Título: Aplicaciones informáticas para el GDPR: ¿adaptar empresas o crear una cultura de privacidad?

Autor: Josep Aragonés Salvat

Resumen: Exposición sobre el cambio de mentalidad que los profesionales de privacidad debemos adoptar a consecuencia de la sustitución de la LOPD por el GDPR. Visión de las prácticas actuales de adaptación a la normativa y desarrollo de procedimientos para una nueva interpretación de la protección de datos basada en la cultura de privacidad. Diseño de nuevas aplicaciones informáticas que ayuden al consultor a configurar el cumplimiento del nuevo Reglamento Europeo de Protección de datos.

Texto:

Las prácticas del consultor: adaptar o concienciar

La normativa de protección de datos se basa fundamentalmente en la relación entre las empresas que tratan datos personales y las personas afectadas por este tratamiento.

Lo primero que se encuentra el consultor cuando realiza una adaptación de protección de datos es cómo transmitir el objetivo del servicio que va a prestar al responsable de la empresa: si se realiza por una obligación legal para evitar sanciones, o por una concienciación de privacidad donde lo relevante es proteger los datos personales y no las sanciones.

El primer caso es el más común actualmente, se adapta la empresa para que cumpla la normativa y se le informa con multitud de documentos ¡de papel! donde está todo lo que la ley determina. A esto se le llama cumplimiento pero el significado real es cumplo y miento. A partir del momento en que una empresa está adaptada y ha pasado por el trámite reglamentario, el responsable se queda con la conciencia tranquila porqué la empresa está cumpliendo y no se preocupa más de la protección de datos. ¿Qué pasa entonces?, que se olvida de firmar contratos, que realiza un tratamiento nuevo y ni se acuerda que debe diseñar un procedimiento para la obtención de datos y la comunicación al interesado, etc. porque piensa que ya está cumpliendo la normativa. Año tras año el consultor le va recordando sus obligaciones y le actualiza el documento de seguridad. Y el empresario continúa teniendo la conciencia tranquila y la sensación que está cumpliendo. Esto es la cultura de legalidad: Adaptar.

Si por el contrario optamos por concienciar al responsable de la protección de datos, deberemos empezar por identificar al interesado. Más fácil introducción imposible, porqué estamos hablando con una persona y a ésta le están tratando sus datos otras empresas. Cuando el interlocutor (aunque responsable de la empresa) se pone en la piel del interesado, es cuando empezamos a crear cultura de privacidad. Si a cada operación de tratamiento se incorpora una visión como interesado, estaremos dando sentido a la protección de datos y el responsable de la empresa estará predispuesto a pensar en ella antes de diseñar un nuevo tratamiento, no por una obligación legal, que también, sino porqué está concienciado de ello. Esto es la cultura de privacidad: Concienciar.

Qué debemos olvidar de la LOPD

En España existen más de 3 millones de empresas activas y probablemente un tercio están adaptadas a la LOPD, otro tercio sabe que debe adaptarse pero no lo ha hecho y las restantes o piensan que no les afecta o ni saben que existe.

La LOPD establece la obligación de notificar los ficheros en un registro público para su consulta general y así poder discernir cuales empresas están o no adaptadas a la normativa. En el considerando del GDPR ya se advierte que esta medida no ha dado el fruto esperado, ya que la adaptación a la LOPD se ha basado principalmente en el registro de dichos ficheros a la autoridad de control.

Aunque el objetivo final que se pretendía con este registro no se ha logrado, lo que sí se ha conseguido es que la mayoría de empresas se hayan enterado que existe una legislación de protección de datos que deben cumplir y que, de no hacerlo, les pueda afectar con sanciones económicas. Eso sí, a desgracia de las malas prácticas de comerciales, dichos por sí mismos consultores, que revisan dicho registro

habitualmente para amenazar las empresas que no tienen los ficheros debidamente inscritos. Con el nuevo Reglamento esto ya no será posible. Vamos a aprovechar esta oportunidad para que estas prácticas no tengan lugar y los servicios de privacidad solo estén en manos de profesionales.

