presentarse a la Autoridad de control competente en la solicitud de NCV (WP 133), es decir, el contenido propiamente de las NCV y el contenido del formulario de solicitud de aprobación, ya que no siempre coinciden.
- Dar a los principios su contenido correspondiente.
- Explicar y comentar, uno a uno, los nuevos principios.

El art. 47 RGPD, regulador de esta materia, está claramente inspirado en los documentos de trabajo relacionados con las NCV aprobados por el GT 29. Sin embargo, especifica algunos elementos nuevos que deben tenerse en cuenta al actualizar las NCV existentes o al adoptar nuevos conjuntos de NCV para garantizar su compatibilidad con el nuevo marco establecido por el RGPD.

Estas novedades se resumen en los siguientes puntos:

- Derecho a presentar una reclamación: los sujetos interesados (titulares de los datos) deberían poder presentar su reclamación ante la autoridad de control en el Estado miembro de su residencia habitual, lugar de trabajo o lugar de la presunta infracción[20] o ante el tribunal competente de los Estados miembros de la UE (a elección del interesado, para actuar ante los tribunales donde el exportador tenga un establecimiento o donde el interesado tenga su residencia habitual[21];
- Transparencia: los interesados deben recibir, en particular, la información estipulada en los artículos 13 y 14 RGPD e información sobre sus derechos en cuanto al ejercicio y los medios para ejercerlos.
- Ámbito de aplicación: las NCV deben especificar la estructura y los datos de contacto del grupo de empresas o grupo de empresas que participan y de cada uno de sus miembros[22]. Las NCV también deben especificar su alcance material, por ejemplo, las

[19] Art. 47.2 RGPD
[20] Art. 77 RGPD
[21] Art 79 RGPD
[22] Art. 47.2.a RGPD

transferencias de datos o el conjunto de transferencias, incluidas las categorías de datos personales, el tipo de procesamiento y sus fines, los tipos de datos afectados y la identificación de los destinatarios en el tercer país o países[23].

- Principios de protección de datos: junto con los principios de transparencia, legitimidad, limitación de objetivos, calidad de los datos y seguridad, las NCV también deben explicar los otros principios a los que se hace referencia en el artículo 47.2.d, como, en particular, los principios de legalidad, minimización de datos, períodos de almacenamiento limitados, garantías al procesar categorías especiales de datos personales o los requisitos con respecto a las transferencias posteriores a organismos no sujetos a las NCV.
- Rendición de cuentas o *accountability*: como dice el art. 5.2 RGPD: "El responsable del tratamiento será responsable del cumplimiento de lo dispuesto en el apartado 1 y capaz de demostrarlo ('responsabilidad proactiva')" [24].
- Legislación de terceros países: las NCV deben contener el compromiso de que, cuando exista un requisito legal de un tercer país aplicable a algún miembro del grupo de empresas, que pueda tener un efecto adverso sustancial a las garantías proporcionadas por las NCV, se informará a la autoridad de control competente (a menos que se prohíba lo contrario, como una prohibición en virtud del derecho penal para preservar la confidencialidad de una investigación policial). Esto incluye cualquier solicitud legalmente vinculante para la divulgación de datos personales por parte de una autoridad encargada de hacer cumplir la ley o un organismo de Seguridad del Estado.

Y, ¿qué establece el Reglamento en relación con las NCV que ya están en vigor? Las autorizaciones de un Estado miembro o una autoridad de control basadas en la Directiva 95/46/CE[25] seguirán siendo válidas hasta su modificación, sustitución o derogación, los grupos con NCV aprobados deberían, al prepararse para el RGPD, alinear sus NCV con los requisitos del RGPD[26].

En cualquier caso, las NCV para responsables deben cumplir una serie de requisitos que procedemos a explicar:

[23] Art. 47.2.b RGPD
[24] Art. 5.2 RGPD
[25] Art. 26.2 Directiva 95/46 CE
[26] Art. 46.5 RGPD

7.1.1. Naturaleza Vinculante

- Interna[27]

Las NCV deben ser legalmente vinculantes para cada miembro integrante del grupo corporativo, incluyendo sus empleados. Para ello, el grupo debe explicar cómo se va a asegurar el fiel cumplimiento de las NCV. Esto se puede hacer de diversas formas:

- Para las compañías, mediante un acuerdo intragrupo o mediante compromisos unilaterales, en el caso de que la empresa que lo asuma se encuentre en un Estado miembro que lo reconoce como vinculante y si este miembro del grupo puede legalmente obligar a otros miembros sujetos a las NCV. Se podrán usar otros medios si se logra demostrar el carácter vinculante de las NCV.
- Para los empleados, mediante acuerdos individuales, cláusulas en el contrato de trabajo, políticas internas o convenios colectivos. En todo caso, se especificarán las posibles sanciones en caso de incumplimiento.

Estas informaciones se deben incluir tanto en la solicitud de autorización de la NCV ante la autoridad de control como en la propia NCV. No será necesario incluir una explicación adicional en la NCV de cómo se piensa hacer efectiva la normativa, pero sí en la solicitud, para que la autoridad de control lo pueda valorar.

- Externa

Las NCV deben conferir expresamente derechos a los sujetos titulares de los datos para que puedan hacer cumplir las NCV como terceros beneficiarios. Esta información debe estar incluida tanto en la solicitud de autorización de las NCV, como en ellas mismas. Estos sujetos de datos deben ser capaces de hacer cumplir los siguientes elementos:

- Principios de protección de datos[28]
- Transparencia y accesibilidad a las NCV[29]
- Derechos de acceso, rectificación, supresión, restricción, limitación, oposición, portabilidad y derecho a no estar sujeto a decisiones basadas únicamente en el procesamiento automatizado, incluidos los perfiles[30]
- Que la legislación nacional no impida el respeto de las NCV[31]

[27] art. 47.1.a y 47.2.c RGPD
[28] art. 47.2.d RGPD.
[29] art.47.2. g RGPD.
[30] Art. 47.2.e, 15, 16, 17,18, 21, 22 RGPD

- Derecho a quejarse a través del mecanismo interno de quejas de las empresas[32]
- Deberes de cooperación con la autoridad de protección de datos competente[33]
- Deben posibilitar el derecho a presentar una denuncia ante la autoridad de control competente[34], (a elección entre el Estado miembro de su residencia habitual, lugar de trabajo o lugar de la presunta infracción, de conformidad con el artículo 77 del RGPD) y ante el tribunal competente de los Estados miembros de la UE (a elección del interesado para actuar ante los tribunales cuando el responsable del tratamiento o procesador tenga un establecimiento o cuando el interesado tenga su residencia habitual de conformidad con el RGPD[35]

Además de lo dicho en este punto, se debe reconocer en las NCV el derecho a obtener una reparación e, incluso, en los casos que corresponda, una indemnización[36].

No se debe entender que estos derechos se extiendan a aquellos elementos de las NCV que pertenecen a los mecanismos internos implementados dentro de las entidades, tales como los detalles de la capacitación, los programas de auditoría, la red de cumplimiento y el mecanismo para la actualización de las reglas.

Se deberá nombrar la sede del grupo en la UE o el miembro que tenga la función de aceptar la responsabilidad y acordar tomar las medidas necesarias para remediar los actos de otros miembros fuera de la UE vinculados por las NCV y para pagar una compensación por cualquier daño material o no material resultante de la violación de las NCV por parte de los miembros del NCV[37]. Esta información debe constar tanto en el formulario de solicitud, como en la propia normativa.

Las NCV también deben nombrar un miembro que sea responsable, dentro de la UE, que pueda responder por todos aquellos miembros de las NCV que se encuentren fuera y las hayan violado. En este caso, este miembro responsable tiene que demostrar que tiene activos suficientes para pagar una compensación por daños resultantes del incumplimiento de ese otro miembro, así como tiene la carga de la prueba para demostrar que el miembro situado fuera de la UE no es responsable de ninguna violación de las reglas que haya provocado la reclamación del interesado. Si lo demuestra, se libra de la responsabilidad.

