La Pyme frente a la nueva Ley de Protección de Datos (LOPD)

La Ley Orgánica de Protección de Datos de Carácter Personal, LOPD, sustituta de la LORTAD, sigue alcanzando hitos de cumplimiento de plazos para la adecuación de las empresas en lo que a la custodia y tratamiento de la información personal en formato electrónico se refiere.
Veremos algunas reflexiones, estrategias y consideraciones, adecuadas para las pequeñas empresas que no cuentan con recursos o conocimiento especializado, pero no entraremos en detalles sobre la Ley, que puede consultarse en el servidor web de la Agencia de Protección de Datos, en su página https://www.agenciaprotecciondatos.org/datd.htm y que fervientemente recomendamos leer

Antonio Requejo

Director de la División de Seguridad de Germinus Solutions.

La LOPD es de aplicación a ficheros con información de datos de carácter personal de personas físicas, tanto en formato electrónico como "tradicional". Adicionalmente a la publicación de la Ley se publicó el Reglamento de Medidas de Seguridad de los Ficheros Automatizados que contengan Datos de Carácter Personal. Este Reglamento, tal y como se deduce por su título, se centra en establecer las medidas de seguridad de cada uno de los niveles de seguridad de la Ley en lo que a ficheros electrónicos, redes de comunicación, y tratamiento informatizado de los datos se refiere. El Reglamento puede encontrarse en Internet, en la misma página anteriormente citada.

Los ficheros, dependiendo de su contenido, se clasifican en tres niveles con diferente y creciente nivel de exigencia:

- El nivel más bajo es el **nivel Básico**: Todos los ficheros que contengan datos de carácter personal son, por defecto, al menos de nivel Básico.
- El **nivel Medio** engloba a ficheros con información sobre infracciones administrativas o penales, Hacienda Pública, servicios financieros, así como los conjuntos de ficheros de nivel Básico que contengan da-

tos que permitan estimar la personalidad del individuo. Las medidas son todas aquellas aplicables al nivel Básico y otras adicionales.

- El **nivel más alto** queda para los ficheros que contengan datos relativos a la ideología, religión, creencias, origen racial, salud o vida sexual. La exigencia es máxima con estos ficheros.

El ámbito de aplicación de la Ley y las medidas a las que se refiere el Reglamento no se aplican solamente a los ficheros en sí, sino que las localizaciones físicas, hardware, software, redes y personal involucrado en su ciclo de vida también entran en consideración.

Los plazos para la adecuación de la seguridad de los ficheros (no aplicable a los nuevos desde la publicación de la Ley, que ya deben cumplir con ella) son (eran):

- **Nivel Bajo:** Antes del 26 de marzo de 2000.
- Nivel Medio: Antes del 26 de junio de 2000.
- **Nivel Alto:** Antes del 26 de junio de 2002.

Por completar, simplemente citar que las sanciones van desde los 600 € a los 600.000 €, cifras que pueden resultar catastróficas para muchos pequeños negocios.

Es la impresión generalizada que la situación de los ficheros de datos se encuentra aún distante de la situación ideal, y que al igual que las Tecnologías de la Información y Comunicaciones (TIC) han favorecido el desarrollo, eficiencia y eficacia de las pequeñas y medianas empresas, esas mismas tecnologías conllevan un nivel de complejidad que muchas de estas PYMEs (Pequeña y Mediana Empresa) y SoHos (Small Office & Home Office) tienen dificultad en manejar. Algunas fuentes cifran en más del 80% el volumen de PYMEs que incumple en algún punto la LOPD. Aun así, Juan Manuel Fernández López, Director de la Agencia, ha reiterado en numerosas ocasiones la evolución positiva que está teniendo la implantación de la Ley.

Un punto importante del que hay que partir es que, al contrario de lo que puede suceder con otros ámbitos del mundo empresarial y organizativo, en aspectos de Protección de Datos una empresa pequeña y una gran multinacional sólo se diferencian en el volumen de datos, pero el tipo y complejidad de las medidas, excepto por el citado volumen, son las mismas. Aunque las inversiones necesarias y los gastos de mantenimiento serán obviamente proporcionales a dicho volumen, no hay que pensar que para una empresa pequeña es una tarea menor. Proporcionalmente a su tamaño es una tarea importante y de complejidad no despreciable. Pensemos en una farmacia, por ejemplo. Aun siendo un negocio generalmente local, que involucra a pocos empleados, los datos que mantienen tienen una gran sensibilidad, merecedora de la calificación de nivel alto. Una empresa farmacéutica que trabaje con ensayos clínicos probablemente cuente con más información, con más ficheros, pero serán del mismo nivel. Las exigencias de la Ley son las mismas con una que con otra, y las medidas a implantar son cualitativamente las mismas.

También es cierto que las pequeñas empresas deben analizar convenientemente hasta qué punto y cuáles son las medidas directas que deben aplicar, ya que no es inusual que parte de la gestión del ciclo de vida (por ejemplo la destrucción) de los datos sea realizada por un tercero, al que se contratan sus servicios. Recordemos que la delegación en un tercero no supone una trasferencia de la responsabilidad, sino una compartición, aunque puede suponer no tener que implantar medidas directamente por nuestra parte.

