DEFINICIÓN DE SERVICIO DE CONSULTORÍA PARA LA ADAPTACIÓN INTEGRAL DE PROCESOS AL CUMPLIMIENTO NORMATIVO EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES.

Este documento se refiere exclusivamente a los servicios de consultoría externa prestados por empresas especializadas en aspectos relativos al cumplimiento de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD) y las normas relacionadas con ella. En particular, este ámbito abarca al cumplimiento normativo y en materia de seguridad de la citada Ley así como del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (RLOPD). Por otra parte, procederá tener en cuenta en su caso aspectos de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico (LSSI) y la legislación de telecomunicaciones relacionada con el tratamiento de datos personales. Asimismo, el consultor deberá conocer adecuadamente la legislación sectorial propia del ámbito de actividad al que aplique la LOPD y los requisitos regulatorios de que se trate en ámbitos como la salud, la administración electrónica, las finanzas, los seguros, las comunicaciones electrónicas, los hidrocarburos, la energía eléctrica, u otras normas específicas sectoriales. Evidentemente, en caso de tratamientos de datos de empleados, el conocimiento de la legislación laboral resulta imprescindible.

Para una adecuada lectura de este documento deben tenerse en cuenta dos advertencias:

1. El documento se refiere a proyectos integrales, o si se prefiere lo que en el lenguaje coloquial se denomina como implementación o implantación de la LOPD. Sin embargo, es evidente que pueden contratarse estudios específicos que no son objeto de este texto.

2. No se propone aquí ninguna guía estandarizada que los consultores puedan aplicar de forma directa. Únicamente trata de contemplar los distintos aspectos que usualmente incluye un proyecto integral de este tipo, siendo sus autores plenamente conscientes de la flexibilidad con que se puede abordar cada caso, y de la mayor importancia que cobrarán unos u otros aspectos dependiendo del tipo de encargo o del objetivo final perseguido por el cliente.

1.- ¿Qué significa la consultoría externa?

Se trata de un asesoramiento externo *a la organización, pero que requiere un estudio y conocimiento de ésta, -sea empresa o administración pública-, y del equipo de personas que la integran. Este tipo de consultoría, sin perjuicio de que pueda incluir consejo estratégico o desarrollar labores prospectivas, debe culminar con propuestas de actuación concreta que permitan bien adaptarse al cumplimiento de la legislación, bien corregir aquellos problemas detectados durante la labor auditora previa.*

El sustrato material sobre el que se proyecta esta labor de consultoría se centra sobre «los datos de carácter personal registrados en soporte físico, que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado» (art. 2.1 LOPD), entendiendo por datos de carácter personal, según se establece en el artículo 3 LOPD, *«cualquier información concerniente a personas físicas identificadas o identificables»,* con las excepciones del art. 2 del RLOPD. Del mismo modo, deberemos tener a la vista la definición que el mismo precepto legal nos ofrece sobre el concepto de fichero al que delimita como «*todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso»*. Por último, no debemos olvidar que incluso en ausencia de ficheros, por ejemplo cuando una videocámara toma imágenes pero no las graba, deben aplicarse distintas previsiones de la LOPD a los tratamientos entendidos como *«operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias».*

2.-Obligaciones de cumplimiento normativo.

Las principales obligaciones que la normativa en protección de datos de carácter personal impone a quien trate datos, -salvo en caso de uso doméstico-, sea responsable o encargado de los tratamientos de estos datos personales o de los ficheros en los que se albergan los mismos, las podríamos resumir en los siguientes apartados:

- Recoger y tratar datos personales exclusivamente para finalidades legítimas y definidas, y hacerlo cumpliendo determinadas obligaciones formales.
- Captar los datos mediante un procedimiento que garantice que se ha informado adecuadamente a la persona cuyos datos se tratan sobre los aspectos principales del tratamiento y sobre sus derechos y,

cuando proceda, se ha obtenido su consentimiento (libre, específico, informado e inequívoco).