---

[31] Art. 47.2.m RGPD
[32] Art. 47.1.j RGPD
[33] Art. 47.2.k RGPD
[34] Art. 47.2. e RGPD
[35] Art. 79 RGPD
[36] Arts 77 a 82 RGPD
[37] Art. 47.2.f RGPD

Otra posibilidad, en caso de que no sea posible que el grupo corporativo imponga a una entidad específica asumir toda la responsabilidad por cualquier incumplimiento de las NCV fuera de la UE, es que se estipule que cada miembro del grupo que exporte datos de la UE sobre la base de las NCV será responsable de cualquier incumplimiento de estas por parte del miembro del grupo establecido fuera de la UE que recibió esos datos.

Según la nueva normativa[38], todos aquellos interesados titulares de derechos deben tener fácil acceso a las NCV, a la información requerida por el RGPD[39], información relativa al tratamiento de sus datos personales y sobre los medios para ejercer esos derechos, la cláusula relativa a la responsabilidad y las cláusulas relativas a los principios de protección de datos. La información debe ser completa y no solo resumida.

7.1.2. Eficacia

Siguiendo lo establecido en el RGPD, el grupo corporativo deberá proporcionar la formación adecuada sobre las NCV al personal que tiene acceso permanente o regular a datos personales, que están involucrados en la recopilación de datos o en el desarrollo de herramientas utilizadas para procesar datos personales. [40]

Las autoridades de control que evalúan las NCV pueden solicitar ejemplos y explicaciones del programa de formación durante el procedimiento de solicitud. Dicho programa debe especificarse en la aplicación. Asimismo, se debe establecer un proceso interno de gestión de reclamaciones que garantice que cualquier persona pueda ejercer sus derechos[41]. Estas reclamaciones deben ser atendidas, sin demora indebida y, en cualquier caso, dentro de un mes, por un departamento o persona claramente identificada con un nivel apropiado de independencia en el ejercicio de sus funciones. Teniendo en cuenta la complejidad y el número de solicitudes, ese período de un mes puede ampliarse como máximo en dos meses más, en cuyo caso el interesado debe ser informado en consecuencia. El formulario de solicitud debe explicar cómo se informará a los interesados sobre los pasos prácticos del sistema de quejas, en particular:

- Dónde quejarse
- De qué forma
- Retrasos en la respuesta a la reclamación

[38] Art. 47.2.g RGPD
[39] Arts 13 y 14 RGPD
[40] Art. 47.2.n RGPD
[41] Arts 47.2.i y 12.3 RGPD

- Consecuencias en caso de rechazo de la reclamación
- Consecuencias en caso de que la reclamación se considere justificada
- Consecuencias si el interesado no está satisfecho con las respuestas (derecho a presentar un recurso ante el Tribunal y una denuncia ante la autoridad de control).

Igualmente, debe existir un programa de auditoría recogido en las NCV[42]. Las NCV deben crear una obligación de tener auditorías de protección de datos regularmente (por auditores acreditados internos o externos) o por solicitud específica del encargado de proteger la privacidad en la empresa para garantizar verificación del cumplimiento con las NCV. En las NCV se debe recoger que el programa de auditoría cubre todos los aspectos de estas, incluidos los métodos para garantizar que se llevarán a cabo acciones correctivas. Además, el resultado se comunicará al encargado de proteger la privacidad y al consejo de dirección de la empresa correspondiente. Cuando sea apropiado, el resultado puede ser comunicado al consejo de dirección del grupo.

Las NCV deben indicar que las autoridades de control pueden tener acceso a los resultados de la auditoría previa solicitud y otorgarles el poder para llevar a cabo una auditoría de protección de datos de cualquier miembro de NCV, si es necesario.

El formulario de solicitud contendrá una descripción del sistema de auditoría. Por ejemplo:

- ¿Qué entidad (departamento dentro del grupo) decide sobre el plan / programa de auditoría?
- ¿Qué entidad realizará la auditoría?
- Hora de la auditoría (regularmente o a pedido específico de la función de privacidad apropiada).
- Cobertura de la auditoría (por ejemplo, aplicaciones, sistemas de TI, bases de datos que procesan Datos Personales, o transferencias posteriores, decisiones tomadas con respecto al requisito obligatorio según las leyes nacionales que entra en conflicto con las NCV, revisión de los términos contractuales utilizados para las transferencias del Grupo
- Qué entidad recibirá los resultados de las auditorías

Se establece el compromiso para designar un DPO cuando sea necesario de acuerdo con el artículo 37 RGPD, o cualquier otra persona o entidad (como un jefe de privacidad) con la

[42] Arts. 47.2.j y l y 38.3 RGPD

responsabilidad de monitorear el cumplimiento de las NCV que gozan del más alto apoyo administrativo para el cumplimiento de esta tarea[43].

El DPO u otros profesionales de la privacidad pueden ser asistidos por un equipo, o una red de contactos locales, según corresponda, e informará directamente al más alto nivel de gestión[44]. Las NCV deben incluir una breve descripción de la estructura interna, el rol, la posición y las tareas del DPO o función similar y la red creada para garantizar el cumplimiento de las reglas. Así, por ejemplo, se señalaría que: el DPO o jefe de privacidad informa y asesora a la alta gerencia, se ocupa de las investigaciones, supervisores e informes anuales de las autoridades de control sobre el cumplimiento a nivel mundial, y que los contactos locales pueden encargarse de las reclamaciones locales de los sujetos de los datos, informando sobre temas importantes de privacidad, monitoreando la capacitación y el cumplimiento a nivel local.

7.1.3. Deber de cooperación

Las NCV deben contener una obligación clara para todos los miembros de cooperar, aceptar ser auditados por las autoridades de control y cumplir con el consejo de estas sobre cualquier asunto relacionado con las NCV[45].

7.1.4. Descripción del tratamiento y del flujo de datos

Tanto en las NCV como en el formulario de solicitud se especificará su alcance material, con una descripción general de las transferencias para que las autoridades de control puedan evaluar que el procesamiento llevado a cabo en terceros países sea conforme[46].

Se detallarán, no solo las transferencias de datos o el conjunto de transferencias, sino también la naturaleza y categorías de los datos personales, el tipo de procesamiento y sus propósitos, los tipos de datos afectados (datos relacionados con empleados, clientes, proveedores y otros terceros) y la identificación de los destinatarios en el tercer país o países.

Asimismo, deberán contener la estructura y los detalles de contacto del grupo de empresas y de cada uno de sus miembros y especificarán si se aplican a todos los datos personales transferidos desde la Unión Europea dentro del grupo o a todo el procesamiento de datos personales dentro del grupo.

[43] Arts. 47.2.h y 38.3 RGPD
[44] Art. 38.3 RGPD
[45] Art. 47.2.1. RGPD
[46] Art. 47.2.a y b RGPD

7.1.5. Mecanismos para informar y guardar cambios

Las propias NCV deben prever un proceso para ser actualizadas[47]. Cuando estas se modifican, por los motivos que sea, (por ejemplo, porque haya un cambio en la estructura de la empresa o en la legislación aplicable), se debe informar de los cambios, tanto a los miembros del grupo corporativo, como a las autoridades de control competentes. En estos casos, no va a ser necesario volver a pedir autorización de estas siempre que se cumplan estos requisitos:

- Que haya una persona identificada que mantenga una lista completamente actualizada de los miembros del grupo corporativo adscritos a las NCV, que realice un seguimiento y registre las actualizaciones de las NCV, proporcionando la información necesaria a los titulares interesados y autoridades de control.
- Que no se realice ninguna transferencia a un nuevo miembro del grupo hasta que esté vinculado a las NCV y pueda cumplir sus requisitos.

Cualquier cambio en las NCV o en la lista de miembros del NCV debe informarse una vez al año a la autoridad de control competente con una breve explicación de los motivos que justifican la actualización. Cuando una modificación sea susceptible de afectar el nivel de la protección ofrecida por las NCV o afecte significativamente a las mismas (es decir, los cambios en el carácter vinculante), debe comunicarse rápidamente a la autoridad de control competente.