Aprovecho esta circunstancia para hacer un inciso de *mea culpa*. Los profesionales de privacidad, en los cuales me incluyo, aunque no amenacemos a nadie también nos hemos beneficiado de ello, apoyándonos en este registro para identificar la vulnerabilidad de la empresa y advertirles de su incumplimiento. Y si no, sólo hace falta mirar las cláusulas informativas del tratamiento donde parece que lo más importante a informar es que el fichero está inscrito en el Registro General de Protección de Datos. Y por si fuera poco, también cabe mencionar y reflexionar sobre la preocupación del sector en el hecho que ya no sea obligatoria la notificación de ficheros porque van a disminuir notablemente sus recursos comerciales.

A partir de ahora, no podrá sancionarse por la notificación de ficheros o por no disponer de un documento de seguridad, o por no realizar inventarios de soportes o software o por la infinidad de disposiciones burocráticas que establece la LOPD. El nuevo GDPR prima la efectividad de la protección de datos y la transparencia en la información que se transmite al interesado.

Para esto vamos a estar los consultores, para concienciar a los responsables de las empresas que deben proteger los datos y dar una información clara del tratamiento de la misma manera que ellos desearían que otras empresas hicieran consigo mismo. La concienciación es la mejor garantía de protección de datos y fomentarla es sembrar cultura de privacidad.

Qué debemos aprovechar de la LOPD

Mucho. El nuevo Reglamento recoge el espíritu de la LOPD y la mayoría de las disposiciones en ella establecidas. No es un cambio radical, es un cambio conceptual. Aunque existen nuevos preceptos adaptados a la actualidad como el ámbito territorial, el consentimiento explícito, nuevos derechos para los interesados, la evaluación de impacto, etc. y nuevas figuras como el corresponsable del tratamiento o el delegado de protección de datos, la base fundamental sigue siendo la misma y todo el esfuerzo realizado hasta ahora no ha sido en vano. Va a ser más fácil adaptarse al GDPR si ya se está cumpliendo con la LOPD.

Visto esto, debemos aprovechar la publicidad que generará la vigencia del nuevo Reglamento mediante noticias en los medios de comunicación, que seguramente generarán preocupaciones a las empresas para saber en qué medida les afecta. La oportunidad nos viene dada ¡ahora!, no dentro de un año. Este es el momento para diferenciarnos de los demás realizando adaptaciones a la nueva normativa.

Las aplicaciones informáticas que hasta ahora estaban destinadas al cumplimento de la LOPD han hecho su papel porque han sido de gran ayuda para los consultores, pero ¡ahora! también deberán cambiar el chip y adaptarse lo más pronto posible al GPDR. No caigamos en la tentación de apurar la vigencia de 2 años que tiene la LOPD, porqué los consultores no van a esperar este tiempo para adaptar a sus clientes a la nueva normativa.

La máxima para cualquier profesional que se dedique a la privacidad, sea consultor o desarrollador de aplicaciones, ha de ser olvidarse tan pronto como sea posible de la LOPD y sustituirla por el GPDR. Y sobre todo, hacer bandera de ello transmitiéndoselo a las empresas que prestan sus servicios para que participen de este evento y se ocupen de lo mismo.

GDPR, la nueva cultura de privacidad

Para realizar una adaptación al GDPR primero que nada deberemos conocer a fondo la normativa, hacernos una idea general de las nuevas disposiciones y de las que ya no tiene sentido cumplir porque no las recoge el Reglamento. A partir de aquí se podrán diseñar procedimientos de adecuación para migrar de la LOPD al GDPR, o directamente realizar nuevas adaptaciones al GDPR para no caer en la tentación de transmitir a las empresas que la nueva normativa solo incluye algunos cambios con los mismos procedimientos. Como hemos dicho anteriormente, no debemos perder de vista el cambio de mentalidad de obligación legal por concienciación.