- Mantener los datos debidamente actualizados y cancelarlos cuando ya no sean necesarios.
- Implantar medidas que garanticen la seguridad de los datos en sus dimensiones de *confidencialidad* (que nadie no autorizado pueda acceder), *integridad* (que no puedan alterarse los datos por personal no autorizado, ni por el propio personal cuando con ello se incumpla la Ley), y *disponibilidad* (de modo que ante un incidente como un incendio podamos recuperar los datos y/o los sistemas que los soportan). La implementación de medidas de seguridad afecta al medio físico, a aspectos organizativos y técnicos, vincula a todo el personal e incluye la elaboración de un documento de seguridad de obligado cumplimiento para el personal que describa las medidas de seguridad exigidas en el RLOPD, tales como la respuesta ante incidentes de seguridad, los deberes de los empleados o el control de salidas y entradas de datos.
- Registrar y mantener actualizados (o suprimir cuando proceda) los ficheros de datos en el Registro General de Protección de Datos de la Agencia Española de Protección de Datos o seguir el procedimiento específico para su creación establecido en el art. 20 de la LOPD en el caso del sector público.
- Establecer y documentar procedimientos adecuados para la atención del ejercicio de los derechos de acceso, rectificación, cancelación y oposición de los afectados, incluidos los previstos en la LSSI, cuando proceda.
- Adoptar una correcta política en relación con las posibles cesiones de datos a terceros.
- Celebrar contratos que garanticen el respeto de la LOPD por los terceros proveedores de servicios que accedan a datos, a los que técnicamente se denomina encargados del tratamiento.
- Obtener la autorización de la Agencia Española de Protección de Datos en el caso de transferencias de datos de carácter personal fuera del Espacio Económico Europeo, o de países que no tengan la consideración de "seguros" otorgada por la Comisión Europea. O encuadrarlas en una de las causas legítimas que lista la LOPD (art. 34 LOPD).

- Realizar auditorias y controles periódicos para comprobar la bondad de los procedimientos que garantizan la seguridad de los datos.

El desarrollo de un proyecto para la adaptación de procesos al cumplimiento normativo en materia de protección de datos personales, lejos de entenderse exclusivamente como una imposición legal, debería contemplarse como una oportunidad de mejora en el seno de la organización que acomete tal proyecto de consultoría, y así podemos destacar algunas ventajas de tales actuaciones:

- **Protección frente a los riesgos del incumplimiento de la normativa**: Las organizaciones, administraciones y empresas, manejan infinidad de datos personales en el desarrollo de sus actividades y por ello, en caso de infracción, se encuentran expuestas a denuncias por parte de sus clientes/usuarios, empleados, colaboradores y cualquier otro tercero. Cumplir con la normativa es una obligación cada día más importante en la realidad de las organizaciones, y un derecho que se debe garantizar a los ciudadanos por las Administraciones públicas, que además genera confianza a los clientes, usuarios y administrados, y seguridad al mantenimiento y continuidad de las actividades de la organización.

- **Contribución a la calidad de la organización**: El cumplimiento de la normativa en materia de protección de datos, contribuye a la mejora de las condiciones de actualización de la información, a la racionalización de la seguridad de los sistemas de información, a la exactitud de los ficheros y permite ofrecer a los usuarios seguridad y confianza. Además, la implantación de medidas de seguridad en los sistemas de información puede ser objeto de certificación de calidad (ISO 27001, entre otras).

- **Diferenciación de la imagen corporativa frente a competidores**: Los usuarios sabrán que la organización está orientada a respetar la confidencialidad y el derecho de protección de datos, además de cumplir con la normativa, desarrollando un compromiso de calidad y ética empresarial. Saben que, en la organización, sus datos serán tratados bajo procedimientos de seguridad. Cada día que pasa, aumenta la cultura de protección de datos y aumenta también el conocimiento por parte de los usuarios de sus derechos hacia un tratamiento adecuado.

- **Protección de los activos del negocio y optimización de procesos**: Estandarizando el tratamiento de los datos personales se alcanza un control más eficaz sobre los datos y una importante mejora en la gestión documental de la organización. Una adaptación realizada de forma efectiva conlleva blindar la información de clientes, usuarios o administrados, proveedores o empleados, evitando riesgos de vulnerabilidad de estos datos.