7.1.6. Garantías para la protección de datos

Estas garantías deben estar basadas en los principios recogidos en el Reglamento, tal y como establece el art. 47.2.d RGPD, y se deben incluir tanto en las NCV como en la solicitud de autorización. La redacción y las definiciones de los principios clave deben ser coherentes con la redacción y las definiciones del Reglamento. Dichos principios no son otros que:

- Transparencia, legitimidad y licitud[48].
- Limitación del propósito[49].
- Minimización y veracidad de los datos[50].
- Períodos de almacenamiento limitados[51].

[47] Art. 47.2.k RGPD
[48] Art. 5.1.a, 6, 9, 10, 13 y 14 RGPD
[49] Art.5.1. b RGPD
[50] Art.5.1.c y d RGPD

- Tratamiento de categorías especiales de datos personales
- Seguridad[52], que incluye la obligación de celebrar contratos con todos los subcontratistas internos y externos que cumplan todos los requisitos establecidos en el RGPD[53] y también la obligación de notificar sin demoras cualquier violación de datos personales a la sede de la UE o al miembro del grupo empresarial con responsabilidades delegadas de protección de datos y al encargado de privacidad y a los titulares de los datos donde es probable que se produzca una violación de datos personales en alto riesgo. Además, cualquier violación de datos personales debe ser documentada (incluyendo los hechos relacionados con la violación de datos personales, sus efectos y las medidas correctivas adoptadas) y la documentación debe ponerse a disposición de la autoridad de control que lo solicite[54].
- Restricción de transferencias y de transferencias posteriores a encargados y responsables del tratamiento que no forman parte del grupo[55].

Para demostrar el cumplimiento de las NCV, los miembros deben mantener un registro de todas las categorías de actividades de tratamiento llevadas a cabo de acuerdo con los requisitos establecidos en la normativa[56]. Este registro debe mantenerse por escrito, incluso en formato electrónico, y debe ponerse a disposición de la autoridad de control que lo solicite.

Con el fin de mejorar el cumplimiento y cuando sea necesario, las evaluaciones de impacto de protección de datos deben llevarse a cabo para las operaciones de tratamiento que tengan altas probabilidades de conllevar un riesgo para los derechos y libertades de las personas físicas[57]. Cuando la evaluación del impacto indique que la tramitación daría lugar a un riesgo elevado en ausencia de medidas adoptadas por el responsable del tratamiento para mitigar el riesgo, la autoridad de control competente, antes del procesamiento, debería ser consultada, atendiendo al art. 36 RGPD.

Deben implementarse medidas técnicas y organizativas apropiadas diseñadas para implementar principios de protección de datos y para facilitar el cumplimiento de los

[51] Art. 5.1.e RGPD
[52] Art. 5.1.f y 32 RGPD
[53] Art. 28.3 RGPD
[54] Arts. 33 y 34 RGPD
[55] Este extremo solo se podrá llevar a cabo siempre que se proporcione una protección adecuada, de acuerdo con los artículos 45, 46, 47 48 RGPD, o que se aplique una derogación según el 49 RGPD.
[56] Art. 30.1 RGPD
[57] Art. 35 RGPD

requisitos establecidos por las NCV en la práctica, es decir, se ha de garantizar la protección de datos desde el diseño y por defecto[58].

Según el RGPD[59], cuando un miembro del grupo empresarial tenga motivos para creer que la legislación aplicable le impide cumplir con sus obligaciones recogidas en las NCV o tiene un efecto sustancial en las garantías provistas por las NCV, informará de inmediato a la sede de la UE o el miembro de la UE con responsabilidades de protección de datos delegadas (excepto donde lo prohíba una autoridad de aplicación de la ley, como la prohibición del derecho penal de preservar la confidencialidad de una investigación policial).

Además, las NCV deben contener el compromiso de que cuando cualquier requisito legal al que esté sujeto un miembro del grupo empresarial en un tercer país, sea susceptible de tener un efecto adverso sustancial sobre las garantías proporcionadas por las NCV, el problema debe ser informado a la autoridad de control competente. Esto incluye cualquier solicitud legalmente vinculante para la divulgación de los datos personales por parte de una autoridad encargada de hacer cumplir la ley o un organismo de seguridad del Estado. En tal caso, se debe informar claramente a la autoridad de control competente sobre la solicitud, incluida la información sobre los datos solicitados, el organismo solicitante y la base legal para la divulgación (a menos que esté vedado, como una prohibición penal para preservar la confidencialidad de una investigación policial).

Si en casos específicos se prohíbe la suspensión y / o notificación, las NCV deberán estipular que el miembro del grupo empresarial solicitado hará todo lo posible para obtener el derecho a renunciar a esta prohibición, a fin de comunicar la mayor cantidad de información posible y lo antes posible, y ser capaz de demostrar que así fue.

Si, en los casos anteriores, a pesar de haber hecho sus mejores esfuerzos, el miembro del grupo empresarial solicitado no está en posición de notificar a las autoridades de control competentes, debe comprometerse en las NCV a proporcionar, anualmente, información general sobre las solicitudes recibidas a las autoridades de control competentes.

En cualquier caso, las NCV deben declarar que las transferencias de datos personales por un miembro del grupo a cualquier autoridad pública no pueden ser masivas, desproporcionadas e indiscriminadas de una manera que iría más allá de lo que es necesario en una sociedad democrática. Las NCV podrían indicar que, cuando la legislación de un Estado miembro o la legislación de la UE requiera un nivel más alto de protección para los datos personales, esta tendrá prioridad sobre las NCV.

[58] Art. 25 RGPD
[59] Art. 47.2.m RGPD

En cualquier caso, los datos personales se procesarán de acuerdo con la legislación aplicable según lo dispuesto en el RGPD[60] y la legislación nacional pertinente.

7 Las NCV para encargado (BCR-C)

Vamos a proceder a analizar el contenido de las obligaciones para los encargados.

7.2.1. El deber de respetar las NCV para los miembros

Las NCV serán jurídicamente vinculantes y contendrán un deber claro para cada miembro participante del Grupo de empresas, incluidos sus empleados. Esta información se incluirá tanto en las propias normas, como en el formulario de solicitud.
Las NCV también declararán, expresamente, que cada miembro, incluidos sus empleados, respetará las instrucciones del responsable con respecto al procesamiento de datos, así como las medidas de seguridad y confidencialidad que se proporcionan en el Acuerdo de Servicio[61].
El grupo de empresas tendrá que explicar en su formulario de solicitud de qué forma las NCV van a ser vinculantes:

- Cada miembro participante deberá ser parte de uno o más de estos acuerdos:
    - Acuerdo intragrupo
    - Compromisos unilaterales (esto solo es posible si el miembro que asume la responsabilidad se encuentra en un Estado miembro que reconoce compromisos unilaterales como vinculantes y si este miembro puede vincular legalmente a los demás miembros participantes de las NCV), u
    - Otros medios (solo si el grupo demuestra cómo se logra la vinculación)
- Sobre los empleados por uno o más de:
    - Acuerdo / compromiso individual y separado con sanciones, o cláusula en el contrato de empleo con sanciones, o
    - Políticas internas con sanciones, o
    - Convenios colectivos con sanciones.