Para ello, es imprescindible la formación. Si el responsable de la empresa comprende y se conciencia del objetivo será mucho más fácil que entienda el procedimiento. La formación transmitida al interlocutor no puede ser genérica, deberá ser clara, sencilla, específica y ajustada a las particularidades de cada empresa, solo así el responsable se interesará por las propuestas que le planteemos, solo así entenderá que debe diseñar su organización para proteger los datos personales. Si conseguimos esto habremos logrado que cumpla el 50% del Reglamento porque su principal objetivo es concienciar al responsable para que transmita al personal y encargados del tratamiento que deben proteger los datos personales y mantener su confidencialidad. Este procedimiento confiere al interlocutor un sentido lógico del Reglamento y una actitud proactiva para adoptar sus disposiciones.

El 50% restante vendrá dado por la implementación de los procesos de protección de datos que obliga la normativa, que una vez compartidas y entendidas por el responsable de la empresa, también deberían imponerse para garantizar la licitud del tratamiento y la seguridad de los datos.

Debemos tener en cuenta que no todas las empresas son iguales y que la mayoría piensan que ya están protegiendo los datos, pero hay infinidad de eventualidades, de las cuales no son plenamente conscientes, que pueden ocasionar violaciones de seguridad que afecten los datos y consecuentemente la intimidad de las personas. Es aquí donde deberemos poner el énfasis, en la concienciación para elaborar protocolos personalizados de políticas de información y de seguridad que garanticen la protección de datos.

Esta va a ser la gran labor del consultor, concienciar, formar y escudriñar en las operaciones de tratamiento que realiza la empresa para establecer una correspondencia entre los procedimientos usados y la aplicación de la normativa. No valdrán documentos automatizados generalizados para todo tipo de empresas, lo que realmente valdrá será la profesionalidad del consultor para evaluar las intenciones del responsable y asesorarle adecuadamente con el fin que el tratamiento se ajuste a la legalidad.

De la misma forma, las aplicaciones informáticas dedicadas al GDPR, deberían diseñarse con este cometido para que realmente ayuden a los consultores a realizar su trabajo. Pero esto no es todo, también deberían diseñarse para ser usadas por el responsable de la empresa, para incorporar la aplicación a su sistema organizativo como una herramienta más de uso habitual como la facturación, contabilidad, etc. Solo así tendrá la percepción que no es una obligación legal sino que la protección de datos va incluida en la gestión cotidiana de la empresa.

Las aplicaciones informáticas, una gran ayuda para el consultor

Volvemos a recuperar el enunciado de este artículo, “Aplicaciones informáticas para el GDPR: ¿adaptar empresas o crear una cultura de privacidad?”. Tal como hemos descrito anteriormente, la respuesta es crear una cultura de privacidad. Y, ¿cómo diseñar una aplicación que favorezca la concienciación? Vamos a ello.

Actualmente hay infinidad de aplicaciones que los consultores usan para realizar adaptaciones a la LOPD y que han hecho su función muy dignamente. Estas aplicaciones basan su diseño en la aplicación de la LOPD, o sea en la notificación de ficheros y su estructura de datos, en el inventario de soportes y mobiliario donde se almacenan datos, en la identificación de mecanismos de seguridad, etc. Todo ello sin menoscabar la gran utilidad para el registro de personal y empresas externas con sus correspondientes contratos y para generar la documentación que obliga la LOPD, entre ella el tan codiciado documento de seguridad, que dicho aparte casi nadie se lee.

Las nuevas aplicaciones para el GDPR lo tienen más fácil que con la LOPD. No será necesario notificar ficheros, ni inventariar nada, ni identificar mecanismos de seguridad, ni llevar registros de accesos o de entradas y salidas de soportes, etc. A nada de esto obliga la nueva normativa. Pero esto no significa que ya no se deberá documentar ni registrar nada, al contrario, el Reglamento impone unos ejes principales que deben cumplirse para que el tratamiento sea lícito, la información y transparencia con el interesado y la adopción de medidas adecuadas de protección de datos. Y no menos importante, exige que el responsable sea capaz de poder demostrarlo.

Las aplicaciones informáticas deberían recoger el espíritu del Reglamento y ofrecer mecanismos para una actualización instantánea de cualquier operación de tratamiento que pueda realizar el responsable como documentación probatoria de cumplimiento.