3. ¿Cómo se desarrolla la labor de consultoría? El proyecto.

Para el éxito de un proyecto de adaptación plena a la LOPD, se hace necesario que el consultor y el cliente conozcan la organización y los procesos que en ella se desarrollan, tanto en la parte general como en la parte que afecta a las tecnologías de la información y comunicación. El objetivo es determinar los riesgos de la actividad de la organización para determinar el enfoque del proyecto de adecuación dentro de la cultura de la organización donde deba integrarse.

Para lograr esto, el consultor debe obtener una comprensión suficiente del entorno ante el que se encuentra. Ello debe incluir una comprensión general de las diversas prácticas organizativas y funciones relacionadas con el objeto del proyecto, así como los tipos de sistemas, plataformas y aplicaciones que se utilizan para realizar los diversos tratamientos de datos.

El consultor también debe comprender el ambiente normativo en el que opera la organización. Por ejemplo, si el cliente asesorado es médico, el consultor deberá conocer con detalle aspectos relacionados con la gestión de historias clínicas. Lo mismo pasaría –por ejemplo- en el caso de las Administraciones públicas, donde deberá conocer las especificidades que la normativa les aplica.

Asimismo, se deben considerar otros aspectos como la medida en que la organización externaliza o subcontrata sus funciones y servicios para alcanzar sus objetivos.

Este conocimiento, puede obtenerse a través de:

- Lectura de documentación sobre antecedentes que incluyan publicaciones sobre el sector.
- Visitas a las instalaciones del cliente. Por un lado, supone una primera revisión de la seguridad de las instalaciones y, por otro, nos ayuda a alcanzar una primera visión del entorno en el que opera la organización.
- Entrevistas con el personal clave de la organización.
- Estudio de legislación, normas o reglamentos que se apliquen específicamente a la organización o al sector en que ésta opera.

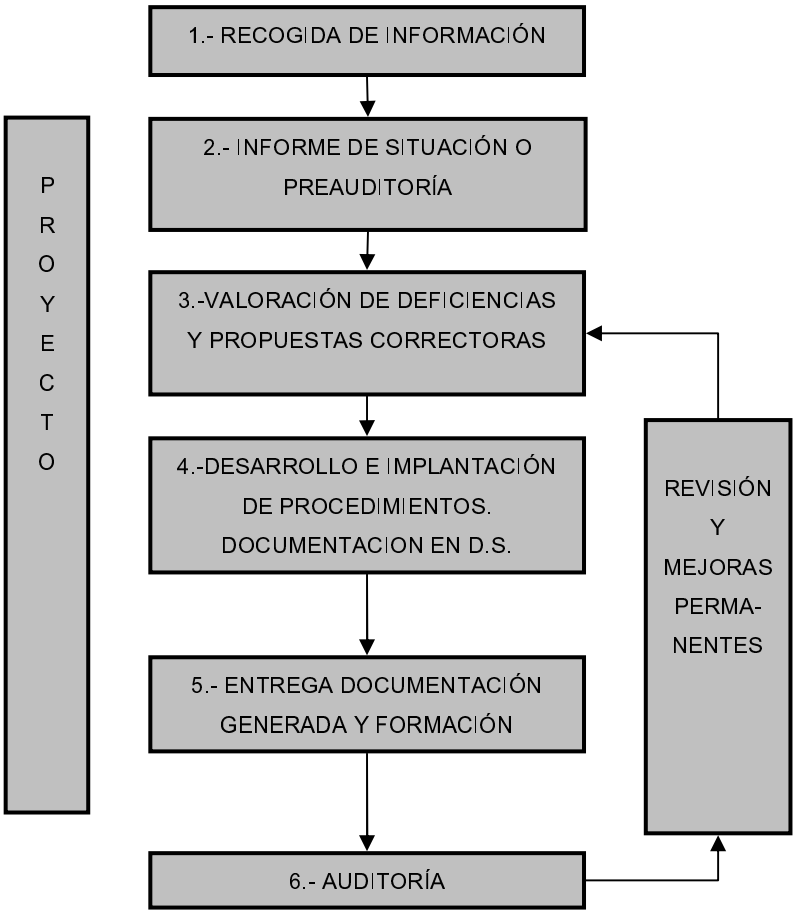
Algunos aspectos esenciales para entender la organización son los siguientes:

- La función de la organización (lo que hace y cómo lo hace), sus metas y objetivos estratégicos.
- Los principales tipos o categorías de datos tratados, el volumen de transacciones y los activos involucrados para tal actividad.
- Las finalidades específicas de cada tratamiento.
- Las unidades organizativas que permitan desarrollar la actividad.
- El número de entornos de trabajo, centros de procesos de datos y dispersión geográfica de los mismos.
- Las entidades jurídicas implicadas, y la forma en que se relacionan, en el caso de grupos de empresas.
- Las aplicaciones clave y los sistemas informáticos que las soportan utilizados para procesar y controlar estas transacciones de datos.
- Planificación de nuevos proyectos que impliquen nuevas finalidades o tratamiento de nuevos datos.

Al realizar un proyecto de adecuación, uno de los mayores problemas es, sin duda, la inexistencia de guías de procedimiento y estándares para desarrollar tal proyecto, motivo por el cual, cada consultora lo hace de una forma. A continuación se indican algunas actuaciones que debería contener cualquier proyecto de adecuación plena, aunque debe subrayarse la flexibilidad con que las mismas puedan desarrollarse en el contexto del proyecto y sobre la base del método particular de trabajo de cada consultora:

- Informe de situación inicial o preauditoría
- Proyecto de adecuación e implantación
- Auditoría externa
- Mejora continua (Damming) y mantenimiento de la adecuación.

Podemos esquematizar el proyecto de la siguiente forma:



La recogida de información.

Mediante uso de formularios y entrevistas con los usuarios, y la realización de visitas presenciales a las instalaciones de la organización, se procede a recoger la documentación e información necesaria para poder realizar el oportuno análisis del flujo de datos dentro (y fuera) de ésta.

Esta información es necesaria para la localización y clasificación de los datos personales en ficheros o tratamientos que, posteriormente en el desarrollo del proyecto, deberán ser contemplados (y, en su caso, registrados). Es recomendable, una vez recogida la información, proceder a su inventariado.

La información la podemos clasificar en:

JURÍDICA	TÉCNICA:	ORGANIZATIVA:
▪Contratos clientes o usuarios ▪Contratos empleados ▪ Colaboradores externos ▪ Contratos proveedores ▪ Contratos con encargados del tratamiento ▪ Flujos de datos (empresas del grupo, otros terceros, trasferencias internacionales) ▪ Recogida de datos (cláusulas, formularios, etc.) ▪ Derechos ARCO ▪ Página WEB ▪Políticas internas (uso de recursos TIC, denuncia de irregularidades, medidas de seguridad, códigos "éticos", etc.)	▪Topografía de red y comunicaciones ▪ Inventario de equipos y aplicaciones Procedimientos de seguridad	▪Centros de trabajo ▪ Departamentos ▪ Cargos Organigrama

*** El volumen de información jurídica, técnica u organizativa puede coincidir con la que se indica a título de ejemplo, ser menor o incluso requerir información adicional. Por ejemplo, es posible que en una PYME no existan transferencias internacionales de datos y, sin embargo, aspectos aparentemente ajenos con lo aquí definidos como la seguridad perimetral o la orografía de una zona sísmica pueden tener un carácter relevante.**

El informe de situación de partida o preauditoría:

Aunque *no existe obligación legal*, la elaboración de este tipo de informes resulta muy útil en la mayor parte de las ocasiones. Tras la primera fase de recogida de documentación, se procede a su análisis y dicho análisis ha de concluir en la emisión de un informe que persigue el conocimiento de la situación actual de la organización en relación al cumplimiento de la normativa vigente.

