Pérez-Llorca

Servicios DORA

En Pérez-Llorca somos conscientes de la magnitud y complejidad del marco normativo de la resiliencia digital de las entidades financieras, así como del reto que supone para las entidades afectadas la actualización de sus políticas, esquemas de funcionamiento y relaciones con terceros proveedores, de cara a garantizar el cumplimiento de la normativa aplicable. Por ello, hemos configurado un equipo multidisciplinar de expertos en la materia y estaremos encantados de ayudarle y acompañarle en el proceso de adaptación.

ÁMBITO DE APLICACIÓN DE DORA

Asesoramiento legal sobre el ámbito de aplicación de DORA:

1. Cuáles son las entidades que están sujetas al cumplimiento de las exigencias de DORA:
   a. desde el punto de vista de las entidades financieras (bancos, agencias de valores, infraestructuras de mercado, sociedades gestoras, entidades de pago etc.) y
   b. desde el punto de vista de los proveedores TIC esenciales (p.ej., riesgo de designación para entidades tecnológicas dentro de grupos financieros.
2. Qué entidades dentro del grupo empresarial están sujetas al marco de control de DORA, incluidas las entidades establecidas fuera de la UE.

Revisión de políticas escritas de externalización

aplicadas por la entidad para adaptarlas a DORA, así como de los procesos internos de gobernanza en las tomas de decisión relativas a externalización de servicios de TIC intragrupo y fuera del grupo.

Determinación de la figura de un proveedor tercero de servicios de TIC

Análisis de las funciones llevadas a cabo por parte del proveedor de la entidad financiera y de los servicios que le presta a la misma (especial hincapié en los sistemas de SaaS en los que no existe integración) y evaluación de la esencialidad de las funciones externalizadas. Explicación de los requisitos que determinan la aplicación de DORA a los proveedores.

Análisis de cadenas de subcontratación y su sujeción a DORA

Determinación de si determinados proveedores de un prestador de servicios de la entidad (proveedor tercero de servicios de TIC) es considerado “subcontratista” a efectos de DORA y, en su caso, determinación de los aspectos regulatorios que resultan de aplicación (cláusulas de auditoría y problemática asociada en caso de que el proveedor no disponga de dicha facultad; subencargo de tratamiento, etc.).

INTERACCIÓN CON OTRAS NORMAS

Diseño de marcos de control y cumplimiento integrados

Podemos ayudar a las entidades a diseñar marcos de control y cumplimiento que integren las normas DORA con otras normativas relevantes como GDPR, CER, NIS2, PSD2, Solvencia 2, IA Act., etc. Este servicio permitirá a las entidades financieras tener una visión unificada y coherente de sus obligaciones regulatorias, facilitando su gestión y cumplimiento.

GESTIÓN DEL RIESGO DE LA ENTIDAD FINANCIERA

Soporte en el diseño e implementación de un marco regulatorio interno:

Ayudamos a las entidades a establecer los procedimientos y protocolos necesarios para gestionar el riesgo operativo digital, realizar pruebas de resiliencia, notificar incidentes y supervisar los servicios subcontratados.

Asesoramiento en la formación y concienciación del personal sobre las buenas prácticas en materia de ciberseguridad y resiliencia operativa digital:

Asesoramos sobre los derechos y deberes derivados del Reglamento DORA.

Asesoramiento en la aplicación de medidas de ‘seguridad por defecto’ y ‘seguridad desde el diseño’:

Nos centramos en ayudar en la mejor definición de estas medidas desde las primeras fases del diseño y desarrollo de productos, servicios y procesos de TIC.

Asesoramiento en la promoción de la ‘ciberhigiene’ y la sensibilización sobre ciberseguridad:

Nuestro trabajo se enfoca aquí al desarrollo de estas prácticas entre sus empleados y clientes.

Asesoramiento en la gestión de crisis e incidentes cibernéticos:

Nuestro trabajo implica no sólo el apoyo ante incidentes y crisis cibernéticas, sino en las precauciones contractuales en la cadena de subcontratación con proveedores de servicios de TIC que mitiguen o prevengan este tipo de situaciones

Pérez-Llorca

Servicios **DORA**

GESTIÓN DEL RIESGO DERIVADO DE TERCEROS

Revisión y adaptación de acuerdos y modelos contractuales con proveedores terceros de servicios de TIC:

Nuestro trabajo se orienta a que los contratos cumplen con los siguientes requisitos y estándares de calidad:

1. Requisitos regulatorios del Reglamento DORA: cumplimiento de los estándares de diligencia en la gestión de proveedores que marcan las directrices EBA (en caso de que resulten de aplicación); cláusulas de auditoría; cláusulas de terminación; cláusulas de continuidad de negocio; cláusula de subcontratación; regulación del encargo de tratamiento de datos personales; cláusulas de responsabilidad, confidencialidad, cláusula en la que se regule la póliza de seguros; cláusulas de gestión de ciberseguridad y notificación de incidentes.
2. Estándares de calidad para asegurar la posición contractual de la entidad financiera: establecimiento de las obligaciones de proveedor tercero de servicios de TIC; cláusula de conflictos de interés; cláusula de ley aplicable y jurisdicción; o cláusula de resolución alternativa de conflictos.
3. Llevanza y negociación de contratación: Negociación de clausulado regulatorio con grandes proveedores de servicios TIC, teniendo en cuenta la complejidad y las reticencias que presentan ante la imposición de cláusulas estrictas de subcontratación, auditoría, responsabilidad, etc.

Asesoramiento en la estructuración de funciones de seguimiento de acuerdos con proveedores terceros de servcios de TIC:

Apoyamos a nuestros clientes para que estas funciones se adapten a sus necesidades organizativas específicas y determinamos los riesgos de que un proveedor tercero de servicios de TIC sea sistémico.

Asesoramiento en la gestión de la relación de 'dependencia' con componentes de terceros:

Nuestro trabajo se centra en identificar y documentar estas dependencias para optimizar las actividades de ciberseguridad.

APLICACIÓN DE LA NORMA POR PARTE DEL REGULADOR Y RÉGIMEN SANCIONADOR

Soporte en la interpretación de la norma y asesoramiento ante su aplicación por parte de reguladores:

Asistimos en la gestión de posibles reclamaciones o procedimientos administrativos relacionados con el Reglamento DORA.

Asesoramiento sobre las posibles sanciones en caso de incumplimiento:

Acompañamiento en el análisis de los riesgos económicos derivados de posibles incumplimientos de DORA, a efectos de procedimientos contables (p.ej., provisionado) o de seguro (p.ej., pólizas de ciberincidentes).

Contactos

Raúl Rubio
Socio de Propiedad Intelectual, Industrial y Tecnología

rrubio@perezllorca.com
T. +34 91 353 45 59

Josefina García Pedroviejo
Socia de Servicios Financieros y Fondos de Inversión

jgarciapedroviejo@perezllorca.com
T. +34 91 389 01 09

Joaquín Ruiz Echauri
Socio de Seguros y Reaseguros

jruiz-echauri@perezllorca.com
T: +34 91 432 51 58