Aplicar la normativa mediante una aplicación informática

El Reglamento europeo nos obliga a diseñar el tratamiento para que por defecto estén protegidos los datos y el interesado pueda obtener el gobierno de los mismos, por eso las aplicaciones deberán tener en cuenta este procedimiento, o sea definir los ficheros y aplicarles la normativa a cada uno de ellos. Lo primero y más importante, reitero, es la formación. Una vez el responsable del tratamiento sea consciente del alcance y la finalidad del GDPR podrá configurar y clasificar los datos personales que está tratando en ficheros y asignarles las categorías de datos y de tratamiento que les afecte la normativa.

El Reglamento dispone de una normativa específica para distintas categorías de datos o de tratamiento. Por esta razón la aplicación debería contener una tecnología para aplicar esta clasificación al fichero antes de aplicarle la normativa que le corresponda.

Cuando la empresa tenga definidos los ficheros y las categorías que trata, deberá determinar cuáles datos son de su responsabilidad y cuáles son por encargo de otra empresa. La diferencia es imprescindible detallarla porque con los datos que somos responsables determinamos los medios y los fines del tratamiento y con los datos que nos han encargado tratarlos, los medios y los fines nos vendrán dados por las instrucciones recibidas en el encargo.

La LOPD solo distinguía los ficheros como responsable (los que se notificaban a la AEPD) y el encargado era un autorizado para tratarlos. El GDPR obliga al encargado a ofrecer garantías suficientes para implementar políticas técnicas y organizativas apropiadas para cumplir las disposiciones del Reglamento y también a ser capaz de demostrarlo. Por este motivo lo más aconsejable es añadir al tratamiento los ficheros de encargado y aplicarles la normativa que les corresponda como tal. La empresa se va a concienciar más de la magnitud de la protección de datos si tiene detallados todos los ficheros que está tratando, sean o no de su responsabilidad.

Una vez creados los ficheros, con sus categorías de datos y de tratamiento, se les han de aplicar los principios del tratamiento, determinando los fines, la minimización, la exactitud y los criterios de conservación para cada uno de ellos, excepto para los ficheros de encargado que nos vendrán dados por las instrucciones del responsable. Para tratamientos existentes, esta operación servirá como auditoría de cumplimiento. Para futuros ficheros deberá diseñarse el tratamiento para que los cumplan por defecto.

Existen otras disposiciones que afectan a todos los datos en general y la aplicación debería poder determinar su cumplimiento, como son el diseño de una política de información para asegurar la lealtad y transparencia con el interesado y la creación de una política de seguridad para garantizar la integridad y confidencialidad de los datos.

Con estas funciones ya tendremos la estructura del tratamiento y le habremos aplicado la normativa que le afecta. A partir de aquí deberán registrarse las personas autorizadas a tratar datos y asignarles los permisos de acceso a los ficheros para realizar el tratamiento que le ha sido encomendado. De la misma forma procederemos con las empresas externas, registrándolas y asignándoles los ficheros que les hemos encargado para tratar datos. Por supuesto también deberán generarse los contratos pertinentes a cada una de las figuras que intervengan en el tratamiento y poder realizar un control eficiente de sus firmas para poder demostrar la responsabilidad proactiva a que obliga el Reglamento.

Las empresas externas deberán diferenciarse, como en la LOPD, por su responsabilidad en el tratamiento como encargados, destinatarios o sin permiso de acceso a datos, y en caso de tratar datos de otras empresas como responsables o cesionarios. También deberemos tener en cuenta la nueva figura de corresponsable del tratamiento cuando varios responsables determinan por separado los fines o los medios de tratamiento.

Debido al auge de aplicaciones de internet para tratar datos merece capital importancia la licitud de las transferencias internacionales de datos. La normativa detalla disposiciones específicas que deberán

implantarse para que estos tratamientos se reflejen en los contratos y en las políticas de información y de seguridad antes mencionadas.