Este informe deberá contener los diversos ficheros y/o tratamientos de datos personales que se hayan detectado, y dentro del mismo deberíamos encontrar:

- Nivel de seguridad que precisen los ficheros que trata la organización.
- Procedimientos a desarrollar/modificar e implementar.

• Lista de medidas preliminares de tipo jurídico, técnico y organizativo a implantar

• Cronograma de actuaciones a llevar a cabo en función de criterios establecidos (reducción de riesgo de imposición de sanciones, inversión a realizar, recursos disponibles, etc.).

El proyecto de adecuación e implantación plena.

Éste debe reunir ciertas características específicas:

• Debe ser un proyecto lo más **completo** posible. El objetivo del mismo pasa por conseguir una adecuación integral. Sin embargo, en ocasiones puede haber clientes que busquen o consultores que ofrezcan una adecuación parcial o en distintas fases en función de los recursos disponibles o por mero desconocimiento. Por ejemplo, sólo desde el punto de vista jurídico, pero dejando fuera la parte técnica u organizativa. En cualquier caso, el cliente debe entender y el consultor debe hacer saber que una adecuación plena a la LOPD debe ser entendida como un proceso integral, donde los componentes jurídicos, técnicos y organizativos deben interactuar.

• El servicio suele contratarse bien como un **paquete único cerrado** o bien como un servicio que puede ser más flexible en tiempo, recursos y costes incluyendo un **asesoramiento continuado**. En cualquier caso, lo óptimo es que la organización cuente con una adecuación completa e integral.

• **Reducción de costes**. Al coste del proyecto de adecuación debemos sumarle el coste de las medidas a implementar. Este último puede ser reducido mediante la aplicación de acciones correctivas y mejoras en la organización antes de llevar a cabo cualquier implementación de medidas definitiva. No obstante la implantación de las medidas a adoptar en ocasiones será labor del propio cliente o - por ejemplo – de una empresa informática (cuando se trate de medidas de esta índole). En el presupuesto que después forme parte del contrato deberá precisarse si se incluye o no la implantación de estas medidas.

• **Mantenimiento** de la adecuación. El proyecto de adecuación puede incorporar un apartado relativo al mantenimiento de la adecuación una vez realizada.

• **Documentación** asociada al proyecto. Es muy importante que durante la realización de los trabajos de adecuación se genere la documentación necesaria. Esto hace que todo el trabajo realizado se documente correctamente. Parafraseando una expresión jurídica podría decirse que *lo que no se documenta, no se ha realizado*. Además, como se ha subrayado, es imprescindible mantener en el tiempo la adecuación conseguida y, para ello, es fundamental tener toda la documentación organizada.

El proyecto, además, debería, al menos idealmente, incluir la **formación de los usuarios** de quienes dependa la eficacia de los procedimientos implementados. Esta formación, deberá perseguir:

- Trasladar al responsable los conocimientos básicos del derecho fundamental a la protección de datos.
- Explicar los diferentes procedimientos establecidos en la entidad a los efectos de cumplir con la normativa.
- Concienciar al personal sobre su obligación de confidencialidad.
- Dar a conocer las consecuencias en ámbito laboral, civil y penal del incumplimiento de sus obligaciones en materia de protección de datos.

La auditoría.

Finalizado el proyecto de adecuación puede ser muy valioso conocer el grado de cumplimiento de la normativa que la organización haya alcanzado para determinar si es suficiente o si, por el contrario, aún resultan necesarios más cambios.

Además, cuando nos encontramos con ficheros o tratamientos de datos de nivel medio o alto, esta posibilidad de realizar una auditoría interna o externa para comprobar la bondad del proyecto desarrollado se convierte en una obligación normativa que debe cumplirse al menos cada dos años, salvo que se produzcan cambios sustanciales que obliguen a una auditoría extraordinaria. Esta auditoría puede ser llevada a cabo por personal propio, siempre que esté debidamente formado para ello, o por personal externo. Los principios que rigen la labor auditora suponen bien contratar personal externo, bien escoger personal interno ajeno al área auditada para garantizar la objetividad.

Mejora continua.