7.2.2. El deber de cumplimiento de las NCV de cara a terceros

- Derechos que son directamente ejecutables contra el encargado

[60] Art. 5 RGPD
[61] Arts. 28, 29 y 32 del RGPD

Las NCV deben otorgar derechos a los titulares de los datos para hacer cumplir las NCV como terceros beneficiarios contra el encargado, donde los requisitos están específicamente dirigidos a los encargados de acuerdo con el RGPD. Esta información debe incluirse tanto en las propias NCV como en el formulario de solicitud. A este respecto, los interesados al menos podrán imponer los siguientes elementos de las NCV directamente contra el encargado:

- Deber de respetar las instrucciones del responsable con respecto al procesamiento de datos, incluidas las transferencias de datos a terceros países[62],
- Obligación de implementar medidas de seguridad técnicas y organizativas apropiadas[63] y deber de notificar cualquier infracción de datos personales al responsable[64]
- Deber de respetar las condiciones al contratar un encargado dentro o fuera del Grupo[65]
- Deber de cooperar y ayudar al responsable a cumplir y demostrar el cumplimiento de la ley, como para responder a las solicitudes de los interesados en relación con sus derechos[66]
- Fácil acceso a las NCV[67]
- Derecho a presentar una denuncia a través de mecanismos internos
- Deber de cooperar con la autoridad supervisora[68]
- Disposiciones de responsabilidad, compensación y jurisdicción[69]
- Legislación nacional que impide el respeto de NCV[70]

- Derechos que son exigibles contra el encargado en caso de que el interesado no pueda presentar un reclamo contra el responsable:

Las NCV deben conferir expresamente derechos a los titulares de datos con el objeto de cumplir las NCV como terceros beneficiarios en caso de que el interesado no pueda presentar una reclamación contra el responsable de datos, ya sea porque el responsable de datos haya desaparecido o dejado de existir, o se haya declarado insolvente. Todo ello, a menos que cualquier entidad sucesora haya asumido todas las obligaciones legales del responsable de

[62] Arts. 28.3.a, 28.3.g. y 29 RGPD
[63] Arts. 28.3.c y 32 RGPD
[64] Art. 33.2 RGPD
[65] Arts. 28.2, 28.3.d. 28.4, 45, 46 y 47 RGPD
[66] Arts. 28.3.e, 28.3.f, 28.3.h RGPD
[67] Art.47.2. g RGPD
[68] Arts. 31 y 47.2.l RGPD
[69] Arts 47.2, 79 y 82 RGPD
[70] Art.47.2.m RGPD

datos por contrato, en cuyo caso el interesado puede hacer valer sus derechos contra tal entidad. Los derechos de los titulares de los datos mencionados cubrirán los recursos judiciales por cualquier violación de los derechos de terceros beneficiarios garantizados y el derecho a obtener reparación y, cuando corresponda, recibirán una indemnización por cualquier daño (daño material pero también moral). En particular, los interesados tendrán derecho a presentar una queja ante la autoridad de control competente (elección entre la autoridad de control del Estado miembro de la UE de su residencia habitual, lugar de trabajo o lugar de la presunta infracción) y ante el tribunal competente del Estado miembro de la UE (elección del interesado para actuar ante los tribunales donde el responsable o encargado tiene un establecimiento o donde el interesado tiene su residencia habitual de conformidad con el RGPD[71]). Cuando el encargado y el responsable involucrados en el mismo tratamiento sean responsables de cualquier daño causado por dicho tratamiento, el interesado tendrá derecho a recibir una compensación por todo el daño directamente del encargado[72]

7.2.3. Responsabilidad hacia el responsable

Las NCV se vincularán con el Responsable a través de una referencia específica al mismo en el Contrato de Servicio que deberá cumplir con el RGPD[73].

El Responsable tendrá el derecho de hacer cumplir las NCV contra cualquier miembro grupo participante por infracciones que causaron (y esto se incluirá tanto en la solicitud como en las propias NCV) y, además, contra cualquier encargado externo establecido fuera de la UE.

Las NCV contendrán un deber para el encargado en la UE o miembro residente en la UE con responsabilidades delegadas o el encargado exportador de la UE para aceptar la responsabilidad y aceptar tomar las medidas necesarias para subsanar los actos o infracciones de otros miembros del grupo establecidos fuera de la UE y pagar una indemnización por los daños resultantes de una violación de las NCV.

Este miembro aceptará la responsabilidad como si la violación hubiera sido cometida por él en el Estado miembro en el que se encuentra, en lugar del miembro situado fuera de la UE o el encargado externo establecido fuera de la UE. Este miembro no puede delegar sus obligaciones en un sub-encargado (interno o externo del grupo) para evitar sus propias responsabilidades.

[71] Art 79 RGPD
[72] Art. 82.4 RGPD)
[73] Art. 28 RGPD

Si no es posible para algunos grupos con estructuras corporativas particulares imponer toda la responsabilidad por cualquier tipo de incumplimiento de las NCV fuera de la UE en una entidad específica, otra opción puede consistir en declarar que todos y cada uno de los miembros que exportan datos de la UE serán responsables de las infracciones por parte de los sub-encargados (internos o externos del grupo) establecidos fuera de la UE que recibieron los datos de este miembro del NCV de la UE.

Este responsable debe incluir en el formulario de solicitud que tiene activos suficientes para pagar una indemnización por los daños resultantes del incumplimiento de las NCV y también tendrá la carga de la prueba para demostrar que el miembro de fuera de la UE o el encargado externo no es responsable de ninguna violación de las reglas que haya resultado en la reclamación del interesado. También le tocará demostrar que el miembro de fuera de la UE o el encargado externo no fueron responsables del incumplimiento que dio lugar a dichos daños o de que no se produjo dicha violación. Si lo consigue, puede liberarse de cualquier responsabilidad.

Las NCV deben incluir la obligación de que el acceso a las mismas sea fácil para los interesados y, en particular, un fácil acceso a la información sobre los derechos de terceros beneficiarios para el interesado que se beneficia de ellos.

En cuanto el acceso para el responsable, el acuerdo de servicio garantizará que las NCV sean parte del contrato. Las NCV se anexarán al Acuerdo de servicio o se hará una referencia al mismo con la posibilidad de acceso electrónico.

El acceso a los sujetos de los datos debe ser garantizado para todos los interesados, titulares de derechos como terceros beneficiarios, que deberían recibir la información sobre el procesamiento de sus datos personales y sobre los medios para ejercer esos derechos. Se publicarán en el sitio web del Grupo de Encargados u otros medios apropiados de una manera fácilmente accesible para los interesados o al menos un documento que incluya todos (y no un resumen) de la información detallada.

7.2.4. Garantía de eficacia de las NCV

Las NCV y los formularios de solicitud deben indicar que se proporcionará la formación adecuada sobre las NCV al personal que tiene acceso permanente o regular a los datos personales que participan en la recogida de datos personales o en el desarrollo de herramientas utilizadas para procesar datos personales.

Las Autoridades de Supervisión que evalúan las NCV pueden solicitar algunos ejemplos y explicaciones del programa de formación durante el procedimiento de solicitud, y el programa de formación debe especificarse en la aplicación.

Adicionalmente, las NCV deben contemplar que exista un solo punto de contacto para todos los interesados, que abarque a todos los encargados del tratamiento.

Todos los miembros tendrán la obligación de comunicar una reclamación sin demora al responsable sin obligación de responderla (excepto si se ha acordado lo contrario con el mismo).

Las NCV contendrán un compromiso para que el Encargado responda las quejas de los sujetos titulares de los datos cuando el responsable haya desaparecido o haya dejado de existir legalmente o se haya declarado insolvente.

En todos los casos en que el encargado responda las reclamaciones, éstas serán tratadas sin demora indebida y, en cualquier caso, dentro de un mes por un departamento o persona claramente identificada que tenga un nivel apropiado de independencia en el ejercicio de sus funciones. Teniendo en cuenta la complejidad y el número de solicitudes, ese período puede prorrogarse por dos meses como máximo, en cuyo caso el interesado debe ser informado el reclamante.

El formulario de solicitud debe explicar cómo se informará a los interesados sobre los pasos prácticos del sistema de quejas, en particular:

- dónde quejarse,
- de qué forma
- retrasos en la respuesta a la queja,
- consecuencias en caso de rechazo de la queja
- consecuencias en caso de que la queja se considere justificada
- consecuencias si el interesado no está satisfecho con las respuestas (derecho a presentar un recurso ante el Tribunal / Autoridad supervisora)

Las NCV deben imponer, también, la obligación al grupo de empresas de tener auditorías de protección de datos regularmente (por auditores acreditados internos o externos) o por solicitud específica de la persona que lleve a cabo la supervisión de la privacidad (o cualquier otra función competente en la organización) para asegurar la verificación del cumplimiento de las NCV.

Las NCV deben indicar que:

- La auditoría cubre todos los aspectos incluidos en las NCV, incluidos los métodos para garantizar que se llevarán a cabo acciones correctivas.