Al igual que las transferencias internacionales de datos, se deberá poder asignar a cada fichero las diversas categorías de tratamiento, para aplicarles las disposiciones específicas que establece el Reglamento, por ejemplo en la elaboración automatizada de perfiles, el tratamiento de datos a gran escala y los tratamientos que prevean un alto riego para los derechos y libertades de los interesados.

También deberá disponer de mecanismos para la llevanza de un registro de actividades y aplicarlo como responsable o encargado del tratamiento según cumpla los requisitos establecidos en el Reglamento.

Solo queda la documentación. La aplicación deberá contener un apartado con las cláusulas generales a aplicar para la información del tratamiento y la obtención del consentimiento, pero también para personalizar la política de información de acuerdo con el tratamiento y poder personalizar documentos específicos para transferencias internacionales o elaboración de perfiles. No basta solo con facilitar una documentación generalizada sino que deberá poder adaptarse a la particularidad de cada operación de tratamiento.

De la misma manera deberá poder diseñar una política de seguridad personalizada a cada empresa para analizar desde el diseño y por defecto los riesgos del tratamiento y, si es el caso, llevar a cabo una evaluación del impacto para poder mitigar dichos riesgos.

Toda la documentación que genere la aplicación debe estar diseñada para ser útil al responsable de empresa. Debe contener información clara y precisa. Estar organizada tipo informe para que le dé un valor añadido al receptor. Con solo reportar la documentación que obliga el GDPR no será suficiente, porque son documentos necesarios pero no específicos. Lo mismo que pasa con la facturación o la contabilidad, los documentos legales no aportan información añadida, se tiene que filtrar y establecer conceptos comerciales para que reporten la información que realmente interesa al responsable de la empresa. Lo mismo debe procurar la aplicación, generar documentación que de sentido a todo este cometido y que aporte un valor añadido al destinatario.

Y por último, las garantías de cumplimiento que establece el Reglamento van a ser vitales para fomentar la cultura de privacidad. Cualquier empresa que quiera garantizar el cumplimiento debería obtener una certificación que le sirviera para demostrar la transparencia del tratamiento ante los interesados (personas clientes) y garantizar el cumplimiento en caso de tratar datos por encargo (empresas clientes).

Todo lo aquí reflejado debería formar parte de un informe de protección de datos que contenga un resumen sintetizado y expuesto de forma clara y concisa de la información más relevante del tratamiento y la protección de datos, para que el responsable de la empresa se dé cuenta que lo que está llevando a cabo tiene una importancia vital para su empresa y para su repercusión en la sociedad.

Conclusiones

Como resumen de la adaptación al GDPR detallamos los procedimientos mínimos que debería disponer una aplicación informática que se dedique a ello:

- Diseño agradable y sencillo para promover la concienciación de privacidad.
- Formación sintetizada y personalizada para cada tipo de categoría de datos o de tratamiento.
- Identificación de los datos personales que trata la empresa (selección de ficheros de responsable y de encargado).
- Asignación de la normativa para cada fichero según su categoría de datos y de tratamiento.
- Revisión de la normativa que afecta a la empresa en general según los ficheros que utiliza.
- Registro de personal y empresas externas con la generación de contratos personalizados para cada tipo responsabilidad y control de firmas.
- Selección de documentos informativos vinculados al tratamiento específico de la empresa: consentimientos, cláusulas, avisos legales, certificados, logos, etc.
- Creación de los informes que obliga la normativa para personalizarlos al tratamiento: responsabilidad proactiva, registro de actividades, evaluaciones de impacto, etc.

- Estado general de la protección de datos con información clara y específica de las faltas de cumplimiento: normativa, informes, registros, contratos, etc.
- Acceso directo de las empresas responsables a su protección de datos.

El nuevo Reglamento europeo de protección de datos nos brinda una oportunidad única y tenemos que aprovecharla. Olvidémonos de la LOPD y apostemos por el GDPR. Conseguiremos que la concienciación impere sobre la sanción. De nosotros depende cambiar la cultura de la legalidad por la de privacidad.

Animo a todos los profesionales de privacidad a esforzarse para alcanzar este objetivo. Si lo conseguimos, nuestro trabajo va a ser valorado y nuestra profesión respetada.