El proceso de adecuación integral no es un proceso estático, de forma que una vez que finaliza es necesario mantenerlo en el tiempo. Para ello, es imprescindible un proceso de mejora continua y mantenimiento.

Cuando una organización realiza un proyecto de adecuación e implementa un conjunto de medidas de seguridad y procedimientos de actuación, lo hace en función de los usos de los datos de carácter personal que está llevando a cabo en ese momento concreto y la situación actual de la tecnología. Pero, con el tiempo, la organización cambia, se adapta, modifica sus procesos y sus tratamientos. En definitiva, aparecen en ella nuevos usos para los datos de carácter personal. Las

tecnologías cambian, las amenazas pueden ser otras. Estos cambios pueden hacer que una organización deje de cumplir la normativa. Por tanto, es necesario llevar a cabo revisiones y mejoras del proyecto de adecuación realizado.

Es muy importante tener en cuenta el concepto de revisión y mejora continua puesto que de esta forma la organización podrá adaptar, de forma progresiva, la adecuación ya realizada a los cambios y nuevas situaciones que se vayan produciendo.

Si la organización no opta por la mejora continua, con el transcurso del tiempo puede encontrarse ante la necesidad de realizar una adecuación más profunda y costosa. Resulta así recomendable mantener para no tener que realizar todo el proceso de nuevo.

Por otro lado, el cumplimiento de la normativa sobre protección de datos de carácter personal incluye de forma intrínseca el concepto de mantenimiento y mejora continua. Un claro ejemplo de esto (y desde luego no es el único) lo tenemos en el mantenimiento del propio documento de seguridad, que recoge muchos aspectos relativos a las medidas, los accesos, el personal y otros. Si se producen cambios en la organización es lógico pensar que dicho documento será actualizado. Y así lo contempla el artículo 88.7 del RLOPD cuando establece:

> «El documento de seguridad deberá mantenerse en todo momento actualizado y será revisado siempre que se produzcan cambios relevantes en el sistema de información, en el sistema de tratamiento empleado, en su organización, en el contenido de la información incluida en los ficheros o tratamientos o, en su caso, como consecuencia de los controles periódicos realizados. En todo caso, se entenderá que un cambio es relevante cuando pueda repercutir en el cumplimiento de las medidas de seguridad implantadas».

4. El precio del proyecto *vs.* el coste del proyecto.

Desarrollar la labor consultora comporta disponer de una adecuada infraestructura. En particular, es necesario dotarse de un personal cualificado y asistirse de herramientas de análisis. Como cualquier empresa, las consultoras soportan costes fijos vinculados a su infraestructura, personal, medios de producción, seguros de responsabilidad civil, consumos que generan y/o distintos costes variables. Por tanto, difícilmente podrán ofrecer un servicio gratuito. Sin embargo, en el mercado proliferan las empresas que ofrecen “LOPD gratis”, ya sea ofreciendo directamente al cliente asesorado que declare haber recibido un servicio que nunca se presta, ya sea “regalando” este servicio.

Como el lector de este documento habrá podido deducir, los costes de formación son significativamente menores que los derivados de una buena implantación de medidas de cumplimiento de la LOPD. Por tanto, cualquier oferta que equipare ambos servicios u ofrezca uno a cambio de otro plantea tres posibilidades: 1) Nos enfrentamos a algún tipo de fraude; 2) El servicio será equivalente a lo que se pague por él; 3) El oferente está entrando en el mercado con pérdidas, lo que en la situación actual parece cuando menos irracional cuando no increíble.

Por ello, quien ofrezca un servicio subvencionado DEBE PROBAR QUE EL ASESORAMIENTO ES EL OBJETO DE LA SUBVENCIÓN O PUEDE ESTAR COMETIENDO UN FRAUDE SANCIONABLE, y si lo es la formación, O EL ASESORAMIENTO QUE SE OFRECE RESPONDE A LOS PARÁMETROS QUE DEFINE ESTE DOCUMENTO O VD. RECIBIRA UN SERVICIO INADECUADO POR INSUFICIENTE.