- El resultado se comunicará a la persona encargada de supervisar la privacidad o equivalente y al consejo correspondiente de la empresa que controla al grupo de empresas, y también se pondrá a disposición del Responsable. Cuando sea apropiado, el resultado puede ser comunicado a la junta del padre principal.

Las NCV deben declarar que las Autoridades de Supervisión competentes para el Responsable pueden tener acceso a los resultados de la auditoría previa solicitud y otorgar a las Autoridades de Supervisión el poder para llevar a cabo una auditoría de protección de datos de cualquier miembro de NCV si es necesario.

Cualquier encargado o sub-encargado que procese los datos personales en nombre de un responsable en particular aceptará, a petición de ese responsable, prestar sus instalaciones de procesamiento de datos para la auditoría de las actividades de tratamiento relacionadas con ese responsable, que deberá llevar a cabo el responsable. o un organismo de inspección compuesto por miembros independientes y en posesión de las cualificaciones profesionales requeridas, obligado por un deber de confidencialidad, seleccionado por el responsable del tratamiento, en su caso, de acuerdo con la Autoridad supervisora.

El formulario de solicitud contendrá una descripción del sistema de auditoría. Por ejemplo:

- Qué entidad (departamento dentro del grupo) decide sobre el programa de auditoría,
- Qué entidad realizará la auditoría,
- Hora de la auditoría
- Cobertura de la auditoría (por ejemplo, aplicaciones, sistemas de TI, etc)
- Qué entidad recibirá los resultados de las auditorías.

7.2.5. El Delegado de Protección de Datos (DPO)

Se debe incluir en las NCV el compromiso de designar un DPO cuando sea necesario de acuerdo con el RGPD[74] o cualquier otra persona o entidad (como un jefe de privacidad) con la responsabilidad de supervisar el cumplimiento de las NCV. Esta persona o entidad deberá contar con el apoyo del más alto nivel directivo.

El DPO o esa otra persona o entidad como se menciona, respectivamente, pueden ser asistidos, en el ejercicio de esta función, por un equipo de contactos locales, según corresponda. El DPO informará directamente al más alto nivel de gestión[75].

[74] Art. 37 RGPD
[75] Art. 38.3 RGPD

7.2.6. Deber de cooperación

Las NCV contendrán una obligación clara para que todos los miembros del grupo de empresas cooperen y acepten ser auditados por las Autoridades de Supervisión competentes, además de la obligación clara para cualquier encargado o sub-encargado de cooperar y ayudar al responsable a cumplir con la normativa de protección de datos.

7.2.7. Descripción del tratamiento de datos y flujos de estos.

Las NCV contendrán una lista de las entidades que están vinculadas.
La empresa que presente unas NCV dará una descripción general a la Autoridad de Supervisión del alcance material de estas (naturaleza esperada de los datos transferidos, categorías de datos personales, tipos de datos afectados por las transferencias, tipos de tratamiento y sus fines, así como si se importan o exportan datos de la UE y de fuera.
Las NCV deberán especificar la estructura y los detalles de contacto del grupo de empresas miembros de las NCV.
Las NCV indicarán que corresponde al Responsable aplicar las NCV a:

- Todos los datos personales procesados por el o los encargados que están sometidos a la legislación de la UE (por ejemplo, los datos han sido transferidos desde la Unión Europea),
- Todo el procesamiento de datos procesados por el o los encargados dentro del grupo sea cual sea el origen de los datos.

7.2.8. Mecanismos para informar y guardar los cambios en las NCV

Las NCV se pueden modificar, pero deben imponer la obligación de informar de los cambios a todos los miembros de estas, a las Autoridades supervisoras competentes y al responsable.
Cuando un cambio afecta las condiciones de tratamiento, la información debe entregarse al responsable de manera oportuna para que tenga la posibilidad de objetar el cambio o rescindir el contrato antes de que se realice la modificación (por ejemplo, sobre cualquier cambio previsto) sobre la adición o sustitución de subcontratistas, antes de que los datos se comuniquen al nuevo encargado).
Las actualizaciones de las NCV o de la lista de miembros del NCV se permiten sin tener que volver a solicitar una autorización siempre que:

- Una persona concreta mantiene una lista completamente actualizada de los miembros del NCV y de los sub-encargados que debe ser accesible para el responsable de datos, el sujeto titular de los datos y las Autoridades de supervisión.
- Esta persona mantendrá un registro de las actualizaciones de las reglas y proporcionará la información necesaria de forma sistemática al responsable de datos y a las Autoridades de Supervisión que lo soliciten.
- No se realiza ninguna transferencia a un nuevo miembro de las NCV hasta que el nuevo miembro de NCV esté efectivamente vinculado y pueda cumplir con las normas.
- Cualquier cambio sustancial en las NCV o en la lista de miembros del NCV se debe informar una vez al año a la Autoridad de Supervisión competente con una breve explicación de los motivos que justifican la actualización. Cuando una modificación afecte el nivel de protección ofrecido por las NCV o afecte de manera significativa las NCV (es decir, cambios en la vinculación), debe comunicarse rápidamente a la Autoridad de Supervisión competente.

7.2.9. Garantías para la protección de datos

Las NCV deben incluir los siguientes principios que debe observar cualquier miembro integrante:

- Transparencia, imparcialidad y licitud, que supone que los encargados y sub-encargados tendrán la obligación general de asistir y ayudar al responsable a cumplir con la ley (por ejemplo, ser transparente acerca de las actividades del encargado para permitir que el responsable lo haga correctamente) informar al interesado);
- Limitación de propósito, que implica el deber de procesar los datos personales solo en nombre del responsable y de acuerdo con sus instrucciones documentadas, incluso con respecto a las transferencias de datos personales a un tercer país, a menos que así lo requiera la legislación de la Unión o del Estado miembro a la que el encargado está sujeto. En tal caso, el encargado informará al responsable de ese requisito legal antes de que se procese, a menos que dicha ley prohíba dicha información por motivos importantes de interés público[76]. En otros casos, si el encargado no puede proporcionar dicho cumplimiento por los motivos que sean, debe informar

[76] Art. 28.3 RGPD

oportunamente al responsable del tratamiento de esa incapacidad, en cuyo caso el responsable tiene derecho a suspender la transferencia de datos y / o rescindir el contrato.

Al finalizar la prestación de servicios relacionados con el tratamiento de datos, los encargados y sub-encargados, a elección del responsable, eliminarán o devolverán todos los datos personales transferidos al responsable y eliminarán las copias de los mismos y certificarán al responsable que lo han hecho, a menos que la legislación impuesta sobre ellos requiera el almacenamiento de los datos personales transferidos. En ese caso, los encargados y sub-encargados informarán al responsable y garantizarán la confidencialidad de los datos personales transferidos.

- Calidad de los datos, para cuyo cumplimiento los encargados y sub-encargados tendrán la obligación general de asistir y ayudar al responsable a cumplir con la ley, en estas situaciones:
    - Los encargados y sub-encargados ejecutarán las medidas necesarias cuando el responsable lo solicite, para que los datos se actualicen, corrijan o eliminen. Los encargados y sub-encargados informarán a cada miembro de las NCV a quien se le han revelado los datos de cualquier rectificación o eliminación de datos.
    - Los encargados y sub-encargados ejecutarán las medidas necesarias, cuando el responsable lo solicite, para eliminar o anonimizar los datos a partir del momento en que ya no sea necesario el formulario de identificación. El encargado y los sub-encargados se comunicarán con cada entidad a la que se hayan divulgado los datos de cualquier eliminación o anonimización de datos.
- Seguridad: los encargados y sub-encargados tendrán la obligación de implementar todas las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado a los riesgos presentados por el procesamiento según lo dispuesto en el RGPD[77]. Los encargados y sub-encargados también tendrán la obligación de ayudar al responsable a garantizar el cumplimiento de las obligaciones establecidas en los artículos 32 a 36 RGPD, teniendo en cuenta la naturaleza del tratamiento y la información disponible para el encargado[78]. Los encargados y sub-encargados deben implementar medidas técnicas y organizativas que cumplan al menos los requisitos de la ley aplicable del responsable de datos y cualquier medida particular existente

[77] Art. 32 RGPD
[78] Art.28.3. f RGPD

especificada en el Acuerdo de servicio. Los encargados deberán informar al responsable sin demora después de conocer cualquier violación de datos personales.