Esta complejidad de la que se habla, se debe principalmente a que las actuaciones que se requieren para adaptar la custodia, tratamiento y uso, y movimiento de la información, hay que realizarlas de forma ineludible en tres frentes:

- Organizativo: La LOPD y el Reglamento hablan de la existencia de figuras y roles dentro de la organización, como el Responsable del Fichero o el Responsable del Tratamiento, pero además, las empresas deberán incorporar, probablemente dentro de su Política de Seguridad, procedimientos corporativos que aseguren que sus empleados conocen y respetan la Ley en el uso que dan a los ficheros con la información a la que la LOPD resulta de aplicación. Estos procedimientos han de tener la doble vertiente de ser aplicables tanto a las nuevas tecnologías como a los ficheros más tradicionales. Igualmente, se deben de proveer todos aquellos procedimientos de gestión de los ficheros, incluyendo la capacidad de cancelación o rectificación por parte de las personas físicas a las que se refiera (lo que la Ley denomina "interesado" o "afectado"). Todo ello además de la redacción obligatoria del Documento de Seguridad, según el nivel que se trate.

Esta sobrecarga administrativa puede resultar gravosa en exceso para las pequeñas empresas, cuya formalización suele ser muy baja, pero a su vez se puede aprovechar para acometer la labor de formalizar ciertas operaciones de la organización e inculcar la cultura del procedimiento de trabajo. Las pequeñas y medianas empresas encontrarán muy conveniente acudir a empresas externas que les apoyen (nunca les sustituyan) en el trabajo de realización de su Plan de Adecuación a la LOPD en su parte procedimental.

- **Tecnológico:** El Reglamento establece las medidas técnicas de protección que deben tener cada uno de los niveles en que se clasifican los ficheros, clasificación que aparece dentro del citado Reglamento. El nivel alto, que es de aplicación a los ficheros con información sobre ideología, religión, salud, vida sexual y similares, establece estrictos niveles de seguridad en el acceso, almacenamiento, distribución y respaldo. Como ejemplo, exige que se disponga de respaldo de los datos en varias localizaciones geográficas, que los datos del control de acceso (fecha, hora, usuario, fichero accedido...) se guarden durante dos años, o que toda trasmisión de los mismos sea cifrada. Una empresa de tamaño pequeño encontrará gravoso no sólo el desembolso necesario para dotarse de la infraestructura de soporte a las medidas, sino también el proceso de selección, mantenimiento y formación asociados a la inclusión de controles, auditorías y procedimientos.

Nuevamente el apoyo de empresas especializadas en seguridad lógica facilitará estas labores y proporcionará una correcta selección y dimensionamiento que lleven a una minimización de costes. Adicionalmente, se puede acudir a la externalización de parte de la seguridad. Esta opción supone una elección muy ventajosa, pues se reducen costes y se obtiene acceso a profesionales muy cualificados. Varias de las posibles soluciones técnicas que pueden hacer cumplir el Reglamento son susceptibles de ser externalizadas. Por citar alguna, aparte de la instalación y puesta en marcha de los sistemas para asegurar la confidencialidad de las comunicaciones se puede externalizar completamente el servicio, y cumplir la obligación (para el nivel más alto) de cifrar las comunicaciones mediante un servicio de red privada virtual externalizado. Firmando los correspondientes contratos y acuerdos de nivel de servicio (SLA) y confidencialidad (NDA) asegurаríamos nuestras obligaciones de forma solidaria con el proveedor de servicios.

Pero no nos quedemos en que todas las medidas son complejas y caras. Para algunas de las obligaciones, como por ejemplo la de informar al usuario de que se están recogiendo sus datos, habrá que incluir información junto a los formularios web o junto a los enlaces de correo electrónico, por ejemplo. Estas "medidas" tan concretas no suponen un trastorno importante.

Otro ejemplo puede ser la custodia en localización física alternativa de las copias de respaldo y los registro de acceso; empresas especializadas disponen de logística y espacio para la gestión ágil de copias de back-up, tanto para su recepción como para su búsqueda o envío al cliente.

- Por último, el frente **Jurídico**, en el que posiblemente requiramos conocer la exacta interpretación de la Ley a nuestro caso particular. Tanto Ley como Reglamento son bastante claros, pero existen algunos puntos que pueden resultar equívocos y suscitar diferentes interpretaciones. Aunque la experiencia del personal técnico, experto en seguridad, es una fuente fiable (siempre que la elección sea la adecuada, por supuesto), nunca está de más y es casi obligado consultar a expertos juristas que, preferentemente cuenten con un conocimiento en jurisprudencia aplicada a las nuevas tecnologías. Puede ser necesario conjugar los conocimientos técnicos y jurídicos para establecer qué nivel de seguridad merece, por ejemplo, el uso que hacemos de las cookies desde nuestro servidor web, o la lista de direcciones de correo electrónico para la distribución de información. ¿Qué sucede con los seguros médicos? ¿Suscribir uno para nuestros empleados puede ponernos en situación de obligación de aplicar las medidas más estrictas del Reglamento?

Muchas empresas cuentan con asesoría jurídica, por lo que les resultará natural ampliar y complementar los trabajos técnicos con asesoramiento legal especializado.

En resumidas cuentas, no se puede sino apremiar a todas las PYMEs a que aseguren su cumplimiento estricto Ley y Reglamento. Afortunadamente en España contamos con profesionales de la seguridad (en todas sus vertientes) con experiencia y trayectoria suficientes como para proporcionar ayuda y soporte a empresas que no cuenten con recursos técnicos, jurídicos y de gestión suficientes. ❑