- Derechos de los titulares de los datos: los encargados y sub-encargados ejecutarán las medidas técnicas y organizativas adecuadas, en la medida en que sea posible, cuando el responsable lo solicite, para el cumplimiento de las obligaciones del responsable de responder a las solicitudes de ejercicio de los derechos de los titulares de los datos. establecido en el Capítulo III del RGPD[79], incluyendo la comunicación de información útil para ayudar al responsable a cumplir con el deber de respetar los derechos de los interesados. El encargado y los sub-encargados transmitirán al responsable cualquier solicitud de los titulares de los datos a menos que esté autorizado para responderla directamente.
- Sub-tratamiento dentro del Grupo: los datos pueden ser sub-procesados por otros miembros de las NCV solo con la autorización escrita o específica del responsable. El Contrato de Servicio especificará si una autorización previa general dada al comienzo del servicio sería suficiente o si se requerirá una autorización específica para cada nuevo encargado. Si se otorga una autorización general, el encargado debe informar al responsable de cualquier cambio previsto relacionado con la adición o el reemplazo de un sub-encargado de manera oportuna, de modo que el responsable tenga la posibilidad de objetar el cambio o rescindir el contrato. antes de que los datos sean comunicados al nuevo sub-encargado.
- Transferencias sucesivas a sub-encargados externos: los datos pueden ser sub-procesados por no miembros de las NCV solo con la autorización escrita o específica del responsable previamente informado. Si se otorga una autorización general, el encargado debe informar al responsable de cualquier cambio previsto relacionado con la adición o el reemplazo de los sub-encargados de manera oportuna, de modo que el responsable tenga la posibilidad de objetar el cambio o rescindir el contrato antes. los datos se comunican al nuevo sub-encargado.

Cuando el miembro de las NCV subcontrate sus obligaciones en virtud del Acuerdo de servicios, con la autorización del responsable del tratamiento, solo lo hará mediante un contrato u otro acto jurídico conforme a la legislación de la Unión o del Estado miembro con el sub-encargado que proporcione una protección adecuada según lo establecido en el RGPD[80] y que garantiza que las mismas obligaciones de protección de datos establecidas en

[79] Art. 28.3.e RGPD
[80] Arts. 28, 29, 32, 45, 46, 47 RGPD

el Acuerdo de servicios entre el responsable y el encargado se imponen al encargado, proporcionando en particular garantías suficientes para implementar medidas técnicas y organizativas apropiadas de tal manera que el tratamiento cumpla con los requisitos del RGPD[81].

Los encargados tendrán la obligación de poner a disposición del responsable toda la información necesaria para demostrar el cumplimiento de sus obligaciones[82] y permitir y contribuir a las auditorías, incluidas las inspecciones realizadas por el responsable u otro auditor ordenado por el responsable. Además, el encargado informará inmediatamente al responsable si, en su opinión, una instrucción infringe las disposiciones del RGPD u otras disposiciones de protección de datos de la Unión o los Estados miembros. Esta información debe constar tanto en el propio articulado de las NCV como en el formulario de solicitud.

Para demostrar el cumplimiento de las NCV, los miembros deben mantener un registro de todas las categorías de actividades de tratamiento llevadas a cabo en nombre de cada responsable de acuerdo con los requisitos establecidos en el RGPD[83]. Este registro debe mantenerse por escrito, incluso en formato electrónico, y debe ponerse a disposición de la autoridad de control a petición[84].

Los miembros también ayudarán al responsable a implementar medidas técnicas y organizativas apropiadas para cumplir con los principios de protección de datos y facilitar el cumplimiento de los requisitos establecidos por las NCV en la práctica, como la protección de datos por diseño y por defecto[85]

Las NCV y el formulario de solicitud contendrán la lista de las entidades vinculadas por las NCV, incluidos los detalles de contacto.

Cuando uno de estos miembros tenga razones para creer que la legislación existente o futura aplicable le puede impedir cumplir con las instrucciones recibidas del responsable o sus obligaciones impuestas por las NCV o el Contrato de Servicio, tendrá la obligación de notificar inmediatamente esto al responsable, que tiene derecho a suspender la transferencia de datos y / o rescindir el contrato, al encargado de la sede de la UE o al miembro de la UE con responsabilidades de protección de datos delegadas, pero también a la Autoridad supervisora competente para el responsable y la autoridad supervisora competente para el encargado.

[81] Art. 28 RGPD
[82] Art. 28.3.h RGPD
[83] Art.30.2 RGPD
[84] Arts.30.3 y 30.4 RGPD
[85] Arts 25 y 47.2.d RGPD

Cualquier solicitud jurídicamente vinculante de divulgación de los datos personales por una autoridad en aplicación de la ley o un organismo de seguridad del Estado se comunicará al responsable a menos que esté prohibido (como una prohibición penal para preservar la confidencialidad de una investigación policial). En cualquier caso, la solicitud de divulgación debe quedar en suspenso y la Autoridad supervisora competente para el responsable y la Autoridad supervisora competente del encargado deben estar claramente informadas sobre la solicitud, incluida la información sobre los datos solicitados, el cuerpo solicitante y la base legal para la divulgación (a menos que esté prohibido).

Las NCV deben especificar la relación entre las NCV y la ley pertinente aplicable.

Las NCV deben indicar que, cuando según la legislación local, por ejemplo, la legislación de la UE requiera un nivel más alto de protección para los datos personales, tendrá prioridad sobre las NCV.

En cualquier caso, los datos se procesarán de acuerdo con la ley aplicable.

8 Discusión

Hasta ahora hemos estado haciendo un repaso de cómo la nueva normativa europea ha contemplado la figura de las NCV y cómo el GT 29 ha adaptado su doctrina a los nuevos principios del RGPD. En el cuadro 1, que se muestra a continuación, se puede ver de forma gráfica cómo ha sido esa evolución y los diferentes aspectos que han ido regulándose hasta llegar a la actualidad:

Cuadro 1: Evolución legislativa NCV

<table>
<tr><th colspan="3">Directiva 95/46 CE, 24/10/1995</th><th colspan="2">RGPD, 27/04/2016</th></tr>
<tr><th>Primeros contenidos (Austria, Holanda y Alemania)</th><th>WP 74, 03/06/2003</th><th>WP 108, 14/04/2005</th><th>WP 256, 29/11/2017 (NCV para responsables)</th><th>WP 257, 29/11/2017 (NCV para encargados)</th></tr>
<tr><td>Criterios de homologación de NCV</td><td>mantenimiento y conservación de los libros y registros;</td><td>Checklist para solicitud de aprobación de NCV</td><td>Naturaleza Vinculante (interna y externa)</td><td>Deber de respetar las NCV</td></tr>
<tr><td rowspan="20"></td><td>veracidad y precisión en las comunicaciones con los usuarios y el gobierno;</td><td>WP 133, 10/01/2007</td><td colspan="2">Garantía de eficacia de las NCV</td></tr>
<tr><td>procedimientos para garantizar que el asesoramiento a los clientes y las decisiones comerciales no se vean afectados por conflictos de intereses;</td><td>Solicitud estándard para aprobación de NCV</td><td colspan="2">Deber de cooperación con las autoridades de control</td></tr>
<tr><td>protección de la información confidencial;</td><td>WP 153, 24/06/2008</td><td colspan="2">Descripción del tratamiento y flujo de datos</td></tr>
<tr><td>prohibición del uso indebido de los activos corporativos;</td><td>Tabla con elementos y principios a incluir en NCV</td><td colspan="2">Mecanismos para informar y guardar cambios</td></tr>
<tr><td>eliminación de discriminación y acoso impropios;</td><td>WP 195a, 17/09/2012</td><td colspan="2">Garantías para la protección de los datos</td></tr>
<tr><td>prohibición de sobornos;</td><td>Formulario de aplicación estándard de NCV</td><td></td><td>Responsabilidad ante el responsable del tratamiento</td></tr>
<tr><td>la implementación de prácticas comerciales éticas y el cumplimiento de las leyes que fomenten la competencia en el mercado;</td><td>WP 204, 19/04/2013</td><td rowspan="15"></td><td>Deber de cumplimiento de cara a terceros</td></tr>
<tr><td>prohibición del comercio de valores basado en información privilegiada</td><td>Documento explicativo de NCV para encargados de tratamiento</td><td>DPO</td></tr>
<tr><td>Sistema de auditoría interna y / o externa</td><td>WP 212, 27/02/2014</td><td rowspan="13"></td></tr>
<tr><td>Departamento de quejas</td><td>Requisitos de NCV</td></tr>
<tr><td>Designación de un responsable con sede en la UE</td><td>WP 107, 14/04/2015</td></tr>
<tr><td>Jurisdicción</td><td>Procedimiento de cooperación para dictámenes comunes sobre las garantías de las NCV</td></tr>
<tr><td>Principio de transparencia</td><td>WP 244, 13/12/2016</td></tr>
<tr><td>Procedimiento de coordinación con autoridades de control nacionales</td><td>Directrices para determinar la autoridad de control principal</td></tr>
<tr><td rowspan="2"></td><td>WP 154, 24/06/ 2018</td></tr>
<tr><td>Marco para la estructura de las NCV</td></tr>
</table>

Fuente: elaboración propia

No obstante, y, a pesar de los cambios introducidos observamos que las NCV han gozado de escasa relevancia. De hecho, si atendemos al Anexo 1, podemos comprobar que, tras años de regulación, apenas encontramos en Europa ejemplos de grupos de empresas que hayan recurrido a esta figura.

¿Cuáles son los motivos que han podido provocar dicha escasa relevancia en el panorama español y europeo? Es difícil de saber, aunque aquí apuntamos una serie de causas:

1. La propia estructura empresarial de cada país. En España, con datos de enero de 2017, podemos decir que el 99,98% de las empresas son pymes[86]. Claramente esta realidad impide que se pueda acudir a esta figura. La media de la UE está en el 99,80%, por lo que tampoco apunta a que, con este tejido empresarial, esta figura vaya a aflorar ahora.
2. La protección de datos es una materia cuya regulación cada vez es más rígida y la obligación de someter a las empresas a un marco jurídico adicional al ya establecido, en lugar de generar la percepción deseada de facilitador del proceso de transmisión de datos internacionales, ya que se puede crear la impresión que es una capa más a cumplir, un filtro que puede generar obligaciones adicionales a las legales ya previstas.
3. Burocratización para obtener la autorización. Se necesita presentar cuantiosa información, obtener la autorización de la autoridad de control competente y del resto de entidades, como hemos explicado. Esto puede suponer una burocracia que, a priori, haga desestimar esta opción.
4. Falta de cultura empresarial en materia de protección de datos. Este factor, puede ser revertido ahora con la entrada en vigor del RGPD dadas las nuevas obligaciones impuestas que han provocado que se genere un interés en la materia que antes no existía.

9 Reflexiones finales y propuestas

Tras el análisis llevado a cabo hasta ahora, consideramos oportuno retomar la idea original que motivó la creación de las NCV para valorar si esta evolución en la normativa europea ha servido para presentar a las NCV como medidas simplificadoras de procesos de autorización de transferencias internacionales de datos o, si, por el contrario, su efecto no ha sido el esperado.

Como ya hemos apuntado anteriormente, nos encontramos inmersos en un entorno de mercados globalizados, de actores interconectados procedentes de realidades muy diversas por lo que necesitamos dar una respuesta jurídica garantista que, si bien no podemos pedir que fomente, sí que podemos intentar que no desincentive el uso de los instrumentos legales que garanticen el cumplimiento de las normas.

[86] Ministerio de Economía Industria y Competitividad (2017). Retrato de la PYME. [consultado el 12 junio 2018]. Disponible en: http://www.ipyme.org/Publicaciones/Retrato-PYME-DIRCE-1-enero-2017.pdf

A lo largo de este trabajo hemos ido explicando el desarrollo de la herramienta que permite a los grupos empresariales o uniones de empresas definir un marco de actuación aplicable a las operaciones internacionales en el tratamiento de datos.

De esta forma, hemos podido comprobar que su principal finalidad es la de garantizar un nivel adecuado de protección a la vida privada y el respeto al derecho fundamental de la protección de datos personales de los ciudadanos, para lo que es necesario que se cumplan unos requisitos. Adicionalmente, con este instrumento se pretende fomentar la adopción de estándares de privacidad a una pluralidad de destinos que no cuentan con una misma normativa sobre protección de datos aplicable, o si la tienen puede responder a estándares de calidad diferentes.

Es claro el esfuerzo realizado por aquellos solicitantes de las NCV, para conseguir un tratamiento adecuado de los datos personales en entornos diversos. No podemos olvidar que las NCV incentivan a las empresas a desarrollar, de manera voluntaria, sus propios programas de protección transfronteriza de datos a nivel corporativo, adaptándose a la naturaleza de su negocio y la forma en que aprovechan la información, por encima de los estándares contemplados en la normatividad existente. Ello conlleva una serie de ventajas, como, por ejemplo, la eliminación de cláusulas contractuales tipo entre todos los integrantes del grupo de empresas, dado que las NCV permiten la libre circulación de datos basado en un único instrumento que ofrece las garantías necesarias de protección, de carácter vinculante y obligatorio, dentro, y fuera del grupo. Así, se contribuye a la generación de una cultura en la protección de datos en el grupo.

Una vez llegados a este punto, la cuestión que se plantea es: ¿son las NCV la solución que se esperaba? Si atendemos a los resultados obtenidos por las mismas, difícilmente podremos decir que sí. Los motivos ya fueron expuestos en el punto anterior de este documento.

¿De qué manera se puede revertir la situación de forma que las NCV se conviertan en un instrumento útil?

Si, como creemos, el uso de esta figura puede ayudar a facilitar y proteger la transmisión de datos personales hasta que no se instauren unos estándares de seguridad y calidad internacionales que nos permitan dejar de usar estos instrumentos, queremos hacer las siguientes propuestas:

- Creación, por parte de las agencias de control o el SEPD, de modelos de NCV al estilo de las cláusulas tipo, pre-marcando aquellas partes que sean editables de las que son imperativas. Si facilitamos su proceso de autorización fomentaremos su uso.

- Dadas las características del tejido empresarial europeo, no tiene mucho sentido, si queremos generalizar el uso de esta herramienta, que se limiten las NCV a las grandes corporaciones. Las empresas pueden tener vínculos comerciales muy sólidos y duraderos sin necesidad de formar uniones de empresas o grupos empresariales. Simplemente se basan en sus relaciones comerciales. Para la aplicación de las NCV se podrían imponer una serie de requisitos que permitieran demostrar la solidez de la relación comercial, de forma que fueran suficientes para poder justificar la aplicación de NCV.
- Procedimientos más ágiles para la recepción y resolución de quejas y reclamaciones.
- Programas de educación y formación del personal.

La entrada en vigor del RGPD, que ha dado un nuevo impulso a esta figura, creemos que ha sido una oportunidad perdida, tal y como sigue concebida, para generalizar su uso. Habría que replantear su objeto, en la manera propuesta, para poder hacer de ellas una herramienta accesible para la gran mayoría del tejido empresarial europeo.

A partir de ahora, se abre una nueva oportunidad para saber si efectivamente dichos cambios pueden afectar la escasa relevancia que, hasta ahora, han tenido las NCV.

10 Bibliografía

- Comisión europea [Internet]: "¿Qué son los datos personales?" [consultado el 12 junio 2018]. Disponible en: https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_es#referencias.
- Gardain, A.M. (2005). Transferencia de datos personales a países terceros. Reglamentos Corporativos de Carácter Obligatorio ¿Nuevos instrumentos jurídicos? ¿Derecho aplicable? Datospersonales.org: La revista de la Agencia de Protección de Datos de la Comunidad de Madrid, 17.
- Ministerio de Economía Industria y Competitividad (2017). Retrato de la PYME. [consultado el 12 junio 2018]. Disponible en: http://www.ipyme.org/Publicaciones/Retrato-PYME-DIRCE-1-enero-2017.pdf
- Recio Gayo, M. 2017: Normas Corporativas Vinculantes (BCRs): comentarios a los nuevos documentos de trabajo del GT29. Diario La Ley, Nº 1, Sección Ciberderecho, 12 de diciembre de 2017, Editorial Wolters Kluwer. Disponible en http://diariolaley.laley.es/home/DT0000260045/20171212/Wke.Presentation.WebControls.DocumentControl.Export.ashx?id=dc1 [consultado el 12 junio 2018].

- **Fuentes jurídicas utilizadas:**

Constitución Española de 1978:

Art. 18.4

Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos:

Art. 26

Art. 27

Reglamento Europeo de Protección de Datos (UE) 2016/679 del Parlamento y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos):

Art. 4.20
Art. 5
Art. 13

Art. 14
Art. 15
Art. 16
Art. 17
Art. 18
Art. 21
Art. 22
Art. 25
Art. 26
Art. 27
Art. 28
Art. 29
Art. 30
Art. 32
Art. 33
Art. 34
Art. 35
Art. 36
Art. 38
Art. 45
Art. 46
Art. 47
Art. 48
Art. 49
Art. 64.1. f
Art. 70
Art. 77
Art. 78
Art. 79
Art. 79
Art. 80
Art. 81
Art. 82

- **Jurisprudencia**

2000

STC de 30 de noviembre de 2000

- **Doctrina**

- Unión Europea. WP 74 (11639/02): Transfers of personal data to third countries: Applying Article 26 of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers. Documento adoptado por el Grupo de Trabajo del Artículo 29 el 3 de junio de 2003 [consultado el 12 junio 2018]. Disponible en:

http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2003/wp74_en.pdf

- Unión Europea. WP 244 Rev.1 (16/ES): Directrices para determinar la autoridad de control principal de un responsable o encargado del tratamiento. Documento adoptado por el Grupo de Trabajo del Artículo 29 el 13 de diciembre de 2016 y revisadas y adoptadas por última vez con fecha 5 de abril de 2017 [consultado el 12 junio 2018]. Disponible en: http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48140
- Unión Europea. WP 256 (17/EN): Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules. Documento adoptado por el Grupo de Trabajo del Artículo 29 el 29 de noviembre de 2017 [consultado el 2 de mayo 2018]. Disponible en: https://webcache.googleusercontent.com/search?q=cache:MwcuZFUkkGsJ:https://ec.europa.eu/newsroom/just/document.cfm%3Fdoc_id%3D48798+&cd=1&hl=es&ct=clnk&gl=es
- Unión Europea. WP 257 (17/EN): Working Document setting up a table with the elements and principles to be found in Processor Binding Corporate Rules. Documento adoptado por el Grupo de Trabajo del Artículo 29 el 29 de noviembre de 2017 [consultado el 2 de mayo 2018]. Disponible en: https://webcache.googleusercontent.com/search?q=cache:EBHjcEM5ICUJ:https://ec.europa.eu/newsroom/just/document.cfm%3Fdoc_id%3D48799+&cd=1&hl=es&ct=clnk&gl=es

Anexo 1

Listado de empresas con NCV aprobadas (a fecha de junio 2018)[87].

Compañía	Autoridad de Control competente
Deutsche Post DHL	BfDI (Alemania)
Deutsche Telekom	BfDI (Alemania)
Airbus (Controller)	CNIL (Francia)
Atos (Controller and Processor)	CNIL (Francia)
AXA	CNIL (Francia)
Axa Private Equito	CNIL (Francia)
BMC Software (Controller and Processor)	CNIL (Francia)
Bristol Myers Squibb	CNIL (Francia)
Capgemini (Controller and Processor)	CNIL (Francia)
CMA-CGM	CNIL (Francia)
Corning (Controller)	CNIL (Francia)
ENGIE (ex GDF SUEZ; Controller)	CNIL (Francia)
General Electric (GE)	CNIL (Francia)
Hermès	CNIL (Francia)
HP Enterprise (Controller)	CNIL (Francia)
HP Inc. (ex Hewlett Packard; Controller)	CNIL (Francia)
International SOS	CNIL (Francia)
Legrand (Controller)	CNIL (Francia)
Linkbynet (Controller and Processor)	CNIL (Francia)
LVMH	CNIL (Francia)
Michelin	CNIL (Francia)
NOVARTIS	CNIL (Francia)
OVH	CNIL (Francia)
Safran	CNIL (Francia)
Salesforce (Processor)	CNIL (Francia)
Sanofi Aventis	CNIL (Francia)
Schneider Electric	CNIL (Francia)
Société Générale	CNIL (Francia)
Sopra HR Software (ex HR Access; Controller and Processor)	CNIL (Francia)
Total	CNIL (Francia)
ArcelorMittal Group	CNPD (Luxemburgo)
e-Bay	CNPD (Luxemburgo)
Johnson Controls	DPA Belga
Mastercard (Controller and Processor)	DPA Belga
Merck Sharp & Dohme (MSD)	DPA Belga

[87] https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/binding-corporate-rules_en

Starwood Hotels and Resorts (Controller)	DPA Belga
UCB (Controller)	DPA Belga
Maersk Group	DPA Danesa
Novo Nordisk A/S	DPA Danesa
Rockwool	DPA Danesa
Continental Group	DPA de Baja Sajonia (Alemania)
BMW	DPA de Bavaria (Alemania)
Giesecke & Devrient	DPA de Bavaria (Alemania)
Osram	DPA de Bavaria (Alemania)
Siemens Group	DPA de Bavaria (Alemania)
Simon-Kucher & Partners	DPA del Norte del Rhin-Westphalia (Alemania)
ABN AMRO Bank N.V.	DPA Holandesa
Akzo Nobel N.V. (Controller)	DPA Holandesa
Align Technologies B.V. (Controller and Processor)	DPA Holandesa
BakerCorp International Holdings Inc. (Controller)	DPA Holandesa
D.E. Master Blenders 1753 ("DEMB") ex Sara Lee International B.V. (indirect subsidiary of Sara Lee Corporation	DPA Holandesa
DSM	DPA Holandesa
ING Bank N.V.	DPA Holandesa
Koninklijke DSM N.V. and affiliated companies	DPA Holandesa
LeasePlan Corporation N.V. (Controller)	DPA Holandesa
NetApp Inc. (Controller)	DPA Holandesa
Nutreco N.V.(Controller)	DPA Holandesa
Rabobank Nederland	DPA Holandesa
Royal Philips Electronics	DPA Holandesa
Schlumberger Ltd.	DPA Holandesa
Shell International B.V.	DPA Holandesa
TMF Group B.V. (Controller and Processor)	DPA Holandesa
Akastor ASA (Controller)	DPA Noruega
Aker Solutions ASA (Controller)	DPA Noruega
Kvaerner ASA	DPA Noruega
Intel Corporation	DPC (Irlanda)
Astra Zeneca plc	ICO (Reino Unido)
Accenture	ICO (Reino Unido)
American Express	ICO (Reino Unido)
Atmel	ICO (Reino Unido)
BP	ICO (Reino Unido)
CA plc	ICO (Reino Unido)
Care Fusion	ICO (Reino Unido)
Cargill, Inc.	ICO (Reino Unido)
Citigroup	ICO (Reino Unido)
Ernst & Young	ICO (Reino Unido)
First Data Corporation (Controller and Processor)	ICO (Reino Unido)
Fluor Corporation Inc.	ICO (Reino Unido)

Flextronics International Ltd	ICO (Reino Unido)
GlaxoSmithKline plc	ICO (Reino Unido)
Hyatt	ICO (Reino Unido)
IMS Health Incorporated	ICO (Reino Unido)
JPMC	ICO (Reino Unido)
Linklaters	ICO (Reino Unido)
Motorola Mobility LLC	ICO (Reino Unido)
Motorola Solutions, Inc.	ICO (Reino Unido)
Spencer Stuart	ICO (Reino Unido)
Cardinal Health, Inc.	IDPC (Malta)